Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Материалы
XXIII Международной научно-технической конференции
(Минск, 08 апреля 2025 г.)

Минск БГУИР 2025

УДК 004.056.5
ББК 32.972.5
Т38

Т38 **Технические** средства защиты информации : матер. XXIII Междунар. науч.-техн. конф. (Республика Беларусь, Минск, 08 апреля 2025 года) / редкол. : О. В. Бойправ [и др.]. – Минск : БГУИР, 2025. – 408 с.
ISBN 978-985-543-513-7

Издание содержит тезисы докладов, тематика которых посвящена вопросам технической и криптографической защиты информации, элементной базе средств защиты информации, нормативно-правовому регулированию и подготовке специалистов в области защиты информации.

УДК 004.056.5
ББК 32.972.5

ISBN 978-985-543-621-9

ОГЛАВЛЕНИЕ

TABLE OF CONTENTS

UDC 004.421.3

FACIAL RECOGNITION SYSTEMS

M.M. Hojammedov
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. On the basis of this program, the program that registers employees by face at the entry-exit points is designed for the security of electronic document exchange and the use of cryptographic methods of data protection. The program allows solving the following problems in data transmission systems and computerized systems, i.e., the reliability of information exchange in electronic document exchange and security, high level of confidentiality of the transmitted information, resistance to various crypto-attacks, it allows to carry out tasks such as simultaneous implementation of data encryption and decryption. This program can be installed and used in any office or business.
Keywords: protect, confident, resistance, encryption, decryption.

Introduction

Facial recognition systems. The process of face recognition is usually a set of different tasks that serve to recognize a person from a digital image or video clip. In general, the process looks like this: after the system receives an image from the camera, the face boundaries are determined by algorithms (the face extraction phase). After that, the recognition phase begins, where the face is modified (brightness, alignment, resizing, etc.) and brought to a certain shape. The features are then calculated and directly compared to benchmarks stored in the database. This final stage of comparison is called identification or verification, depending on the system.

Verification: Comparison of samples in a "1:1" scheme. To identify an individual, the system compares the biometric sample with a biometric template stored in the database and asks, "Is this person the same person as the template?" answers the question. Identification: Comparison of samples in a "1:N" scheme. To determine the identity, the system compares the biometric sample with all facial templates stored in the database and asks "who is this?" answers the question.

Recognise face by person. Humans can identify their surroundings in tens of milliseconds. Such a high rate of object recognition is possible because our brains make constant predictions about what we see and compare these predictions with information from the outside world. There are three main steps in human face recognition:

1) to determine the physical characteristics of the subject;165

2) identify the person, based on which we determine whether the person is known to us or not;

3) we know the person, but we still don't know whether we know his name or not.

Scientists have found that certain areas of the human brain are activated at each stage. As psychologists point out, face recognition is more related to the cognitive side of emotion. In fact, face recognition occurs as follows: the brain constantly compares what it sees with what it holds in long-term memory. Ironically, this is how almost all face recognition algorithms already embedded in the database work. For example, when we look at an object such as a watch, we compare what we see with the features specific to the mental image of the watch. Not all watches are the same, and although some models of this object may differ from the prototype in mind, each watch has key features that are unique to it, such as the minute and hour hands that aid recognition, and the dial. The image of the object is then classified into a specific category and stored in memory. The more hours our brain stores, the easier it is to recognize something new.

Object classification is usually the final step in the recognition process, but in the case of face recognition, it's just the beginning. If it is enough to recognize a clock as a clock, it is not enough to recognize a human face as a human face. Almost immediately we judge a person's gender and age, race, and even whether we like them or not. In addition, we immediately determine whether this face is familiar to us. If a person is familiar to us, we immediately start receiving information from them, just like a face recognition algorithm. It can identify a specific person and then access the information and send a signal to the crime agency depending on why it was created.

The problem of face recognition was considered in the early days of computing. Certain companies have been actively developing automated human identification systems for more than 40 years, and today: Smith and Wesson (ASID system - Automated Suspect Identification System); ImageWare (FaceID system); Imagis, Epic Solutions, Spillman, Miros (Trueface System); Vissage Technology (Vissage Gallery System); Visionics (FaceIt System).

Different methods have been proposed to solve the problem of face recognition, among them, based on neural networks, based on Karhunen-Loeve partition, algebraic moments, lines of equal intensity, and elastic (deformation) comparison standards. The development of recognition algorithms focuses on the automatic selection of facial elements (eyes, nose, mouth, chin, etc.) from various images: face, profile and arbitrary angle. In addition, these geometric features are used to solve recognition problems. A common feature in describing these approaches is the lack of comparison in a statistically significant database.

Geometric comparison based on the definition of facial elements – facial elements: eyes, nose, mouth, chin, etc. A face can be recognized even though individual facial elements are not visible enough. The idea of scaling is to find the relative position and features of the individual elements of the face. Even when face elements are entered manually, the computer shows very good results.

A benchmark comparison is a built-in image representation as a byte array – the intensity magnitudes are compared to the large surface – a metric that matches the benchmark. There are several ways to prepare and display benchmarks. Several benchmarks are used for recognition from different perspectives.

A recognition scheme in neural networks is of interest. In particular, the use of a network of hyperbasic functions in feature vector synthesis for arbitrary angle recognition of 3D objects. In this case, the mesh inputs include the surface elements, including their position in the image. The hyperbasic functional grid, the amplitudes of the gradients for each pixel and the centers of the corresponding standards, different centers in different schemes, is similar to the scheme described earlier for comparing Face Elements templates. In these correlation coefficients, instead of the maximum method, linear classification by Gaussian functions of the correlation coefficients can be fitted. The problem of the dependence of the recognition results on the shooting angle can be solved in several ways. If there are images taken from different angles for each individual, the same recognition schemes can be used at the expense of increasing the computational cost. Using hyperbasis functions - classifications with the possibility of interpolation between different projection points is very risky. However, in reality there may be only one face image to create a template. Of course, a single image of a 3D object does not contain enough information. However, if the object belongs to a group of similar objects (prototypes) for which different projection points are known, reasonable extrapolation is possible and the correct projection can be presented for this object from the 2D projection alone. Humans are able to recognize faces rotated 20-300 from the frontal projection. Perhaps they are using information about the structure of the normal face. Another solution to this problem is to use 3D face models to support recognition in non-face

images. As R. Brunelli pointed out, it is possible to identify and solve problems such as working on an expert database related to obtaining other face projections using knowledge about the projections of other typical objects of this class.

Recognise face by using OpenCV library

First, let's learn how to recognize a face in a photo. First, you need to find where the person's face is in the picture and not confuse it with the clock on the wall and the cactus on the window. A simple task for a human may not seem so simple for a computer. To find a face, we need to select the main components such as nose, mouth, eyes, lips. For this we will use the templates shown in Fig. 1.

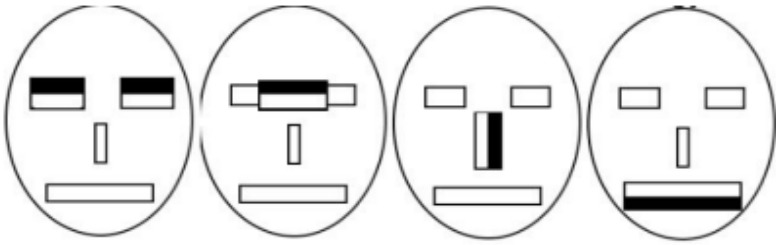


Fig. 1. Basic templates

Using of symbols of Haar. If the templates, if they are the first, match certain areas of the image, we assume that the image has a human face. For each of them, the difference between the brightness of the white and black areas is calculated. This value is compared to a standard and decides whether a part of the human face is present or not. This method is called the Viola-Jones method (also known as Haar cascades). Let's imagine that there are not only big faces in the picture, but also small ones. If we apply the templates to the whole image, we won't find the face there because it will be smaller than the templates. A sliding window method is used to search the entire image for faces of different sizes. It is in this window that the initials are counted. The window appears to slide across the entire image. As each image is passed, the window is enlarged to find larger-sized surfaces.

A face has been found in the photo, but it takes a few more steps to recognize a specific person. We will use the Local Binary Patterns algorithm to solve this problem. Its essence is that we divide the image into slices and compare each pixel in each slice with its 8 neighboring pixels. If the value of the central pixel is greater than its neighbor, we will write 0, otherwise we will write 1. So we will get a specific number for each pixel. In addition, based on these numbers, a histogram is calculated for all the segments that we have divided the image into. The histograms from all the slices are combined into a vector that characterizes the image as a whole. If we want to know how similar two faces are, we need to calculate and compare such a vector for each of them, the calculation of the vector is shown in Fig. 2.

5	8	1		1	1	0
3	4	6		0		1
7	1	3		1	0	0

Fig. 2. Calculation of LBP weight

The vector is written to line 11010001. Fig. 3 shows the face detection algorithm. The CascadePath parameter contains the name of the file with values ready to refer to. This file was downloaded from GitHub.

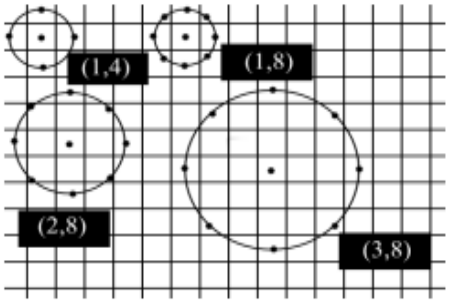


Fig. 3. LBP radius

The following parameters (8, 8) describe the dimensions of the areas shown in Fig. 5, into which we divide the faceted original image. The smaller it is, the more it will be and the better the detection will be.

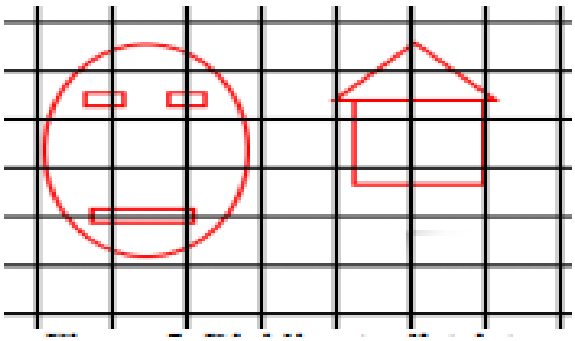


Fig. 4. Dividing to districts

Finally, the last value is the confidence threshold parameter, which defines the threshold value for face recognition. The lower the confidence, the more confident the algorithm is that the image shows a face it knows. When the threshold is low, the confidence means that the algorithm considers only this face as unfamiliar. In this case the threshold is 123.

References

1. Gromov Yu.Y., Didrikh I.V., Ivanova O.G., Ivanovskiy M.A., Odnolko V.G. Information technologies. Tambov. 2015.
2. Abramyan M. E. Electronic Handbook of Programming, Rostov-on-Don, 2005.
3. Abramov S. A., Gnezdilova G. F., Kapustina E. N., Selyug M. I. Programming tasks Vologda, 2000.
4. Shen A. Programming. Theorems and problems. Moscow, 2004.
5. Nikita Kultin "Fundamentals of programming in Delphi XE" St. Petersburg, 2011.

Information about the author

Hojamammedov M.M, teacher, the State Energy Institute of Turkmenistan, mekanhoja2021@gmail.com.

UDC 004.056.5

ZIPF'S LAW PLAYS AN IMPORTANT ROLE IN COPYWRITING

D. Hydyrova, A. Akadova
Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. Zipf's Law, a principle rooted in linguistics and statistical analysis, has profound implications for copywriting, offering insights into how language can be optimized for communication and persuasion. Named after the American linguist George Kingsley Zipf, this law states that in any given corpus of natural language, the frequency of a word is inversely proportional to its rank in the frequency table. In simpler terms, a small number of words are used very frequently, while the majority of words are used rarely. This phenomenon is not just a linguistic curiosity but a powerful tool for copywriters aiming to craft messages that resonate with their audience. By understanding and applying Zipf's Law, copywriters can create content that is both engaging and effective, ensuring that their message is easily understood and retained. The law's relevance to copywriting lies in its ability to highlight the importance of word choice, sentence structure, and overall readability, all of which are critical components of persuasive writing.

Keywords: Zipf's Law; Copywriting; Word Frequency; Linguistics; Power-law Distribution; Readability; Persuasive Writing; Headlines; SEO (Search Engine Optimization); Keyword Optimization.

Introduction

The foundation of Zipf's Law lies in the observation that language follows a predictable pattern, where the most common words – such as "the," "of," and "and"– dominate the text, while less common words appear sporadically. This distribution is not random but follows a power-law distribution, which has been observed in various languages and contexts. For copywriters, this means that the words they choose to emphasize or repeat can significantly impact how their message is perceived. By focusing on high-frequency words, copywriters can ensure that their content is accessible to a wide audience, as these words are more likely to be familiar and easily understood. At the same time, the strategic use of less common words can add depth and nuance to the message, making it more memorable and impactful. This balance between simplicity and sophistication is key to effective copywriting, and Zipf's Law provides a framework for achieving it.

One of the most practical applications of Zipf's Law in copywriting is in the creation of headlines and slogans. These elements are often the first point of contact between a brand and its audience, and their effectiveness can determine whether the message is noticed or ignored. According to Zipf's Law, headlines that incorporate high-frequency words are more likely to capture attention, as these words are processed more quickly and easily by the brain. For example, a headline like "The Best Way to Improve Your Health" is likely to be more effective than one that uses less common words, simply because it relies on familiar language that resonates with a broad audience. However, this does not mean that creativity should be sacrificed for the sake of simplicity. By combining high-frequency words with a unique or unexpected twist, copywriters can create headlines that are both attention-grabbing and memorable.

In addition to headlines, Zipf's Law can also inform the structure and flow of longer copy, such as blog posts, articles, and advertisements. Research has shown that readers tend to skim rather than read every word, especially in the digital age where attention spans are shorter than ever. By organizing content in a way that aligns with Zipf's Law, copywriters can ensure that their key messages are conveyed even to those who only glance at the text. This can be achieved by placing the most important information at the beginning of sentences and paragraphs, where it is more likely to be noticed. Similarly, the use of bullet points, subheadings, and other formatting techniques can help to break up the text and highlight key

points, making the content more digestible and easier to navigate. By leveraging the principles of Zipf's Law, copywriters can create content that is not only informative but also engaging and user-friendly.

Another area where Zipf's Law can be applied is in the optimization of keywords for search engine optimization (SEO). In the digital landscape, where visibility is often determined by search engine rankings, the strategic use of keywords is essential for driving traffic to a website. Zipf's Law suggests that the most effective keywords are those that strike a balance between popularity and specificity. While high-frequency words may attract a larger audience, they are also more competitive, making it harder to achieve a high ranking. On the other hand, low-frequency words may be easier to rank for, but they are less likely to generate significant traffic. By analyzing the frequency distribution of keywords in their niche, copywriters can identify the terms that offer the best combination of reach and relevance, ensuring that their content is both visible and valuable to their target audience.

The psychological underpinnings of Zipf's Law also offer valuable insights for copywriters. The law's emphasis on the relationship between word frequency and cognitive processing aligns with research in psychology, which has shown that familiar words are processed more quickly and with less effort than unfamiliar ones. This has important implications for the readability and persuasiveness of copy, as content that is easy to understand is more likely to be trusted and acted upon. By using high-frequency words and simple sentence structures, copywriters can reduce the cognitive load on their audience, making it easier for them to absorb and retain the message. At the same time, the occasional use of less common words can add variety and interest, preventing the content from becoming monotonous or predictable. This interplay between familiarity and novelty is a key aspect of effective communication, and Zipf's Law provides a scientific basis for achieving it.

Moreover, Zipf's Law can be extended beyond individual words to phrases and concepts, offering additional opportunities for optimization. For example, in the context of branding, the repetition of key phrases or slogans can help to reinforce brand identity and increase recognition. This is because repetition enhances memory retention, making it more likely that the audience will remember the brand and its message. Similarly, in the context of storytelling, the use of recurring themes or motifs can create a sense of cohesion and continuity, making the narrative more engaging and impactful. By applying the principles of Zipf's Law to these broader elements of copywriting, writers can create content that is not only effective in the short term but also memorable in the long term.

While Zipf's Law provides a useful framework for copywriting, it is important to recognize its limitations. The law is based on statistical patterns observed in natural language, and its applicability may vary depending on the context and audience. For example, in technical or specialized fields, the use of low-frequency words may be necessary to convey precise meaning, even if it reduces readability. Similarly, in creative writing, the deliberate use of unconventional language can add depth and originality, even if it deviates from the principles of Zipf's Law. Ultimately, the key to effective copywriting lies in understanding the needs and preferences of the target audience, and using the principles of Zipf's Law as a guide rather than a rigid rule.

In conclusion, Zipf's Law offers valuable insights for copywriters seeking to optimize their content for readability, engagement, and persuasiveness. By understanding the relationship between word frequency and cognitive processing, writers can craft messages that are both accessible and impactful, ensuring that their content resonates with their audience. Whether applied to headlines, SEO, or storytelling, the principles of Zipf's Law provide a scientific basis for effective communication, helping writers to strike the right balance between simplicity and sophistication. While the law is not a one-size-fits-all solution, its application can enhance the

effectiveness of copywriting in a wide range of contexts, making it a valuable tool for anyone seeking to master the art of persuasion through language.

References

1. Ferrer-i-Cancho, R., & Solé, R. V. "Least effort and the origins of scaling in human language." Proceedings of the National Academy of Sciences (2003), 100(3), 788-791.
2. Miller, G. A. "Some effects of intermittent silence." American Journal of Psychology (1957), 70(2), 311–314.
3. Mandelbrot, B. "An informational theory of the statistical structure of language." Communication Theory (1953), 84, 486-502.
4. Piantadosi, S. T. "Zipf's word frequency law in natural language: A critical review and future directions." Psychonomic Bulletin & Review (2014), 21(5), 1112-1130.
5. Zipf, G. K. Human Behavior and the Principle of Least Effort: An Introduction to Human Ecology. Addison-Wesley (1949), (in English).

Information about the authors

Hydyrova D., Senior lecturer of Department of Foreign Languages for Technical Fields Oguz han Engineering and Technology University of Turkmenistan, dunya.haytyeva@gmail.com.
Akadova A., 2nd year student of Computational Linguistics Oguz han Engineering and Technology University of Turkmenistan, akpamykakadova295@gmail.com

UDC 004

DEPLOYING CLOUD, FOG AND EDGE TECHNOLOGIES IN A SMART CITY INFRASTRUCTURE: A COMPREHENSIVE ANALYSIS OF FUNCTIONAL ROLES AND SECURITY ASPECTS

A. Klychev, I. Tagangylyjov
Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. The article provides a detailed analysis of the implementation of cloud, fog and edge computing technologies within the framework of the smart city infrastructure. Cloud computing offers extensive storage and computational scalability; edge computing minimizes latency by processing data at or near the data source; and fog computing serves as an intermediate layer that enables localized, context-aware processing with enhanced reliability. The theoretical foundations of these technologies, their functional features, as well as the relationship with data processing systems that provide operational management of smart city services are considered. Particular attention is paid to assessing security threats associated with distributed architecture, and recommendations are being developed to improve the resilience of information systems.
Keywords: smart city; cloud computing; fog computing; edge computing; technology; security; data; processing; cyber; system.

Introduction

The development of the smart city concept requires the integration of modern information technologies for effective management of infrastructure, transport systems, utilities and urban security. Cloud, fog and edge computing are key components of this digital ecosystem, helping to reduce data latency, optimize resource utilization and improve decision-making. However, in parallel with the implementation of these technologies, the need to address information security issues increases, which becomes an important aspect in the context of cyber threats in the modern digital world.

Main Part

Theoretical bases of cloud, fog and edge technologies. Cloud technologies provide centralized storage, processing and analysis of large volumes of data, which allows

for scalable computing processes. Benefits include the ability to flexibly allocate resources, centralized service management, and a high level of integration with analytical tools. Fog technologies act as an intermediary between cloud services and end devices. They allow data to be preprocessed directly near the source of its origin, which significantly reduces delays and increases the efficiency of distributed systems.

Edge computing is focused on performing analytical and computational tasks directly at the edge of the network. This ensures minimal system response time, reduces the load on central cloud platforms and allows you to quickly respond to changes in real time.

In the context of a smart city, these technologies are used to implement monitoring systems, traffic flow management, environmental control and security. Cloud computing provides analytics base and supports strategic decisions, while fog and edge technologies are responsible the real-time processing needed to implement mission-critical services such as emergency response systems and intelligent traffic management. The Table shows the application areas of these technologies in smart cities, their flexibility, using areas, security, and potential risks.

Table 1. Comparison technologies in smart cities

Feature	Cloud Computing	Fog Computing	Edge Computing
Processing Location	Centralized date centers (local or remote data centers)	Local nodes near data sources (another words between edge and cloud)	Directly on devices/ sensors (or near IoT devices)
Latency	High (due to long data transfer)	Low (closer to devices, but not real-time)	Very low (real-time decisions)
Bandwidth Usage	High (due to sending data to the cloud)	Moderate (less data sent to the cloud)	Low (Local processing)
Scalability	High (easily handles large data volumes)	Moderate (limited by local resources)	Low (limited by the edge device's resources)
Security	Dependent on the cloud provider's protocols	Enhanced (data can be processed locally)	High (minimal data transfer)
Security Risk	Centralized risk	Distributed risk	Device-level risk
Use case	City-wide analytics, big data processing	Real-time IoT applications (e.g., traffic)	Immediate local decisions (e.g., smart sensors)

The integration of distributed computing architectures is associated with a number of issues in the field of information security.

1. Centralized cloud computing threats. Centralized data storage and processing in the cloud attracts the attention of attackers, which can lead to denial of service attacks, data leaks and unauthorized access. Implementing strong encryption and authentication methods is critical.

2. Fog computing vulnerabilities. Fog nodes located at the edge of the network often have reduced security, making them vulnerable to man-in-the-middle attacks and other types of interference. Control over access to data and the implementation of local protection measures are necessary.

3. The risks of edge computing. Devices operating within edge computing may have limited resources to implement comprehensive security measures. This creates potential opportunities for exploiting vulnerabilities, which can negatively affect the overall security of the system.

An integrated computing architecture that combines cloud, edge, and fog computing can effectively balance the trade-offs between latency, processing power, and scalability.

1. Hybrid Models. Critical, time-sensitive applications can be handled at the edge or fog level, while computationally intensive tasks that are less sensitive to latency can be offloaded to the cloud.

2. Orchestration and Resource Allocation. Advanced orchestration frameworks (e.g., Kubernetes-based systems) are being developed to coordinate tasks across these layers, ensuring optimal resource utilization and quality of service.

3. Data Management and Analytics. The integration enables a multi-tiered approach where data is pre-processed at the edge, aggregated and analyzed in the fog, and stored or subjected to deep learning in the cloud.

Such a cohesive framework not only improves responsiveness and reduces network congestion but also enhances fault tolerance and system resilience in dynamic urban environments. Smart city networks must ensure robust security and privacy mechanisms across all computing layers. Challenges include.

1. Data Confidentiality and Integrity. Distributed processing increases the attack surface; thus, encryption, secure authentication, and anomaly detection must be integrated at both the fog and edge levels.

2. Access Control. Fine-grained access policies are needed to manage the diverse set of devices and users interacting with the network.

3. Trust Management. Ensuring the integrity and reliability of data processed at distributed nodes, especially when sensitive information (e.g., healthcare data or public safety alerts) is involved.

The development of standardized frameworks and protocols is crucial to address these security concerns while maintaining system performance. To improve the sustainability of smart city infrastructure, it is recommended.

1. Implementation of multi-level security systems, including complex mechanisms for encryption, authentication and access control.

2. Organization of continuous monitoring of network traffic and prompt response to cyber incidents.

3. Developing security standards for Internet of Things (IoT) devices taking into account the specifics of working in edge computing conditions.

4. Conducting regular audits and testing aimed at identifying and eliminating vulnerabilities in the distributed architecture.

Conclusion

The integration of cloud, edge, and fog computing is central to the development of smart city networks that require low latency, high scalability, and robust security. At the same time, the distributed nature of these systems creates significant security challenges that require the development of comprehensive protective measures. While cloud computing provides the necessary computational power and storage, edge and fog computing address the challenges of latency and localized data processing. Future research should focus on optimizing the interaction of computing platforms, improving security mechanisms, advanced orchestration techniques, unified security frameworks, and dynamic resource allocation strategies to further improve the performance and reliability of smart city infrastructures. Addressing these challenges will enable smarter, more resilient urban environments that can effectively meet the needs of growing populations and evolving technological demands.

References

1. Stojmenovic, I., & Wen, S. The fog computing paradigm: Scenarios and security issues. In 2014 Federated Conference on Computer Science and Information Systems (2014), 1–8.

2. Chiang, M., & Zhang, T. Fog computing for IoT: Security and privacy challenges. In R. Buyya & A.V. Dastjerdi (Eds.), Internet of Things: Principles and Paradigms (Morgan Kaufmann, 2016), 169–186.

3. Yi, S., Hao, Z., Qin, Z., & Li, Q. Fog computing: Platform and applications. In 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb) (2015), 73–78.

Information about the authors

Klychev A., senior lecturer, Oguz Han Engineering and Technology University of Turkmenistan, annamyrat.gylyjov@etut.edu.tm.

Tagangylyjov I., lecturer, Oguz Han Engineering and Technology University of Turkmenistan, i.tagangylyjow@gmail.com, i.tagangylyjov@etut.edu.tm.

UDC 004.056

WEB APPLICATION VULNERABILITY TESTING FRAMEWORK

K.N. Kondo, N. Nasonova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The increasing prevalence of cyberattacks targeting web applications necessitates advanced vulnerability detection techniques. Traditional methods such as Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) face challenges including high false positives, limited coverage of modern architectures (e.g., serverless, microservices), and inefficiency in identifying zero-day vulnerabilities. This paper proposes a hybrid vulnerability testing framework that combines SAST, DAST, and Machine Learning (ML) to enhance detection accuracy and adaptability. The technique integrates static code analysis for identifying insecure coding patterns, dynamic runtime monitoring to detect exploitation attempts, and an ML classifier trained on anomaly datasets to reduce false alarms.
Keywords: SAST; DAST, IAST, Machine learning.

Introduction

With the growth of web applications, there has also been an increase in cyber threats. This has created a need for effective vulnerability testing methods that can find and fix security weaknesses. However, despite improvements in testing techniques, existing methods still have limitations in their coverage and effectiveness. This can make it difficult for organizations to protect their digital assets from evolving cyber threats.

The current problem with vulnerability testing techniques is that they do not adequately address the complex nature of web application vulnerabilities and do not provide practical insights for practitioners. Research has shown that traditional methods of finding vulnerabilities, such as Static Application Security Testing and Dynamic Application Security Testing, have limitations such as high rates of false positives, limited coverage of new threats like API vulnerabilities, and inefficiency in complex systems like microservices.

The vulnerabilities in web applications represent a significant risk, as they can lead to unauthorized data access, financial loss, and reputational damage for businesses and users alike [1, 2]. Consequently, understanding and implementing effective vulnerability testing techniques has emerged as a critical aspect of web security, aiming to bolster defenses against potential exploits [3]. This article addresses the need for a robust, adaptive vulnerability testing technique that minimizes false positives, enhances detection accuracy, and adapts to modern web application architectures.

Main Part

The primary aim of this research is to design and evaluate a hybrid vulnerability testing technique that integrates static, dynamic, and machine learning-driven analysis to improve the detection of security flaws in web applications. Specific objectives include:

1. Analyze limitations of existing SAST, DAST, and Interactive Application Security Testing (IAST) tools in detecting vulnerabilities in modern web architectures.

2. Develop a hybrid testing framework combining static code analysis, runtime behavior monitoring, and machine learning (ML) to reduce false positives and identify zero-day vulnerabilities.

3. Validate the technique against benchmark datasets (e.g., OWASP Benchmark [4]) and real-world applications to measure precision, recall, and scalability.

As researches in this area show, the use of SAST tools achieves 78 % accuracy in detecting SQL injection flaws but struggles with runtime vulnerabilities, while DAST identifies 65 % of cross-site scripting (XSS) issues but generates 30% false positives [5]. A hybrid SAST-DAST approach improves detection rates by 15% but lacks adaptability to serverless environments [6]. A Convolutional Neural Network (CNN) is capable to classify SQL injection patterns with 92% accuracy in controlled environments, however, it performed poorly on encrypted data [7]. In [8] the authors showed, that IAST tools reduced false positives by 40% but required manual configuration. While progress has been made in analyzing current testing techniques and frameworks such as black-box, white-box, and gray-box testing, no unified framework addresses the interplay of these techniques for modern web applications hence gaps remain in integrating these methods into a cohesive strategy that maximizes their strengths. The proposed framework involves four phases given below.

Table 1. Web application vulnerability testing framework

Phase 1: Tool Analysis and Requirement Gathering	1.1 Comparative Study: Evaluate leading tools (e.g., SonarQube for SAST, OWASP ZAP for DAST) using the OWASP Top 10 2021 vulnerabilities as a baseline. 1.2 Gap Identification: Conduct penetration testing on open-source web apps (e.g., WebGoat) to catalog undetected vulnerabilities.
Phase 2: Hybrid Framework Design	2.1 Static Analysis Module: Integrate pattern-matching algorithms with semantic analysis to identify hard-coded credentials and insecure dependencies. 2.2 Dynamic Analysis Module: Deploy a headless browser (e.g., Puppeteer) to simulate user interactions and detect XSS and CSRF flaws. 2.3 ML-Driven Classification: Train a recurrent neural network (RNN) on the CICIDS2017 dataset [9] to classify anomalous HTTP requests and reduce false positives.
Phase 3: Implementation and Validation	3.1 Testing Environment Deployment: test the framework in testing production environment with vulnerable web-applications. 3.2 Benchmark Testing: Compare the framework's performance against OWASP Benchmark and other tools (e.g., Burp Suite) using metrics.
Phase 4: Real-World Deployment with Ethical Considerations	4.1 Real-World Deployment: test the framework in real production environment with web-applications. 4.2 Ensure compliance with ethical hacking standards by obtaining explicit consent for testing production systems. Anonymize sensitive data collected during dynamic analysis.

Conclusion

The proposed hybrid vulnerability testing framework combines SAST, DAST, and ML advantages to enhance web-applications vulnerabilities detection accuracy and adaptability. The technique involves static code analysis for identifying insecure coding patterns, dynamic runtime monitoring to detect exploitation attempts, and an ML classifier trained on anomaly datasets to reduce false alarms.

References

1. Singhal K., Azizi S., Tu T., Mahdavi S. S., Wei J., Chung H. W., et al. (2023) Large language models encode clinical knowledge. Nature. 620, 172–180. https://doi.org/10.1038/s41586-023-06291-2

2. Hassija V., Chamola V., Mahapatra A., Singal A., Goel D., Huang K., et al. (2023) Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. Cognitive Computation. 16, 45–74. https://doi.org/10.1007/s12559-023-10179-8

3. Díaz-Rodríguez N., Del Ser J., Coeckelbergh M., López de Prado M., Herrera-Viedma E., Herrera F. (2023) Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion. 99, 101896. https://doi.org/10.1016/j.inffus.2023.101896

4. OWASP Foundation. (2021). OWASP Benchmark Project. [Online]. Available: https://owasp.org/www-project-benchmark/

5. Johnson M., Patel R. (2021) A Comparative Study of SAST and DAST Tools. Journal of Cybersecurity. 8(2), 45–60.

6. Gupta A., Tyagi L. K., Mohamed A. (2023) A Machine Learning Methodology for Detecting SQL Injection Attacks. 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 184–191. https://doi.org/10.1109/ICTACS59847.2023.10390153

7. Tadhani J.R., Vekariya V., Sorathiya V., Alshathri S., El-Shafai W. (2024) Securing web applications against XSS and SQLi attacks using a novel deep learning approach. Scientific Reports. 14 (1), 1803. doi: 10.1038/s41598-023-48845-4. PMID: 38245563; PMCID: PMC10799887.

8. Olaes T. (2025) SAST, DAST, IAST. [Online]. Available at: SAST, DAST, IAST: Application Security (AppSec) Testing Tools | Balbix

9. CICIDS2017 Dataset. University of New Brunswick, 2021. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

Information about the authors

Kondo K.N., master student, Informations Security dept, Informations Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ntandolis431@gmail.com.

Nasonova N., Dr.of science, Assoc.prof., Professor, Infocommunications dept., Informations Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nasonovan@bsuir.by.

UDC 004.056.5

DEVELOPMENT OF AN ALGORITHMIC SYSTEM FOR DETECTING AND DISARMING THREATS BASED ON FUNCTIONING TABLES

[1] I.Kh. Normatov, [2] M. Atazhanov, [3] R. Karimov

[1,3]National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan
[2]Military Academic Lyceum named after Jaloladdin Manguberdi, Urgench, Khorezm

Abstract. The article provides an analysis of known existing systems designed to collect and automatically analyze events of various information in order to identify threats. Their disadvantages are given. An algorithmic model of information security based on tables of functioning is proposed as a mathematical tool for modeling dynamic discrete systems for detecting and neutralizing threats while ensuring information protection. A method for assessing information security risks and ensuring the confidentiality of information resources is given. The features of working with data flows, management and control over them are considered, mathematical solutions for assessing the protection of information resources and various aspects of assessing the economic effectiveness of ensuring the confidentiality of information resources are presented. One of the ways of analyzing the security of the system is proposed - the construction of dynamic tables of functioning. The description of the main functions and requirements of automatic threat detection and neutralization based on the tables of operation based on the functioning tables (FT) is considered.

Keywords: algorithm; mathematical; information and algorithmic models; information system; functioning table; threats; risks; detection; neutralization.

Introduction

The evolution of information technologies is associated with intelligent systems, which include processes of origin, adaptation and development. It is the systemic approach to IT that determines the methods and algorithms for building systems. The systemic approach to information security (IS) requires identifying its subjects, means and objects, principles of provision, sources of danger, and the direction of dangerous information flows.

The modeling principle allows avoiding errors in designing effective systems. When developing an effective system, the principle of communication comprehensively considers the object of protection, combining the external environment, means of protection and aggressive threats and taking into account the interrelations: source of threat – weakness – action – attack.

The development of a security system is the main condition for ensuring the security of confidential information in an information system, is formulated by studying the system requirements for the system and is aimed at neutralizing system vulnerabilities.

One of the methods of system security analysis is based on dynamic FT of the information system based on Petri nets [3-6]. Based on FT, the operability of the implemented security system is checked and its shortcomings are identified, i.e. with the help of FT, it is determined what actions occur in the system, what states were before these actions and what states the system takes after the action is completed.

Thus, the performance table calculates all risks that threaten the system and valuable information in the system.

Main part

One of the main methods of analyzing the security of systems is the construction of dynamic tables of the IS [1–6]. Algorithmic models based on FT [1, 2] represent a mathematical apparatus for protecting information systems from external and internal threats and are divided into several types:

– a general structural model of ensuring information system security based on FT;

– a mathematical model for identifying threats from external and internal sources;

– synthesis and analysis of the construction of the FT after receiving the necessary data at the "synthesis" stage;

– ways, methods, models and means of destroying detected threats;

– analysis of the information system and threats in the system.

Development of FT and flow chart of threats. The most convenient way to visually display actions in the system is to use a Petri net. The principle of operation and the state of the networkit is determined by itmarked graph anddistribution of chips by positions. The vertices of the graph are the network markings, the arcs are defined by the transition symbol and are constructed for each active transition. Construction stops when there are no activated transitions on the graph or there are no markings. Let us assume that the graph of reachable markings is an automaton. For example, the trajectories in the Petri net are defined as follows (Fig. 1).

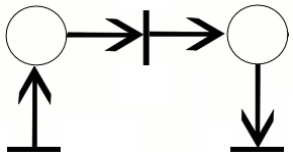


Fig. 1. Trajectory of Petri net movement

At each time interval $t_1 \in T$ the description of the FT is presented in the form of a labeled Petri net: $M = \{P, D, I, O, \mu\}$, where P – sets of positions (states), D – operations (transitions), I– input and O – output states, μ – a function that displays the set of positions in the set of natural numbers N those. $\mu : P \to N$. Each marking μ can be represented as a vector $\mu = (\mu_1, \mu_2, ..., \mu_n)$, where $n = |N|$ and $\forall \mu_i \in N$, $i = \overline{1,n}$. Vector μ defines for each position p_i, $i = \overline{1,n}$ network number of chips, i.e. $\mu(p_i) = \mu_i$, $i = \overline{1,n}$.

The designed FT visually displays all identified threats in the system we protect. After identification by the Petri net graph, all threats move vertically downwards only if it is a threat of the same type. In the example of the following type. The Petri graph goes through such an action due to the uniformity of the threat. Because each O_j – this is one of the types of threats in the GOST "Information technologies, information security, terms and definitions". All of the information security management threats, risks, attacks, methods and means of information protection, protection of sensitive information, information security of telecommunications and mobile networks, data protection and recovery, copy protection and others listed in this information security management standard are distributed in the FT according to their characteristics and the logical actions they perform (Fig. 2).

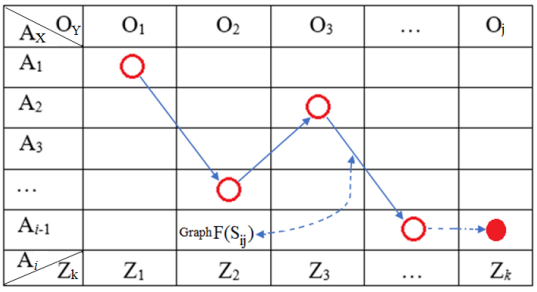


Fig. 2. Functioning table

If the machines are unable to process and destroy threats, then the task is passed on to another machine below. If the threat is combined, then the graph's actions take on a completely different form.

Let's consider the first case, that is, the threat *AB*, which comes from the Internet and consists of two separate parts *A* and *B* (where *A* – utility, driver, image, simple file, etc., *B* – background threat hidden in *A*). In this case, the threat will be pre-processed, blocked and removed before it can cause damage to the system. *A* after the user takes the link to *AB* on the Internet and launch *AB* in the FT network the link will be divided into two parts: *A* and *B* (Fig. 3).

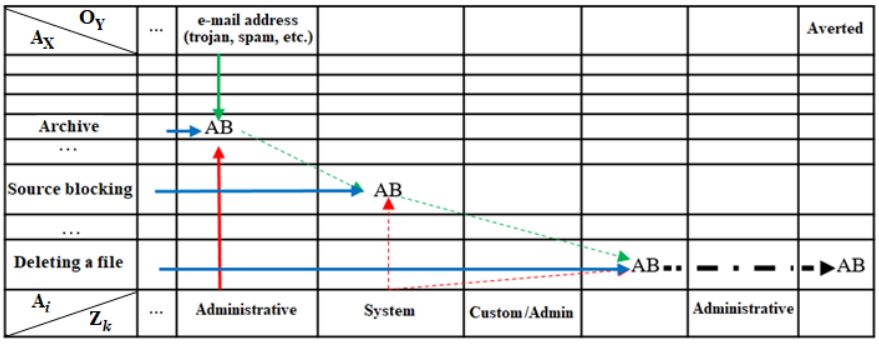


Fig. 3. The first case of the functioning table

In the second case, the threat is considered for the first time, and each of its passages is designated separately. O_Y the row of tables of cases 1 and 2 contains potential threats to the system. In table of cases 2, the paths of threats are shown in red, the prevention of threats is shown in green, and the transition of existing threats to another cell and their prevention is shown in black (Fig. 4).

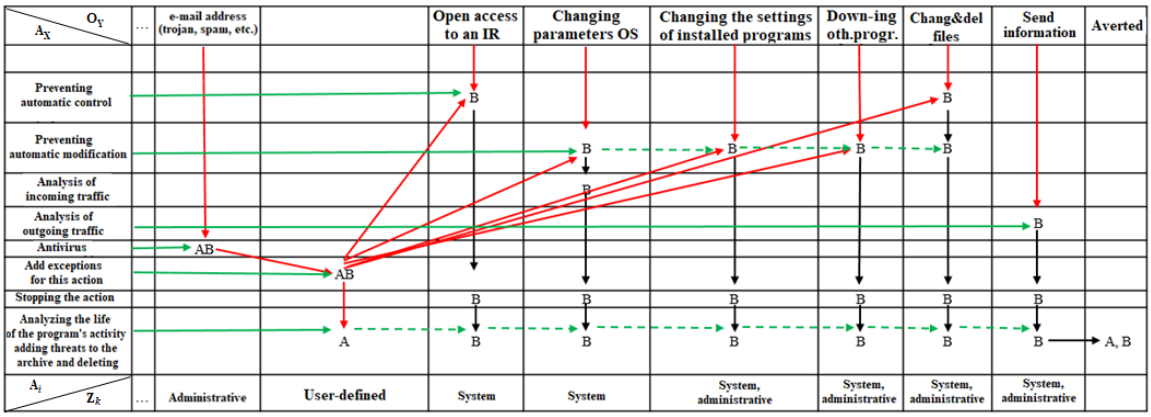


Fig. 4. The second case of the functioning table

The second part can run malicious parts of its program and download other malicious programs without the administrator's permission.

The transition process is calculated as follows. There are 127 threat defenses in the table vertically. If the penetrating threat is a combined one, then it is checked in each cell. To calculate a more effective transition to destroy threats, we have the formula: $P = \sum_{i=1}^{\infty} U_i$, where U – threat, P – transitions by FT. Let A – means of protection against threats, K – class of threats. Then $U = 1$, $P_{\max} = 127$ and when $U = 2$, $P_{\max} = 254$. So $P_{\max} = U * A$.

If the class of threats is defined and the ways of destroying the threat are also clear according to the class, then the formula will be as follows: $P_{\max i} = U(A-(A-K_i))$, $i = \overline{1,9}$. If one of the classes of threats is not defined, then it is equal to zero.

Since threats penetrate in a variety of ways, it is impossible to use one or several of them to calculate an effective way to eliminate threats. It is necessary to use all means of protection against threats. So, transitions along the FT are equal to $P = \sum_{i=1}^{9} P_{\max i}$.

If the penetrating threat is not combined then the maximum processing cell will be calculated vertically by reading the lines, and the minimum will be equal to one.

Conclusion

Thus, in the work, various information events collected for the purpose of identifying threats and their automatic analysis allow developing an effective program for identifying and neutralizing threats to information security. The proposed algorithmic model of information security based on the tables of functioning serves as a mathematical apparatus for modeling dynamic discrete systems for identifying and neutralizing threats when ensuring information security. After the software is launched, threats are launched simultaneously with it, as a result of which the proposed system begins to combat these threats. In most cases, this conflict has the form of an asterisk, and the reason for its distribution in this form is that the conditions for the penetration of a threat in the form of a set are accepted here. The tables of

functioning represent an algorithmic model of an automated control system for ensuring the security of information systems, as well as preventing any threats to information systems and information resources.

References

1. Glushkov V.M. Introduction to ACS. Kyiv: Tekhnika, 1972.
2. Zhuravlev Yu.I. Discrete Mathematics and Mathematical Questions of Cybernetics, M.: Nauka, 1974.
3. Peterson J. Petri net theory and systems modeling. Moscow: Mir, 1984.
4. Marchenkov A.E. Systems approach in research of management of innovative activity of integrated structures // Problems of Radio Electronics" EVT series, 2012, iss. 2, 189–196.
5. Normatov I.Kh., Toshmatov S., Yarashov I. Research and modeling of authentication process using functioning table // Journal of Mathematics, Mechanics and Computer Science, 124 (4), 71–85.
6. Normatov I. Endless individual areas of logic and beginnings of arithmetics // Modern problems of applied mathematics and information technology, 2023, 020008.
7. Normatov I., Yarashov I., Otakhonov A., Ergashev B. Construction of reliable well distribution functions based on the principle of invariance for convenient user access control // 2022 International Conference on Information Science and Communications Technologies, ICISCT 2022.
8. Normatov I.Kh., Ibadullaev D., Tangriberdiev O. Algorithm for constructing a non-degenerated quadratic stochastic operator by binomial distributions // Materials of 8th International conference "Actual problems of applied mathematics and information technologies", 2023, 133–135.
9. Normatov I., Yarashov I., Toshmatov S. Research and modeling of authentication process using functioning table // KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 2024, 124(4), 71–85.

Information about the authors

Normatov I.Kh., Doctor of Physical and Mathematical Sciences, Professor, Director of the Scientific and Innovation Center "Digital Technologies and Cybersecurity" named after Academician V.K. Kabulov at the National University of Uzbekistan named after Mirzo Ulugbek, i_normatov@nuu.uz.
Atazhonov M.N., Teacher of the Military Academic Lyceum named after Jalaluddin Manguberdi, muzaffar19910627@gmail.com.
Karimov R., Basic doctoral student of the National university of Uzbekistan named after Mirzo Ulugbek, karimov_r@nuu.uz.

UDC 004.056

FACE TRACKING WITH AUTOMATIC AGE AND GENDER DETECTION

M.H. Nurlyyeva, J.Sh. Sharipova, N.B. Akiyev
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Annotation. This article examines face recognition technology with automatic age and gender detection. It describes the main algorithms and methods used in this field, including machine learning and computer vision. Particular attention is given to practical applications such as video surveillance systems, marketing, and data analysis for social statistics. The advantages, limitations, and development prospects of this technology are analyzed.
Keywords: face recognition; automatic age detection; gender detection; machine learning; deep neural networks.

Introduction

Modern face recognition technologies are at the peak of development, offering a wide range of possibilities for analyzing visual data. One of the key tasks in this field is the automatic determination of age and gender, which opens new horizons in personalized services, marketing, and security.

The aim of this article is to explore the fundamental principles and methods underlying face tracking technology with age and gender detection, as well as to examine its practical applications.

The article will address the following aspects:

Fundamental algorithms for face recognition and classification of age and gender characteristics;

Technologies used to implement such systems, including machine learning and libraries like OpenCV, TensorFlow, and others;

Practical significance and challenges associated with applying this technology in real-world conditions.

The development of face recognition technologies raises important societal questions about data privacy and ethical considerations. This article will also focus on these issues, as well as the prospects for the future development of this field.

Main Part

Face recognition technology is based on image analysis and the identification of unique human facial features. This process involves several stages: detecting a face in an image, extracting its features (key points such as eyes, nose, and mouth), and comparing them with reference data. Machine learning algorithms, particularly deep neural networks (DNN), play a pivotal role, enabling systems to learn from large datasets and improve recognition accuracy.

Once a face is detected, the system proceeds to classify its age and gender. The following methods are employed.

1. Deep Neural Networks (Deep Learning): These analyze facial features to identify age-related changes (e.g., wrinkles, facial contours) and gender-specific traits.

2. Regression Methods: Used for age estimation, producing a continuous output (e.g., years).

3. Classification Models: Categorize age into groups (e.g., children, adults, elderly) and determine gender (male/female).

The algorithm examples are the following.

1. Convolutional Neural Networks (CNN) extract facial features using convolutional layers. They are widely used for their high accuracy in image processing tasks.

2. OpenCV is an open-source library offering tools for face detection (e.g., Haar Cascade algorithm), image processing, and data analysis.

3. Dlib is another popular library providing precise face detection and tracking. It includes pre-trained models for age and gender estimation.

These technologies are already widely applied in marketing, analytics, and security. However, ongoing development aims to achieve even greater accuracy and versatility, making face recognition systems increasingly effective for various real-world scenarios.

To implement a face tracking system with age and gender detection, the following tools are recommended:

1. Python: the primary programming language due to its simplicity and the abundance of ready-made libraries.

2. OpenCV: a library for working with images and videos, used for face detection.

3. Dlib: a library with powerful algorithms for facial processing and analysis.

4. TensorFlow/Keras: platforms for building and training neural networks, ideal for age and gender detection.

5. Pretrained Models: models like AgeNet and GenderNet simplify system deployment by providing pre-trained capabilities for age and gender classification.

System setup process is the following.

1. Face Detection. Use OpenCV to detect faces in an image. This can be achieved with:

– Haar Cascade Algorithm: a traditional method for detecting objects in an image;

– HOG (Histogram of Oriented Gradients): a feature descriptor that identifies facial regions based on gradients and edges.

2. Facial Feature Extraction. After detecting the face, extract its key features (e.g., eyes, mouth, contours). Dlib and similar tools are commonly used to perform this task efficiently.

3. Age and Gender Classification. Employ pre-trained models to classify the detected face by age and gender. These models process the facial image and return probabilities for each category:

– age: typically output as a continuous value or categorized into groups (e.g., child, adult, elderly);

– gender: predicted as a binary classification (male or female).

This approach ensures a structured pipeline that combines established tools and methods to achieve reliable age and gender detection.

Applications and prospects are the following.

1. Surveillance Systems. Face recognition technologies with age and gender detection are widely used in security systems. Cameras equipped with these algorithms can identify suspicious individuals and analyze visitor flows (e.g., in shopping malls).

2. Marketing and Retail. Companies leverage these technologies to analyze their target audience. For example, stores can gather data on the age and gender of visitors to better tailor their offerings and advertisements.

3. Social Research. These technologies assist in collecting demographic data about populations, which is valuable for urban planning or developing public programs.

4. Healthcare. In medicine, a patient's age and gender are sometimes used for preliminary assessments of health conditions or the risk of specific diseases.

The use of such technologies raises several ethical concerns.

1. Data Privacy: face recognition involves collecting and processing personal data, which can infringe on individuals' right to privacy if done without consent.

2. Risk of Discrimination: errors in classification or algorithmic bias can lead to incorrect conclusions or discrimination based on age or gender.

3. Regulatory Compliance: many countries regulate these technologies under data protection laws (e.g., GDPR in Europe).

4. Risk Mitigation Strategies: to address these challenges:

– implement strict data storage and processing standards;

– ensure algorithmic transparency and fairness;

– obtain informed consent from users;

These measures can help balance technological advancement with ethical considerations and ensure responsible use of face recognition systems.

Future prospects and technology enhancements are the following.

1. Improved algorithm accuracy. The development of more advanced deep learning models will help minimize errors in age and gender detection, leading to greater reliability and precision.

2. Integration with other systems. Combining face recognition with voice assistants or augmented reality (AR) systems will broaden the technology's application range, enabling seamless user experiences in various industries.

3. Energy-efficient solutions. Future technologies will be optimized for low-power devices, making them suitable for mobile and edge devices where energy efficiency is critical.

4. Ethical development. Active involvement of experts in creating standards and ethical guidelines will ensure the development of systems that respect user rights and privacy.

Face recognition with automatic age and gender detection continues to transform various sectors of life. However, its further advancement will require both technical innovation and legal frameworks to address emerging challenges responsibly.

Conclusion

Face recognition with automatic age and gender detection is an advanced technology that has already proven its effectiveness in various fields, such as security, marketing, and social research. In this study, we explored the key algorithms and tools behind this technology and analyzed its practical applications. Special attention was given to ethical concerns and future development prospects.

The technology has immense potential, but its use requires a balanced approach that combines technical capabilities with respect for human rights and privacy.

Recommendations and conclusions are the following.

1. For developers. The development of more accurate and resilient models should go hand in hand with the implementation of data protection methods. Using pre-trained models and libraries like TensorFlow and OpenCV can accelerate the technology's deployment.

2. For companies and organizations. Organizations using such systems must strictly comply with data protection laws. User consent and transparency regarding data processing should be standard practice.

3. For the academic community. Research into ethics and reducing algorithmic bias plays a crucial role in the continued development of this technology.

Face recognition technology with age and gender detection continues to transform our world, opening up new possibilities for personalization and data analysis. However, its implementation requires not only technical expertise but also a thoughtful approach aimed at creating a safe and ethical digital space.

References

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. 2016.
2. Szeliski R. Computer Vision: Algorithms and Applications. 2020.
3. Li J. Face Detection and Recognition: Theory and Practice. 2011.
4. Levi G., Hassner T. Age and Gender Classification using Convolutional Neural Networks. 2015.
5. Dlib Library for Face Recognition and Tracking. 2015.
6. General Data Protection Regulation. 2016.

Information about the authors

Nurlyyeva M., Teacher, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Sharipova J., Student, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Akiyev N., Student, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.

UDC 534.853.6

DEVICE FOR SPEECH-LIKE NOISE SYNTHESIS

[1]K.P. Shakin, [2]B.A. Samake, [2]E.A. Makarenya, [2]O.B. Zelmansky
[1]United Institute of Informatics Problems of the National Academy of Sciences of the Republic of Belarus, Minsk, Belarus
[2]Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The feasibility study of using active means of speech information protection with flexible configuration based on wireless connection is justified. Speechlike noise generating device based on wireless connection for speech information protection is proposed. It is proposed to form two masking speech-like

signals, one with a power equal to the power of the information signal and generated without taking into account the statistical features of the language, the second with significantly greater power and generated taking into account the statistical features of the language, which will increase the resistance of the protection to methods of statistical analysis and signal power analysis. A speech information protection device body modeled in the SolidWorks environment is proposed for subsequent 3D printing. PLA plastic was used in the printing process; a photo of the assembled speech information protection device is presented below in the text of the article. Testing of the developed device was carried out using the Salute Speech neural network.
Keywords: synthesis of speechlike noise; acoustic masking; information security; speech information protection; speech-like noise; white noise; neural network; allophones; confidentiality; simulations.

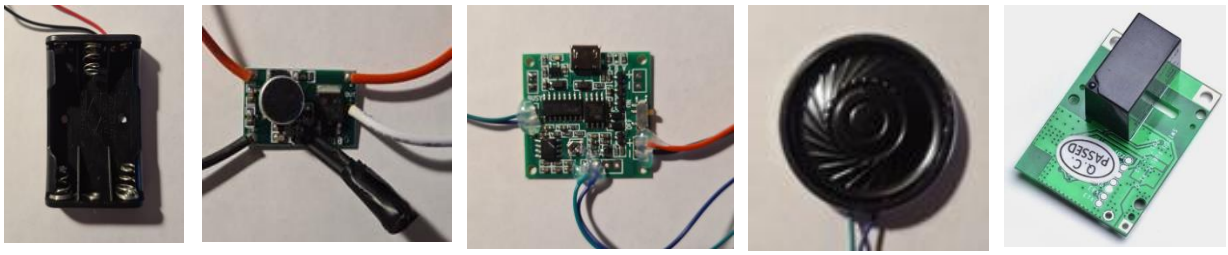
Introduction

At present there is an obvious need to protect speech information from leakage through acoustic and vibrational channels, because there is a significant amount of confidential information is transmitted through the speech, as the most natural form of the communication. It seems more practical and mobile to use active acoustic masking, which reduces "links" between signal and noise at the border of the controlled zone by increasing the noise level [1, 2]. White noise, pink noise, and uncorrelated speech-like interference are widely used as masking signals [3].

However, the interference signals used in modern systems of active protection of speech information do not provide the required level of protection, since they can be provided with the help of modern software that is publicly available on the Internet. In that way there is a proposal to form a masking acoustic signal directly from the hidden signal, which cannot be compensated. The article proposes a device for the formation of speech-like noise, consisting of elements of hidden speech mixed with white noise.

Construction of a device for generating speech-like noise

The following electronic components were selected to build the device: battery compartment, microphone unit, microprocessor unit, acoustic emitter, WiFi module (Fig. 1).



a *b* *c* *d* *e*

Fig. 1. Electronic components of a speech–like noise generation device, a – battery compartment, b – microphone unit, c – microprocessor module, d – acoustic emitter, e – WiFi module

The battery compartment (Fig. 1, *a*) provides power to all components of the device. The microphone node (Fig. 1, *b*) is designed to detect speech and record the voices of speakers in order to form a base of allophones and start the process of synthesizing a speech-like signal. The microprocessor module (Fig. 1, *c*) performs direct synthesis of speech-like signals, storage of the allophone database. The acoustic emitter (Fig. 1, *d*) reproduces the synthesized speech-like signal. The WiFi module (Fig. 1, *d*) allows remote control of the speech information protection device via a smartphone or tablet. Modeling of the body of the speech information protection device was performed in the SolidWorks environment, for the purpose of subsequent 3D printing. Printing was carried out on an AnetA 6 3D printer. The 3D model of the device body is shown in Fig. 2.

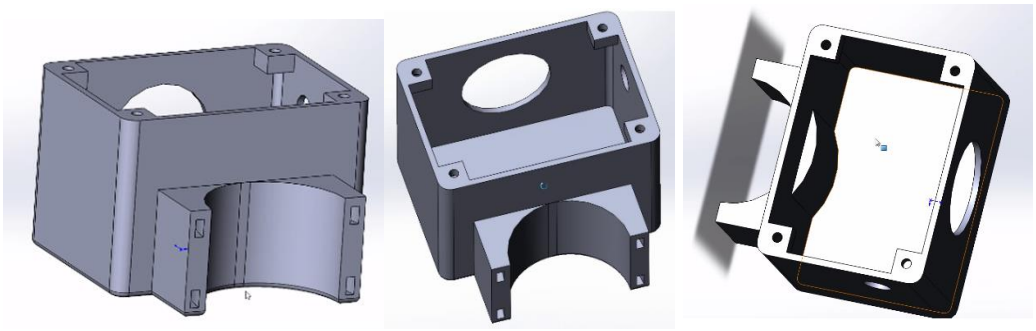


Fig. 2. 3D model of the housing of the speech information protection device

PLA plastic was used for printing a photo of the assembled speech information protection device is shown in Fig. 3.

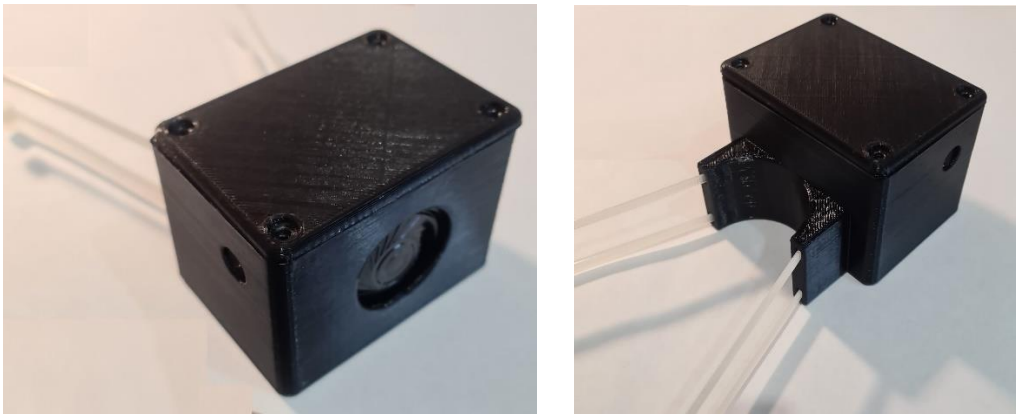


Fig. 3. Speech information protection device

The proposed device for the formation of speech-like noise [4, 5] allows you to form a speech-like interference from the voice of the speaker a direct participant in a confidential conversation, which does not carry any semantic information, and according to its statistical features fully corresponds to Russian speech. Since the level of this interference significantly exceeds the level of the hidden information signal, it is proposed to form an additional speech-like signal also from the speech of this speaker, the level of which will be equal to the level of the hidden signal, but without taking into account the statistical patterns of the language. As a result of mixing an informative signal with an additional speech-like signal, a violation of statistical patterns will occur, as a result of which the mixed signal can be classified as not carrying a semantic load. At the same time, a more powerful speech-like signal corresponding to statistical patterns can be classified as semantic. The signals generated in this way are mixed with white noise in a ratio of 3–15 dB.

Conclusion

A device for the formation of speech-like noise has been developed, implementing the proposed method for the formation of two speech-like interference of different levels directly from the hidden speech and their mixing with white noise. 3D modeling and 3D printing of the housing for the developed device has been carried out, allowing it to be mounted both on walls and pipes. The developed device was tested using the Salute Speech neural network. With a signal-to-noise ratio of 10 dB, the percentage of correctly recognized allophones was no more than 14 %. With a signal-to-noise ratio of 20 dB – 0 %. As a result, the high

efficiency of the generated interference was established in comparison with uncorrelated speech-like interference, as well as interference of the speech chorus type containing up to five voices.

References

1. Bogush R.P., Kurilovich A.V., Fundamentals of information security: teaching and methodological complex for students of the IPK specialty 1-40 01 73 "Software for information systems". Novopolotsk: PSU, 2009. 96 p.
2. Buzov G.A., Kalini S.V., Kondratyev A.V. Protection against information leakage via technical channels: Tutorial. Moscow, 2005.
3. Burlakov M.E., Osipov M.N. Acoustic and vibroacoustic channels of information leakage. Theoretical foundations and basic practical training. Samara, 2021.
4. Valiev E.A., Makarenya E.A. Device for protecting information from leakage via acoustic and vibration channels // Science and education in the modern world: challenges of the 21st century: materials of the XII International scientific and practical conference, Astana, February 10-15, 2023 / National movement "Bobek"; editorial board: E. Abiyev (editor-in-chief) [et al.]. Astana, 2023. P. 25–28.
5. Valiev E.A., Makarenya E.A.; applicant E.A. Valiev, E.A. Makarenya. Device for protecting information from leakage via acoustic and vibration channels: patent. 13220 Rep. Belarus, IPC H04K 3/00, G10L19/14. No. u 20230016; appl. 01/30/2023; publ. 04/17/2023 // Afitsyiny bulletin. 2023. No. 3(152). P. 103.

Information about the authors

Zelmansky O.B., Associate Professor, PhD, Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics".
Shakin K.P., master, head of sector, Research Institute for Technical Information Security.
Samake B.A., postgraduate student of the department of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus.
Makarenya E.A., student of the department of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus.

UDC 004.8:004.7

ARTIFICIAL INTELLIGENCE SECURING IN CYBERSPACE

H. Sudani
Ministry of Higher Education and Scientific Research, Baghdad, Iraq

Abstract. Artificial Intelligence (AI) has become pivotal in enhancing cybersecurity measures across various sectors. By leveraging advanced techniques such as machine learning, deep learning, and natural language processing, AI systems can analyze vast amounts of data in real time to identify patterns indicative of potential threats. This capability enables the proactive detection and mitigation of cyber threats, including sophisticated attacks like phishing and malware intrusions. As cyber threats continue to evolve in complexity and frequency, the role of AI in fortifying cybersecurity defenses becomes increasingly indispensable. Fortunately, Artificial Intelligence (AI) technologies have been introduced into cyberspace to construct smart models for defending systems from attacks. Since AI technologies can rapidly evolve to address complex situations, they can be used as fundamental tools in the field of cybersecurity. In this paper, we review the impact of AI on cybersecurity.
Keywords: Artificial Intelligence; cybersecurity; Cyberspace; Threat Detection; cyberattack; machine learning; deep learning; natural language processing; computer network.

Introduction

The exponential growth of computer networks has led to a tremendous growth in several cyberattacks. All sectors of our society, from government to economy, to critical infrastructures, are largely dependent on computer networks and information technology solutions. Therefore, they are vulnerable to cyberattacks. A cyberattack is an attack launched from one or more computers against other computers or networks. Typically, cyberattacks

aim to disable the target computer, take the services offline, or get access to the target computer's data [1]. Since the first denial-of-service attack in 1988, the number and impact of cyberattacks have increased remarkably. Indeed, cybersecurity has become one of the most challenging tasks in the computer science field; and it is expected that the number and sophistication of cyberattacks will grow continually and exponentially. The exponential growth of computer networks has led to a tremendous growth in number of cyberattacks.

According to the definition provided by Myriam Dunn Cavelty [2]. Cybersecurity has become one of the most important issues in cyberspace [3, 4]. AI-driven solutions can effectively prevent phishing attacks by analyzing and recognizing malicious patterns in emails and websites. Moreover, AI enhances the efficiency of cybersecurity operations by automating routine tasks, allowing security professionals to focus on more complex issues. However, integrating AI into cybersecurity also presents challenges, such as the need to address potential biases in AI algorithms and the importance of maintaining ethical standards.

The role of AI in the field of cybersecurity

The convergence of AI and cybersecurity awareness can revolutionize threat detection, bolster response capabilities, and enhance user training. By leveraging AI's capabilities, organizations can enhance their cybersecurity measures to keep pace with the evolving threat landscape and mitigate risks effectively.

AI works in three ways:

1. Assistive intelligence, which improves on what people already do
2. Augmented intelligence, which allows people to do things they could not otherwise do.
3. Autonomous intelligence, which is the feature of machines acting on their own.

Concerning these three categories, it can be concluded that AI is aimed at solving some of the most complex problems and cybersecurity falls into this category as cyberattacks have become very complex and potentially more catastrophic and have become a complex problem in cyberspace. AI can be used in various areas of cyberspace to analyze data to detect and respond to attacks. AI can also automate processes, which helps security analysts quickly work with semi-automated systems to identify cyberattacks.

Artificial Intelligence in Threat Detection. AI-based security systems can monitor network traffic and user behavior to detect unusual activity. These systems can identify threats such as malware, ransomware, and phishing attacks. Unlike traditional methods that rely on predefined signatures, AI can learn from previous incidents and identify new types of threats, Table 1 shows the role of AI in threat detection.

Table 1. AI-Powered Threat Detection

AI Technology	Description	Example Use
Machine Learning	Identifies patterns in data to detect anomalies	Detecting new forms of malware
Natural Language Processing	Analyzes text and communication for suspicious patterns	Identifying phishing emails
Deep Learning	Advanced learning from vast datasets	Predicting zero-day attacks

AI for Intrusion Detection Systems (IDS). Intrusion detection is another area where AI plays a major role. Using AI, security systems can detect when an unauthorized user attempts to access a network and respond in real-time. AI models are continuously trained based on previous intrusion data to improve their detection capabilities, as described in Table 2. ML classification algorithms use indicator datasets to identify different malware behaviors in the datasets and classify them [5].

Table 2: Comparison of Traditional vs. AI-Enhanced IDS Performance.

Metric	**Traditional IDS**	**AI-Based IDS**
Accuracy	Medium	High
Detection Speed	Slow	Fast
Adaptability	Low	High
Cost	Higher Maintenance	Lower long term cost

As cyber threats continue to evolve, the role of AI will become even more important. The next generation of AI-powered cybersecurity systems will likely include more autonomous decision-making processes, where AI can not only detect but also mitigate threats in real time without human intervention.

Conclusions

The rapid growth of cyber threats and the sophistication of cyberattacks require new, more robust, flexible, and scalable methods. In current research, the main targets of AI-based algorithms for cybersecurity are malware detection, network intrusion detection, and phishing and spam detection. Various researchers leveraged a combination of different AI techniques, such as ML/DL methods together with bioinspired computation, or different learning methods such as supervised learning together with reinforcement learning. Such combinations yield outstanding results. Although the role of AI in solving cyberspace issues is inevitable, some problems related to trust in AI and AI-based threats and attacks would be another concern in the cyber environment. AI must also be continuously monitored and updated to ensure it remains effective in the ever-changing cybersecurity landscape.

References

1. Josh Fruhlinger,"Whatiscyberattack?,".CSO, February 2020https://www.csoonline.com/article/3237324/whatis-a-cyber-attack-recent-examples-showdisturbing-trends.html.

2. Cavelty, Myriam Dunn, "The Routledge Handbook of New Security Studies". 154-162, 2018.

3. Guan ZT, Li J, Wu LF, et al., "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid". IEEE Internet Things J, 4(6): 1934-1944.

4. Wu J, Dong MX, Ota K, et al.,"Big data analysis-based secure cluster management for optimized control plane in software-defined networks,".IEEE Trans Netw Serv Manag, 15(1):27-38.

5. M. Rege, R. Blank, K. Mbah, "Machine learning for Cyber Defense and Attacks". The seventh international conference on data analytics, 2018.

Information about the authors

Sudani H., academic degree (Dr.Sci.(Eng)), academic rank(teacher), position (Head of the Department), Ministry of Higher Education and Scientific Research, info@mohesr.gov.iq.

UDC 004

CONTROLLING DATA SECURITY IN SOCIAL NETWORKS

I. Tagangylyjov, A. Klychev
Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan.

Abstract. In the digital era, social media platforms have become essential tools for communication, business, and social interaction. With over 4.5 billion active users globally, the security of personal data shared on these platforms has become a critical concern. This article explores the various aspects of data security in social media networks, focusing on the types of data involved, the potential risks and threats, and the technologies used to protect user information. It discusses the importance of encryption, blockchain, artificial intelligence, and biometric systems in safeguarding users' personal data. Additionally, the article examines the legal frameworks,

such as the General Data Protection Regulation (GDPR), and the ethical considerations necessary for maintaining privacy and security on these platforms. As the use of social media continues to grow, the integration of advanced technologies and the enforcement of strict privacy regulations are essential for ensuring the protection of users' data and privacy.
Keywords: Data Security; Social Media; Privacy Protection; Encryption; Blockchain Technology; Artificial Intelligence; Biometric Systems; Cybersecurity; GDPR; Data Privacy Regulations.

Introduction

Social media is now not only a platform for communication, but also a major means for business, public and social interactions. In 2025, more than 4.5 billion people use social media to share information, communicate, post and perform other actions. In such conditions, ensuring data security on social media becomes extremely important. Protecting users' personal data and their security requires the use of modern technologies and solutions aimed at protecting them.

Main Part

There are several issues and threats related to the security of social media data. To address these issues, it is important to have a deeper understanding of the types of data and their privacy. Social media data is not only the personal data of users, but also information that can affect public and economic interests.

Data in social networks can be of different types, each of which has its own security measures:

– Personal data: Name, surname, email, phone number, location and other personal data of users. This data indicates the identity of the user, and its protection is one of the most important tasks.

– Geolocation data: Information about the user's location or movements. Geolocation data shows where users are located. Incorrect use of this data may result in loss of privacy of personal data.

– Actions and behavior: Actions, posts, comments, reactions to photos and their social activity. This data can be useful both for the user and for society, but it requires protection from unwanted interference.

– Interaction data: Messages and conversations between users, as well as their posts and comments on platforms. This data is important because it reveals the interactions between users.

Social media data is open to various threats and users face risks related to their identity:

– Fake data and data sharing: Misuse or false use of data can result in people's personal data being misrepresented. For example, creating fake social media accounts to collect information can result in loss of privacy.

– Data theft (cyber attacks): Cyber attacks are one of the most common ways to steal personal data from social media users. In such attacks, the stolen data can be used to gain unauthorized access to user accounts.

– Loss of identity: In social media, a person's identity may be at risk. Users may lose their identity or privacy due to the dissemination of their personal data or wrong actions.

Various technologies and approaches are used to ensure data security in social networks. New technologies strengthen security measures and help protect user data.

Encryption is one of the most important technologies for protecting data on social networks. This method makes data accessible only to authorized users, protecting it from unauthorized use.

– Asymmetric encryption: Two keys (public and private) are used. The private key is stored only by the user, and encrypted data can only be decrypted using the public key.

– Symmetric encryption: One key is used, and the encrypted data is decrypted with the same key. It is a convenient and fast method for protecting data.

Blockchain provides decentralized storage of data in social networks. This technology prevents data from being changed or deleted, giving the user the ability to maintain control over their data.

– Decentralized data storage: IN In a blockchain, data is not stored in one place, but is distributed across several nodes, which reduces the risk of its loss or modification.

Artificial intelligence (AI) and machine learning help analyze user actions on social networks and identify suspicious activities.

– User Behavior Analysis: AI algorithms can detect abnormal user activity and warn of potential threats.

– Threat Prevention: AI technologies can alert you to potential risks in advance and help prevent them.

Biometrics plays an important role in enhancing social network security and user identification. It allows you to grant access to an account only to those users who have passed biometric verification.

– Facial recognition: Biometrics allows you to identify users by their face, limiting account access to authorized individuals only.

– Biometric systems based on fingerprints or other characteristics: Biometrics can be used to improve the security of user accounts.

Legislation and public norms play an important role in ensuring data security on social networks. Different countries adopt laws that help protect user privacy.

The mai laws is General Data Protection Regulation (GDPR). Europe has adopted the GDPR, which gives users full control over their personal data. This law requires social networks to take steps to ensure data security.

In order to ensure data security on social networks, it is important not only to use technology, but also to adhere to ethical standards and social principles. Adopting ethical standards and social norms helps to protect the privacy of users' data.

– Privacy and Public Responsibility: All social media users should have the right to protect their personal information and data, and the ability to control access to it.

Data Security in Social Networks:

– Social networks gather and share various types of data (personal information, posts, photos, geolocation data). This section would explain how this data should be kept confidential and who is responsible for securing it.

– Modern technologies to ensure data security on social networks, such as encryption (end-to-end encryption), and necessary tools to secure communication.

Emerging Solutions:

– Current security methods for keeping users' data private on social networks (masking, data encryption) and their integration with user preferences.

– The importance of new solutions like blockchain technology for ensuring data security on social networks.

Cyberattacks on Social Networks:

– Cyberattacks on social networks and their consequences (external attacks, the use of suspicious programs or phishing attacks).

– How data on social networks and the internet can be compromised, and what security measures need to be implemented to protect it.

Economic, Ethical, and Legal Aspects:

– The economic impact of data security on social networks: How this data creates value in the economy and the need for measures to ensure data quality and security.

– Ethical and legal issues: The protection of personal data in a legal and ethical way, and the importance of regulations that strengthen users privacy rights on social networks.

Intercommunication Systems and Specific Features:

– How communication systems can be improved to manage data security on social networks.

– Expanding the impact of privacy measures and cybersecurity regulations on user experiences in social networks and data security.

Diversity of Data Monitoring Systems:

– Different monitoring methods used to manage data security on social networks, including data analysis, algorithms, and advertisement security.

– Expanding the role of privacy measures in social networks that help users control the privacy level of their interactions.

Future Solutions:

– New solutions for data security in social networks (intelligent algorithms, multi-factor authentication).

– Ensuring the implementation of privacy regulations for various social services, forums, and websites to secure data.

Conclusion

To ensure data security in social networks, it is necessary to use various technologies, laws, ethical standards and public measures. A comprehensive approach using new technologies and solutions allows to protect the identity and data of users in social networks.

References

1. Cavoukian, A., & Dixon, D. (2018). "Privacy by Design: A Counterpoint to the Security-Privacy Debate." International Journal of Information Management, 38(1), 15-21.

2. Zhang, L., & Zhang, Y. (2020). "Data Security and Privacy in Social Media." Journal of Cybersecurity, 16(3), 45-63.

3. Liu, L., & Li, B. (2019). "Privacy Preservation in Social Networks: Techniques and Challenges." Journal of Information Security and Applications, 50, 125-136.

Information about the authors

Tagangylyjov I., Lecturer, Oguz Han Engineering and Technology University of Turkmenistan, i.tagangylyjow@gmail.com, i.tagangylyjov@etut.edu.tm.

Klychev A., Senior lecturer, Oguz Han Engineering and Technology University of Turkmenistan, annamyrat.gylyjov@etut.edu.tm.

UDC 004.056.5

CRYPTOGRAPHIC PRINCIPLES IN THE AGE OF ARTIFICIAL INTELLIGENCE

A. R. Taylyyeva

Oguz han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. Cryptographic information protection is paramount in today's digital age, safeguarding sensitive data from unauthorized access. This discipline employs algorithms to encrypt information, rendering it unintelligible without the correct decryption keys. Encryption ensures confidentiality, while cryptographic hash functions guarantee data integrity by detecting alterations. Secure authentication protocols, like Public Key Infrastructure (PKI), verify identities and prevent repudiation. Effective key management is crucial, encompassing secure key

generation, distribution, and storage. The strength of cryptographic systems relies on robust algorithms and diligent key handling. Ongoing research and development are essential to counter evolving cyber threats. As data breaches become more frequent, the application of strong cryptographic measures is vital for maintaining trust and security in digital interactions. This field is constantly adapting to new challenges, ensuring that sensitive information remains protected.
Keywords: Encryption; decryption; algorithms; keys; integrity; authentication; confidentiality; Public Key Infrastructure; hash functions; cybersecurity.

Introduction

In our modern world, computers and the internet are used for almost everything. We send emails, shop online, and store important documents digitally. All this information needs to be protected from people who might want to steal it or change it. That's where cryptographic information protection comes in. Imagine you have a secret message you want to send to a friend. You wouldn't want anyone else to read it, right? Cryptography is the process of converting between readable text, called plaintext, and an unreadable form, called ciphertext. This occurs as follows:

1. The sender converts the plaintext message to ciphertext. This part of the process is called encryption (sometimes encipherment).
2. The ciphertext is transmitted to the receiver.
3. The receiver converts the ciphertext message back to its plaintext form. This part of the process is called decryption (sometimes decipherment).

Main Part

Encryption: Turning Plain Text into Secret Code: The process of turning your message into a secret code is called encryption. You use an algorithm, which is like a set of rules, to scramble the letters of your message. Think of it as a special recipe that changes your message into something only you and your friend understand. To make the algorithm work, you need a key. A key is like a secret password. Without the key, the algorithm can't scramble or unscramble the message. There are different kinds of keys. Some keys are used for both encryption and decryption, while others come in pairs, a public key and a private key.

Decryption: Unscrambling the Secret Code: When your friend receives the encrypted message, they use the same algorithm and the correct key to turn it back into the original message. This is called decryption. It's like using the recipe in reverse to get back to the original message.

Algorithms: The Secret Recipes: Algorithms are the heart of cryptography. They are mathematical formulas that make encryption and decryption possible. Some common algorithms include AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman). These algorithms are very complex, and it's nearly impossible to break the code without the key.

Keys: The Secret Passwords: Keys are essential for keeping information secure. Without the right key, even the strongest algorithm is useless. There are two main types of keys:

– Symmetric keys: These keys are used for both encryption and decryption. Both the sender and receiver need to have the same key.

– Asymmetric keys: These keys come in pairs: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. The public key encrypts the message, and the private key decrypts it.

Integrity: Making Sure the Message Stays the Same: Integrity means making sure that the message hasn't been changed or tampered with during transmission. To check integrity,

we use hash functions. A hash function takes the message and creates a unique "fingerprint" called a hash. If the message is changed, even slightly, the hash will be different.

Hash Functions: Digital Fingerprints: Hash functions are one-way functions, meaning you can't get the original message back from the hash. They are used to verify that a file or message hasn't been altered.

Authentication: Proving You Are Who You Say You Are: Authentication is the process of verifying that someone is who they claim to be. This is important for preventing unauthorized access to systems and information. For example, when you log in to your email account, you need to provide your username and password, which are used to authenticate you.

Public Key Infrastructure (PKI): Public Key Infrastructure (PKI) is a system that helps manage and distribute public keys. It uses digital certificates to verify the identity of individuals and organizations. PKI helps to ensure that public keys are authentic and haven't been tampered with.

Confidentiality: Keeping Information Secret: Confidentiality is one of the main goals of cryptography. It means keeping information secret from unauthorized people. Encryption is the primary way to achieve confidentiality.

Cybersecurity: Protecting the Digital World: All these cryptographic techniques are part of a larger field called cybersecurity. Cybersecurity is about protecting computers, networks, and data from unauthorized access, damage, or theft. It includes everything from using strong passwords to implementing complex encryption systems.

Why Cryptographic Information Protection Matters

Cryptographic information protection is essential for many reasons:

– Protecting sensitive information: It keeps personal information, financial data, and business secrets safe.

– Ensuring secure communication: It allows people to communicate securely over the Internet.

– Maintaining trust: It helps to build trust in online transactions and services.

– Combating cybercrime: It makes it harder for criminals to steal or manipulate data.

Conclusion

Cryptographic information protection is a fundamental pillar of cybersecurity. By understanding the core concepts and applying appropriate techniques, organizations and individuals can safeguard their sensitive data from unauthorized access and ensure the integrity of their digital communications. As technology continues to advance, cryptography will remain a critical tool for protecting information in an increasingly interconnected world.

References

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier
2. Cryptography and Network Security: Principles and Practice" by William Stallings
3. Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.
4. NIST (National Institute of Standards and Technology) Publications
5. "Guidelines on cryptographic algorithms usage and key management" (2023) Published by the European Payments Council (EPC).

Information about the author

Taylyyeva A.R., Student, Oguz han Engineering and Technology University of Turkmenistan, taylyyewaaynur@gmail.com

UDC 004.896:004.852.4

ARCHITECTURAL FRAMEWORK OF A PROTOTYPE FOR ANOMALY DETECTION IN NETWORK TRAFFIC USING MACHINE LEARNING

X. Wang, A. Prudnik
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This paper presents a prototype application for detecting network traffic anomalies by integrating visual analytics and unsupervised machine learning. Built using a Flask-based three-tier architecture, the system employs the Isolation Forest algorithm for anomaly detection and provides interactive web-based visualizations to enhance human interpretation of complex traffic patterns. Key features include temporal traffic flow visualization, protocol distribution analysis, and anomaly severity classification. The prototype enables network administrators to identify sophisticated intrusions through real-time metrics and supports informed decision-making for threat mitigation.
Keywords: network traffic; anomaly detection; visual analytics; machine learning; web-based dashboard.

Introduction

Network security faces increasing challenges from sophisticated cyber attacks amidst exponential traffic growth. Traditional signature-based detection systems struggle to identify novel threats, necessitating advanced approaches like anomaly detection [1]. While machine learning offers enhanced detection capabilities, unsupervised methods often produce high false positives, and purely algorithmic systems lack interpretability for security practitioners [2, 3]. This research introduces a hybrid framework that combines unsupervised machine learning with visual analytics to address scalability and interpretability challenges. By leveraging the isolation forest algorithm and interactive visualizations, the prototype aims to empower network administrators to detect and contextualize anomalies effectively.

Main Part

The theoretical foundation of this prototype rests on integrating automated anomaly detection with human-centered visual analytics. Unsupervised machine learning, specifically the isolation forest algorithm, is chosen for its ability to identify statistical outliers in high-dimensional data without requiring labeled datasets [4]. This method constructs random binary trees to isolate anomalies, where outliers have shorter path lengths due to their distinct features. Complementing this, visual analytics facilitates human interpretation by transforming complex data into intuitive graphical representations, enabling analysts to contextualize anomalies within operational environments [5]. The theoretical design emphasizes a synergy between machine-driven detection and human-driven analysis to enhance overall system effectiveness in identifying network threats.

The prototype adopts a three-tier architecture comprising data acquisition, analysis, and presentation layers (Fig. 1). The data acquisition layer generates synthetic network traffic using a custom data generator module, producing records with attributes like timestamp, source/destination IPs, protocol, and byte counts for testing purposes. The analysis layer employs the isolation forest algorithm for anomaly detection, with data persistence handled by SQLite and SQLAlchemy ORM. The presentation layer uses a Flask web framework with a Bootstrap-based interface, rendering visualizations via Chart.js for temporal traffic, protocol distribution, and anomaly severity metrics.

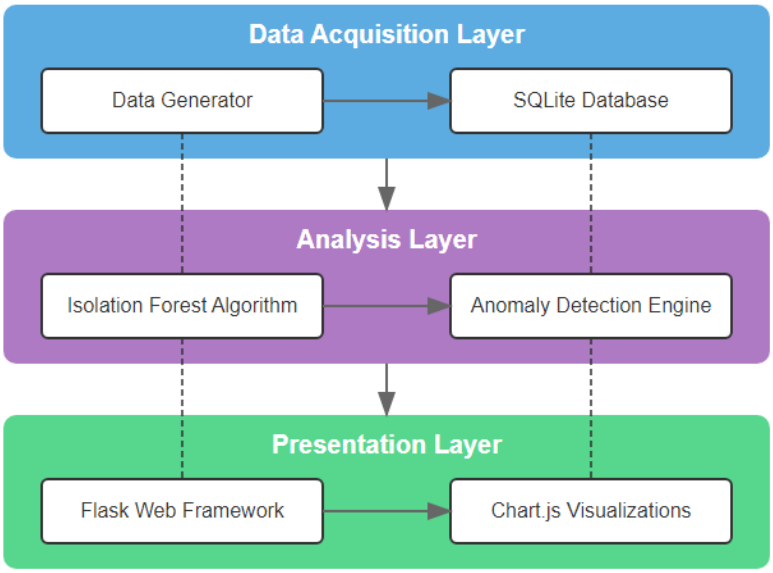


Fig. 1. Three-tier architecture of the network anomaly detection prototype

Components communicate through RESTful API endpoints, ensuring modularity and separation of concerns. Data flows sequentially: traffic records are generated, stored, analyzed in hourly batches, and visualized on-demand via API triggers. This design supports scalability and iterative development while maintaining computational efficiency.

The visual analytics framework transforms network traffic data into interactive visualizations using Chart.js, enhancing human interpretation for network administrators. Temporal traffic analysis is presented through line charts that display traffic volume over adjustable time periods ranging from one hour to seven days, enabling the identification of anomalies such as spikes associated with denial-of-service attacks (Fig. 2). Protocol distribution is visualized using doughnut charts that reveal protocol frequency distributions, facilitating the rapid detection of unusual patterns like tunneling or covert channels. Anomaly severity is depicted through pie charts that classify detected anomalies into critical, high, medium, and low severity levels–defined by thresholds of greater than 0.8, greater than 0.7, greater than 0.6, and 0.6 or below, respectively–using a color-coded scheme ranging from red for critical to blue for low severity, allowing for quick triage. Server-side processing with Flask ensures computational efficiency, while client-side Chart.js rendering provides a responsive user experience, though occasional API endpoint errors indicate a need for improved refresh mechanisms.

The anomaly detection module uses scikit-learn's IsolationForest with 100 estimators and a contamination factor of 0.05, optimized for enterprise network environments [6]. Features include bytes transferred, packet counts, connection duration, and port numbers, normalized via StandardScaler to address scale disparities. The algorithm computes anomaly scores based on path lengths in binary trees, transformed to a $[0, 1]$ range for severity classification.

Processing occurs in one-hour windows to balance efficiency and context, achieving $O(n \log \underline{n})$ time complexity with a theoretical potential to handle approximately 10^5 records per minute on standard hardware. This throughput potential is derived from the algorithmic efficiency of the isolation forest, though the current implementation generates smaller data batches. Memory usage scales linearly with data volume, ensuring resource efficiency during traffic spikes.

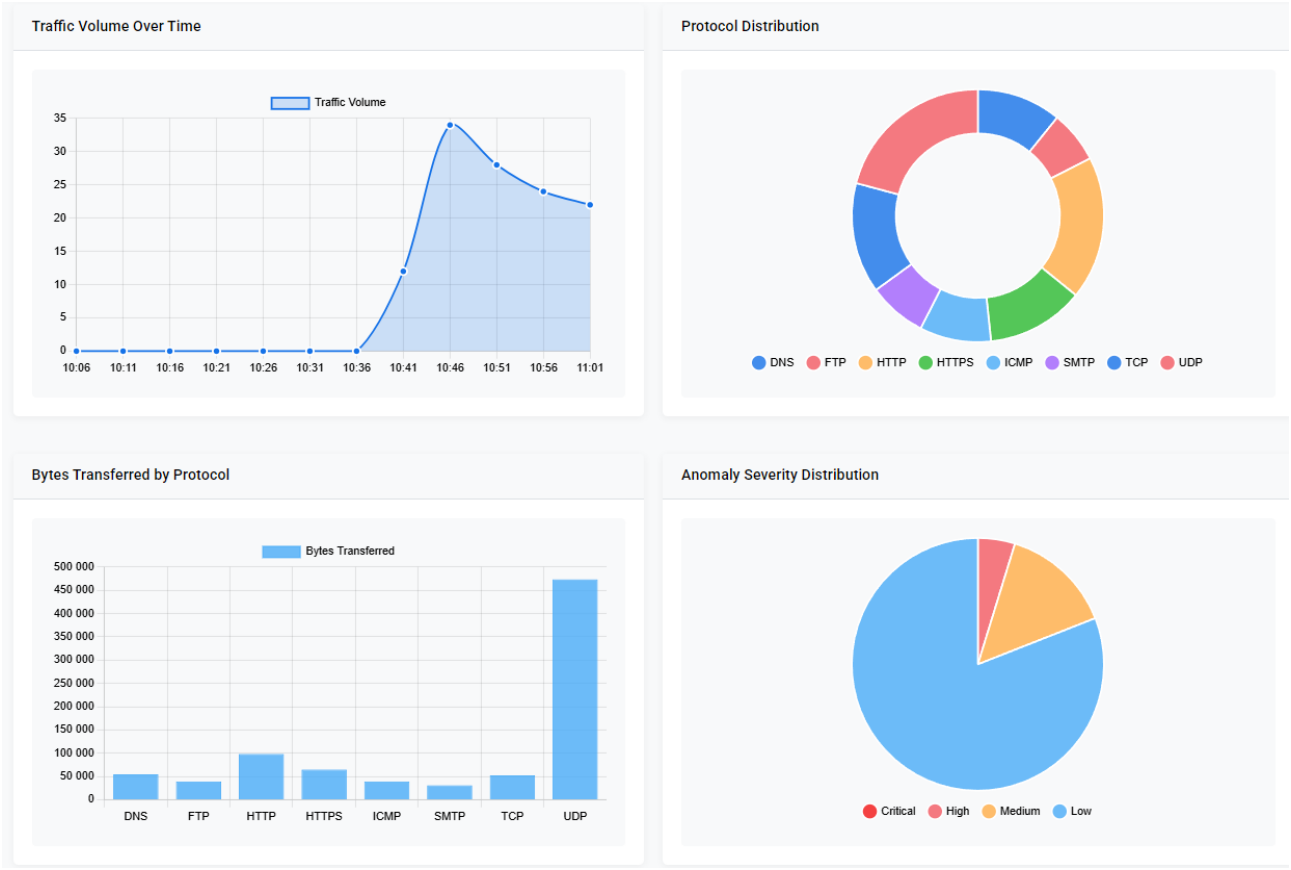


Fig. 2. Interactive visualizations of traffic, protocol, and anomaly severity

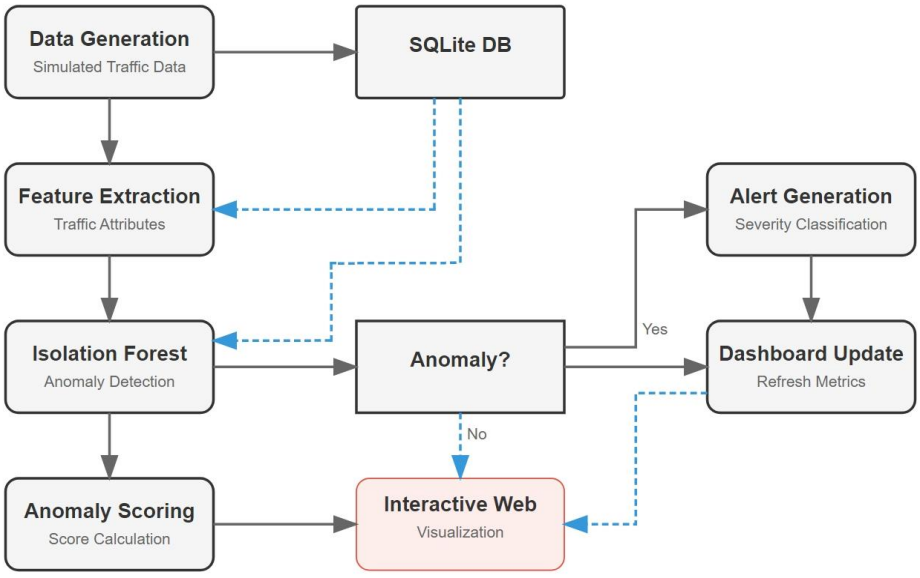


Fig. 3. Workflow of anomaly detection and visualization processes

The Flask-based MVC architecture integrates components through five stages: data generation, storage (SQLite with SQLAlchemy), anomaly detection via API endpoints, severity classification, and visualization. Authentication is managed with Flask-Login and Werkzeug utilities. The design allows algorithm substitution and supports on-demand analysis, though it requires at least 10 records for effective detection and faces challenges with high-cardinality visualizations.

Conclusion

This prototype effectively detects network traffic anomalies by integrating the isolation forest algorithm with interactive visualizations, achieving $O(n \log n)$ complexity and a four-tier severity system. The Flask-based architecture ensures scalability, while Chart.js addresses interpretability challenges. Limitations include cold-start data requirements, linear memory scaling, and occasional API errors. Future work will focus on automated scheduling, API reliability, feedback for model improvement, and WebGL acceleration for visualizations.

References

1. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

2. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303–336. https://doi.org/10.1109/SURV.2013.052213.00046

3. D'Amico A., Whitley, K. (2008). The real work of computer network defense analysts. In J. R. Goodall, G. Conti, K. L. Ma (Eds.), VizSEC 2007 (Mathematics and Visualization, pp. 19–37). Springer. https://doi.org/10.1007/978-3-540-78243-8_2

4 Liu, F. T., Ting, K. M., Zhou, Z.-H. (2008). Isolation Forest. In 2008 8th IEEE International Conference on Data Mining (pp. 413–422). IEEE. https://doi.org/10.1109/ICDM.2008.17

5. Staheli, D., Yu, T., Crouser, R. J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S., Harrison, L. (2014). Visualization evaluation for cyber security: Trends and future directions. In VizSec '14: Proceedings of the Eleventh Workshop on Visualization for Cyber Security (pp. 49–56). ACM. https://doi.org/10.1145/2671491.2671492

6. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE. https://doi.org/10.23919/CYCON.2018.8405026

Information about the authors

Wang X., Master Student of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics".

Prudnik A., Cand. Sci. (Techn.), Associate Professor, Associate Professor of the Engineering Psychology and Ergonomics Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", aleksander.prudnik@bsuir.by.

UDC 004.932.2

METHODOLOGY FOR STUDYING THE INFLUENCE OF FACE ROTATION ANGLE ON THE FACE DETECTION ACCURACY

H. Wei

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The analysis of face detection methods in images was performed. For comparative analysis of efficiency, the Viola-Jones method based on the use of Haar cascades, the method of histograms of directional gradients and the method based on convolutional neural networks were selected. The angles of head tilt in the image were selected as variable parameters. The accuracy and speed of detector operation were determined as measured parameters. For the purposes of the work, the "Labeled Faces in the Wild" (LFW) face database and the "Head Pose Image Database" dataset were selected. Convolutional neural networks showed the best results.

Keywords: face recognition; biometrics; authentication; OpenCV.

Introduction

Facial recognition is an automated process of identifying or verifying an individual based on facial image analysis. Compared to other biometric methods, facial recognition has a number of advantages, including the absence of physical contact and the ability to be implemented using standard equipment: a video camera to obtain an image and a computing device to process it. For successful identification in most applications, a short period of time for an object to be in the camera's field of view is sufficient. Despite the significant amount of research in the field of facial recognition, this topic still contains many unsolved problems. The main difficulty is to ensure reliable identification that does not depend on changes in the angle, lighting, age and appearance of a person.

Face detection in an image is the first step and is an important one, the correct implementation of which determines the success of further steps and the recognition process as a whole. Face detection can also be used to automatically count various objects (people, cars, etc.).

Today, there are numerous methods for detecting faces in an image [1]. A comparison of three methods was made:

– Haar Cascades
– Histogram of Oriented Gradients (HOG) method based on image representation.
– Classifier based on convolutional neural network (CNN).

Main Part

To determine the most effective method of face recognition, it is necessary to evaluate the accuracy and speed. Speed was assessed by the number of detected or recognized faces per second.

The Python 3.12 programming language was used as a development tool. The PyCharm IDE was used as a development environment. The Dlib library formed the basis of the software implementation of the directional gradient histogram method. The Viola-Jones method (Haar detector), as well as face capture, was performed using the OpenCV 4.7.0 computer vision algorithm library. The DNN model for face detector (dnn_samples_face_detector) project was taken as the basis for the neural network. The detector is built on the topology of a deep convolutional neural network.

To study the overall performance of detection algorithms the Labeled Faces in the Wild [2] face photograph database on the Kaggle platform was used. This database contains 13233 images of 5749 people that were collected from the Internet, detected and centered by Viola Jones's face detector. Each image is 250x250 in jpg format.

To study the efficiency of detection algorithms depending on the head tilt angle, the Head Pose Image Database [3] was used. The database contains 2790 images of fifteen people's faces with different rotation and tilt angles from -90 to +90 degrees (Fig. 1). For each person, 2 series of 93 images are available. There are images with and without glasses for each person. The database was created for training and testing machine vision algorithms. The values of the head rotation and tilt angles are combined. The vertical tilt angle "Tilt" can take values from the range {-90°, -60°, -30°, -15°, 0°, +15°, +30°, +60°, +90°}. The horizontal rotation angle "Pan" takes values from the range {-90°, -75°, -60°, -45°, -30°, -15°, 0°, +15°, +30°, +45°, +60°, +75°, +90°}. If the vertical angle is -90° or +90°, the person is looking from below or above, and the horizontal angle is 0°.

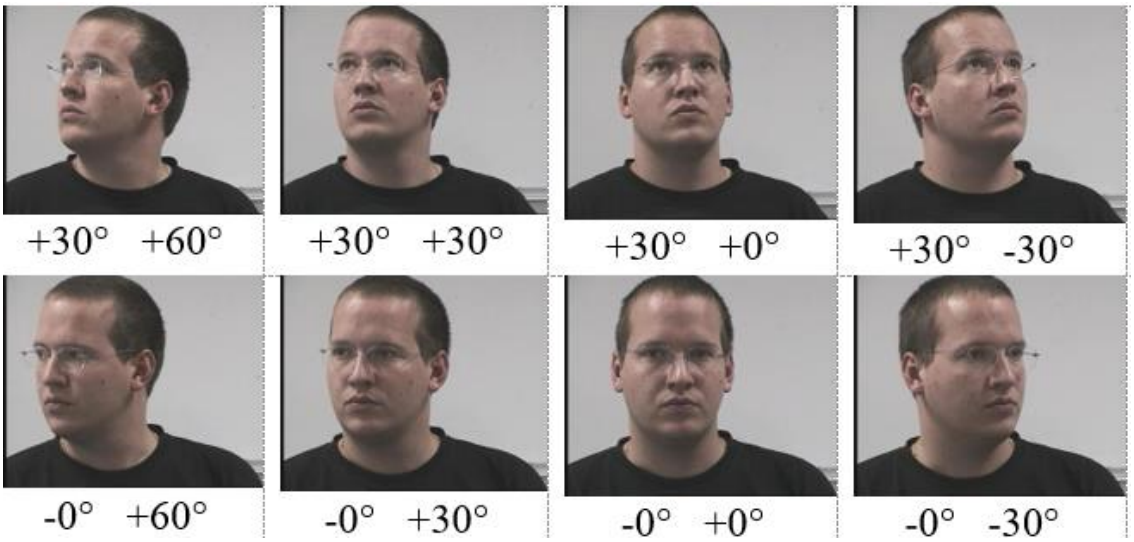


Fig. 1. Different head tilt and pan angles in the "Head Pose Image Database" dataset

The images were fed to the detectors, and the output was a result of 1 or 0 (face detected, face not detected). Accuracy indicators were calculated (the ratio of the number of detected faces to the total number of faces in the sample). Then the head tilt angle indicators were changed and similar calculations were repeated. The results of the evaluation of the speed and accuracy of detection algorithms are presented in Table 1.

Table 1. Performance of faces detection algorithms

Algorithm	Performance, persons/sec	Accuracy, %
Haar Cascades	13.7	47.66
HOG	22.88	55.91
CNN	35.38	93.54

Haar detector was effective at small horizontal and vertical rotation angles (30° in the horizontal and 45° in the vertical planes). The convolutional neural network showed very high results in face detection. A negative result is seen in the face down position and with a rotation of 60° (or more) to the right. All algorithms showed good results in a head position close to the frontal position. A drop in face detection accuracy occurred at head rotation angles to the right or left in the range from 60° to 90°. The detector based on Haar cascades showed the lowest accuracy and speed. shows the result of the detector. The detector based on histograms of directional gradients showed 56 % accuracy and was 1.6 times faster than the Haar detector. In turn, the detector based on the convolutional neural network was about 1.6 times faster than the HOG detector and showed the highest accuracy.

Conclusion

The efficiency of all considered face detection algorithms was high when the face was located close to the frontal one. A decrease in detection accuracy was observed when the head was turned to the right or left by an angle exceeding 60°. The detector based on Haar cascades demonstrated satisfactory results only at head tilt angles of up to 30° in the horizontal and vertical planes. The conducted studies indicate that convolutional neural networks (CNN) are the most effective approach to face detection and recognition within the framework of this work. This fact opens up prospects for using CNN in practical face recognition projects, which is additionally stimulated by the availability of hardware support for the execution

of neural networks in modern smartphones, as well as the availability of a wide range of frameworks for developing and training CNNs.

References

1. Levchuk S.A., Yakimenko A.A. Issledovanie xarakteristik algoritmov raspoznavaniya lic. – Novosibirsk: *Sbornik nauchny`x trudov NGTU*. – 2019. – № 1(94). – С. 55-70. DOI: 10.17212/2307-6879-2019-1-55-70 (in Russian).
2. *Labelled Faces in the Wild (LFW) Dataset* [Electronic resource]. – Access mode: https://www.kaggle.com/datasets/jessicali9530/lfw-dataset. Date of access – 28.02.2025
3. *Head Pose Image Database* [Electronic resource]. – Access mode: http://crowley-coutaz.fr/Head%20Pose%20Image%20Database.html. Date of access – 28.02.2025

Information about the author

Wei H., master's student of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", w1472908715@gmail.com

УДК 004.021, 004.056, 003.75, 681.3.06

НОВОЕ МЕТРИЧЕСКОЕ ПРОСТРАНСТВО ДЛЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ж.К. Абдурахманов
Андижанский государственный университет, Андижан, Узбекистан

Аннотация. В данной статье рассматриваются возможности применения нового расстояния, введенного автором, в различных аспектах технической защиты информации. Это расстояние обладает рядом преимуществ перед классическими метриками, что делает его полезным инструментом в анализе данных. Рассматриваются четыре ключевых направления его использования: обнаружение аномалий, коррекция ошибок, криптографические алгоритмы и биометрическая аутентификация. В системах обнаружения вторжений новое расстояние позволяет повысить точность выявления аномалий. В коррекции ошибок оно способствует более эффективному декодированию данных. В криптографии его применение улучшает генерацию ключей и устойчивость алгоритмов. В биометрической аутентификации оно повышает точность идентификации. Представлены математические модели и формулы, демонстрирующие преимущества нового расстояния. Работа показывает, что предложенный метод может существенно повысить надежность и эффективность современных средств защиты информации.
Ключевые слова: расстояние; защита информации; криптография; биометрия; коррекция ошибок; аномалии; аутентификация; кодирование; метрики; идентификация.

NEW METRIC SPACE FOR INFORMATION SECURITY TASKS

J. K. Abdurakhmanov
Andijan State University, Andijan, Uzbekistan

Abstract. This paper explores the potential applications of a new distance metric introduced by the author in the field of information security technologies. The proposed metric offers advantages over classical distance measures such as the Hamming distance and the Euclidean metric. The study examines its effectiveness in four key areas: anomaly detection, error correction, cryptographic algorithms, and biometric authentication. The new distance metric enables more accurate differentiation of data anomalies, enhances the reliability of error correction codes, strengthens cryptographic mechanisms, and improves the accuracy of biometric recognition systems. Theoretical foundations are supported by mathematical formulations, illustrating the applicability of the metric in various security-related tasks. The research demonstrates that incorporating this metric into security technologies can increase the accuracy, efficiency, and resilience of information protection systems. Future studies will focus on practical implementations of these theoretical findings in real-world security systems.
Keywords: distance, information security, cryptography, biometrics, error correction, anomalies, authentication, coding, metrics, identification.

Введение

Современные технические средства защиты информации требуют эффективных методов анализа данных и обнаружения угроз. Одним из ключевых аспектов является возможность точного измерения различий между объектами данных. В данной работе предлагается применение нового расстояния, обладающего рядом преимуществ перед классическими метриками, такими как Хэммингово расстояние и Евклидова метрика.

Новое расстояние, предложенное в [1], определяется следующим образом. Пусть заданы два конечных множества X и Y. Тогда расстояние $d(X,Y)$ вычисляется по формуле:

$$d(X,Y) = \frac{|X\Delta Y|}{2}$$

где $|X\Delta Y|$ обозначает мощность симметрической разности множеств X и Y. Данное расстояние обобщает Хэммингово расстояние, обеспечивая более тонкую градацию различий между объектами.

Рассмотрим иллюстрирующий пример. Пусть даны два множества битовых строк:

$X = \{101,110,011\}, Y = \{100,110,010\}$.

Симметрическая разность этих множеств равна $\{101,011,100,010\}$, следовательно,

$d(X,Y) = \frac{4}{2} = 2$.

Этот пример демонстрирует, что новое расстояние позволяет учитывать частичные совпадения между объектами, что особенно важно в задачах защиты информации.

Обнаружение аномалий в данных

Аномалии в данных могут указывать на потенциальные угрозы информационной безопасности, включая несанкционированный доступ и сетевые атаки. Новое расстояние позволяет более точно оценивать степень отклонения между нормальными и аномальными данными, что делает его полезным инструментом для систем обнаружения вторжений (IDS). Например:

– В анализе сетевого трафика новое расстояние можно применять для выделения аномальных пакетов данных, используя кластерный анализ аномалий.

– В логах операционной системы можно сравнивать последовательности событий, выявляя подозрительные отклонения от нормального поведения.

– В анализе данных IoT-устройств новое расстояние может использоваться для распознавания неожиданных паттернов активности, сигнализирующих о компрометации устройства.

Математически, если заданы два набора данных X и Y, то степень аномальности можно оценить с помощью следующего выражения:

$$A(X,Y) = \frac{d(X,Y)}{d_{max}}$$

где d_{max} – некоторый эталонный (или максимальный) уровень расстояния, соответствующий нормализующей константе. Например, это может быть:

– максимальное расстояние между объектами в обучающей выборке;

– среднее расстояние в нормальных условиях;

– фиксированный порог аномальности.

Улучшение коррекции ошибок

Передача данных по шумным каналам требует механизмов исправления ошибок. Обобщая известные методы кодирования, новое расстояние может способствовать разработке более эффективных корректирующих кодов. Например:
В кодах с обнаружением и исправлением ошибок новое расстояние можно применять для оптимизации декодирования в условиях высокой зашумленности.
В системах передачи данных по спутниковым каналам оно позволяет адаптивно изменять кодовые параметры в зависимости от уровня помех.
В хранилищах больших данных новое расстояние можно использовать для автоматического восстановления поврежденных фрагментов информации на основе избыточных данных.

Математически, если $d(x,y)$ – новое расстояние между кодовыми словами, а $H(x,y)$ – Хэммингово расстояние, то в ряде случаев выполняется неравенство:

$$d(x,y) \leq \frac{H(x,y)}{2},$$

что позволяет детектировать ошибки на более тонком уровне и применять эффективные алгоритмы исправления. Дополнительно, вероятность ошибки декодирования можно оценить как:

$$P_e = e^{-\alpha d(x,y)},$$

где α – коэффициент, зависящий от характеристик канала передачи данных.

Оптимизация криптографических алгоритмов

Многие криптографические алгоритмы зависят от устойчивости метрик различия. Новое расстояние предлагает ряд преимуществ:

В генерации ключей новое расстояние можно использовать для усиления криптографической стойкости за счет выбора ключей с максимальным различием.

В алгоритмах цифровых подписей оно может обеспечивать более надежную проверку подлинности.

В механизмах хеширования новое расстояние можно применять для улучшения коллизионной устойчивости.

Допустим, ключ K генерируется на основе входных данных X, тогда использование нового расстояния может обеспечивать более равномерное распределение ключей:

$$H(K_1,K_2) > 2d(K_1,K_2).$$

Дополнительно, криптографическая стойкость алгоритма можно выразить через энтропию ключей:

$$S = -\sum p_i \log p_i$$

где p_i – вероятность выбора конкретного ключа.

Биометрическая аутентификация

Современные системы идентификации используют методы сравнения биометрических данных. Новое расстояние позволяет более точно анализировать различия между биометрическими шаблонами, что способствует повышению надежности распознавания. Например:

– в системах распознавания лиц его можно применять для более точного измерения различий между векторными представлениями изображений;

– в системах аутентификации по отпечаткам пальцев оно может повысить точность идентификации при частичных отпечатках;

– в голосовой биометрии новое расстояние может использоваться для выделения тонких различий в акустических характеристиках.

Заключение

Рассмотренные направления демонстрируют широкие возможности применения нового расстояния в технических средствах защиты информации. Его использование может повысить точность обнаружения угроз, улучшить корректирующие коды, усилить криптографические механизмы и повысить надежность биометрической аутентификации. Дальнейшие исследования направлены на практическую реализацию данных идей в конкретных системах безопасности.

Список использованных источников / References

1. Jamolidin Abdurakhmanov . New distance for any finite sets, half the Hamming distance. *TechRxiv.* April 05, 2023.

Сведения об авторе

Абдурахманов Ж.К., кандидат физико-математических наук, доцент, доцент кафедры Информационных технологий Андижанского государственного университета, jamolidinkamol@gmail.com.

Information about the author

Abdurakhmanov J.K., Ph.D. in Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Information Technology at Andijan State University, jamolidinkamol@gmail.com.

УДК 004.651

ЭЛЕМЕНТНАЯ БАЗА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ: КЛЮЧЕВЫЕ КОМПОНЕНТЫ И ТЕХНОЛОГИИ

А.А. Перманова, Ю.А. Рахимова
Инженерно-технологического университет Туркменистана имени Огуз хана, Ашхабад, Туркменистан

Аннотация. Элементная база средств защиты информации (СЗИ) представляет собой совокупность технологических компонентов, которые обеспечивают безопасность данных на различных уровнях их обработки и хранения. В статье рассматриваются ключевые элементы, включающие криптографические чипы, процессоры, аутентификационные устройства, сетевые устройства защиты, а также программные решения для предотвращения несанкционированного доступа и утечек информации. Особое внимание уделяется роли защищенных носителей информации, средств шифрования и средств мониторинга и защиты на уровне операционных систем. Подчеркивается важность интеграции этих элементов в единую систему безопасности для эффективной защиты от угроз в современных информационных системах. В заключении делается акцент на необходимость постоянного обновления элементной базы СЗИ с учетом развития технологий и новых типов киберугроз.
Ключевые слова: Элементная база; Криптографические чипы; Аутентификация; Программные средства защиты.

ELEMENTARY BASE OF INFORMATION SECURITY MEANS: KEY COMPONENTS AND TECHNOLOGIES

A.A. Permanova, Y.A. Rahimova
Oguz Khan Engineering and Technological University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. The element base of information security means (ISM) consists of various technological components that ensure the protection of data at different stages of processing and storage. This paper explores the key

elements of ISM, including cryptographic chips, processors, authentication devices, network security appliances, as well as software solutions designed to prevent unauthorized access and data leaks. Particular attention is given to the role of secure data storage devices, encryption methods, and monitoring and protection tools implemented at the operating system level. The importance of integrating these elements into a unified security system for effective protection against modern cyber threats is emphasized. The conclusion highlights the necessity of continuous updates and enhancements to the ISM element base in response to the rapid development of technologies and emerging cyber threats.
Keywords: Element base; Cryptographic chips; Authentication; Software protection tools;

Основная часть

1. Элементная база. Современные системы защиты информации (СЗИ) становятся все более сложными и многослойными. Одним из важнейших аспектов, определяющих их эффективность, является элементная база, которая включает в себя различные компоненты и устройства, обеспечивающие безопасность данных.

2. Процессоры и криптографические чипы. Одним из ключевых элементов являются специализированные процессоры и криптографические чипы, которые используются для выполнения криптографических операций, таких как шифрование, дешифрование и генерация ключей. Эти устройства могут быть интегрированы в аппаратные средства защиты (например, токены или смарт-карты) и предоставляют высокий уровень безопасности благодаря аппаратной изоляции.

3. Аутентификационные устройства. Для защиты доступа к информации применяются аутентификационные устройства, включая биометрические системы (например, отпечатки пальцев или распознавание лиц), токены, смарт-карты, а также двухфакторную аутентификацию. Эти средства обеспечивают надежную идентификацию пользователей и предотвращают несанкционированный доступ к защищенным данным.

4. Программные средства защиты. Программные компоненты, такие как антивирусное ПО, системы защиты от вредоносных программ, программы для контроля доступа и предотвращения утечек информации (DLP-системы), играют важную роль в защите от внешних и внутренних угроз. Эти средства помогают отслеживать и блокировать вредоносное ПО, предотвращать утечку конфиденциальных данных и обеспечивать контроль за действиями пользователей.

Заключение

Элементная база средств защиты информации представляет собой сложную совокупность различных технологий и устройств, которые обеспечивают многослойную защиту данных от различных угроз. Важно помнить, что для достижения высокой степени безопасности требуется интеграция и координация всех этих компонентов, а также постоянное обновление и совершенствование средств защиты в ответ на новые угрозы.

Список использованных источников

1. Горелов, А. И. Средства защиты информации: обзор технологий и решений. – СПб.: БХВ-Петербург, 2019.

2. Руденко, С. В. Защита информации в современных информационных системах. – М.: Физматлит, 2020.

3. Прохоров, В. Н. Аппаратные средства защиты информации.

4. Лемей Л., Макдональд Дж. «Управление информационной безопасностью: принципы и практика». Нью-Йорк: Уайли, 2020.

5. Сальгадо Р., Джейкобс С. Модули аппаратной безопасности: концепции и практика». - Спрингер, 2021.риптографические устройства. – М.: Издательство «Наука», 2022.

References

1. Gorelov, A. I. Information security tools: a review of technologies and solutions. – St. Petersburg: BHV-Petersburg, 2019.
2. Rudenko, S. V. Information security in modern information system". Moscow: Fizmatlit, 2020.
3. Prokhorov, V. N. Hardware for information security and cryptographic devices. Moscow: Nauka Publishing House, 2022.
4. Lemay, L., & McDonald, J. Information Security Management: Principles and Practices. – New York: Wiley, 2020.
5. Salgado, R., & Jacobs, S. Hardware Security Modules: Concepts and Practices. – Springer, 2021.

Сведения об авторах

Перманова А.А., преподаватель кафедры «Компьютерные науки и информационные технологий» Инженерно-технологического университета Туркменистана имени Огуз хана.
Рахимова Ю.А., студентка факультета Киберфизических систем Инженерно-технологического университет Туркменистана имени Огуз хана.

Information about the authors

Permanova A.A., Teacher of the Department of Computer Science and Information Technologies of the Oguz Khan University of Engineering and Technology of Turkmenistan.
Rahimova Y.A., Student of the Faculty of Cyber-Physical Systems, Engineering and Technology University of Turkmenistan named after Oguz Khan.

УДК 004.056.53

СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.И. Алейникова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь

Аннотация. Рассмотрены основные этапы функционирования SIEM-системы, ключевой фактор, влияющий на эффективность аналитики и работы детектирующей логики SIEM-системы. Рассмотрены примеры воздействия нарушителя на уровень сбора событий информационной безопасности и даны рекомендации по противодействию. Рассмотрены события, для которых необходимо осуществлять мониторинг и настройку корреляционных правил в первую очередь. Приведены примеры настройки корреляционных правил для выявления потенциальных инцидентов информационной безопасности или потенциальных уязвимостей в локальной сети организации. Даны рекомендации по снижению ложноположительных сработок SIEM-системы.
Ключевые слова: система мониторинга, SIEM-система, агрегация, корреляция, управление активами, мониторинг, выявление инцидентов, выявление уязвимостей, ложноположительные сработки.

INFORMATION SECURITY AND INFORMATION SECURITY EVENT MANAGEMENT SYSTEMS

D.I. Aleinikova
Belarusian State University of Informatics and Radio Electronics, Minsk, Belarus

Abstract. The main stages of the SIEM system functioning, a key factor influencing the effectiveness of analytics and the detection logic of the SIEM system, are considered. Examples of the attacker's impact on the level of information security event collection are considered and recommendations on counteraction are given. The events for which it is necessary to monitor and adjust the correlation rules in the first place are considered. Examples of setting up correlation rules to identify potential information security incidents or potential vulnerabilities in the organization's local network are given. Recommendations to reduce the false positive alarms of the SIEM system are given.
Keywords: monitoring system, SIEM, aggregation, correlation, asset management, monitoring, incident detection, vulnerability detection, false positive alarms.

Введение

В настоящее время информационная безопасность является одним из приоритетных направлений для любой организации. Для решения задач быстрого выявления инцидентов и своевременного реагирования на них применяются системы класса SIEM (Security Information and Event Management). Они позволяют анализировать большое количество событий информационной безопасности в локальной сети организации в режиме реального времени, оперативно выявлять угрозы, уязвимости или инциденты, повышая скорость реагирования и способствуя предотвращению или минимизации ущерба от реализации атак.

Основная часть

SIEM-система – ключевой компонент в архитектуре SOC (Security Operational Center), обеспечивающий централизованный сбор информации с различных источников информационной инфраструктуры организации, таких как рабочие станции пользователей, серверы приложений и веб-серверы, базы данных, почтовый и хостовой антивирусы, системы класса IDS/IPS (Intrusion Detection System/Intrusion Prevention System), межсетевые экраны, телекоммуникационное оборудование и другие. На рис. 1 представлены базовые модули классической SIEM-системы [1].

Рис. 1. Базовые модули SIEM-системы
Fig. 1. Basic modules of the SIEM system

После сбора и нормализации событий ключевыми этапами работы SIEM-системы являются агрегация и корреляция полученных событий информационной безопасности.

Агрегация представляет собой сбор и объединение однородных или повторяющихся событий информационной безопасности в единую структуру, которую затем можно использовать для дальнейшего анализа. Пример агрегации – объединение повторяющихся событий о неудачных попытках входа под одной учетной записью с определенного хоста.

Корреляция – анализ различных событий с целью выявления потенциальных инцидентов информационной безопасности. По заданным настройкам SIEM-система обрабатывает приходящие потоки событий информационной безопасности, выявляя взаимосвязи, которые в совокупности могут указывать на потенциальную атаку. Помимо выявления атак, грамотная настройка корреляций событий позволяет снизить число ложноположительных сработок SIEM-системы.

Следует отметить, что возможности аналитики и работы детектирующей логики данной системы напрямую зависят от полноты собираемой телеметрии (событий информационной безопасности) с хостов и средств защиты, составляющих информационную инфраструктуру организации. В основе эффективной работы SIEM лежит управление активами, их инвентаризация.

Учитывая этот факт, нарушители информационной безопасности могут оказывать воздействие на уровень сбора событий информационной безопасности, чтобы сокрыть свое присутствие в локальной сети.

Например, нарушитель может попытаться напрямую остановить сервис логирования событий на хосте, например, с помощью штатных системных средств (SC, PowerShell) или путем модификации соответствующих ключей реестра. В таком случае можно настроить корреляционные правила SIEM-системы учитывая такие события, как отключение службы логирования, очистка журнала мониторинга, а также осуществлять контроль содержимого командной строки в событиях запуска процессов.

Тем не менее, нарушитель может воспользоваться «слепым местом» в локальной сети, когда на некоторых хостах аудит информационной безопасности работает некорректно или не настроен. Стоит отметить, что передовые SIEM-системы оснащены функционалом, отслеживающим доступность подключенных источников, отсутствие определенного типа событий информационной безопасности, задержки в их получении. Использование этого функционала позволит своевременно обнаружить и устранить ошибки в настройках аудита или выявить потенциальную атаку на информационную инфраструктуру.

Рассмотрим примеры событий, для которых необходимо осуществлять мониторинг и настройку корреляционных правил в SIEM-системе [2,3].

Последовательное появление события неудачной попытки авторизации в системе в течение небольшого промежутка времени может указывать на потенциальную атаку подбора пароля. Например, для операционной системы Windows событие с event ID 4625, в котором также указана причина неудачной попытки входа в виде кода или в поле «Failure Reason». Таким образом, можно настроить агрегацию 6 таких событий за 15 минут для одной и той же учетной записи с одного IP-адреса в локальной сети. Еще одним вариантом мониторинга такого события может быть настройка агрегации 4 событий за 15 минут для разных учетных записей, размещенных на одном хосте. Такая последовательность событий также может также указывать на потенциальный перебор учетных записей и паролей к ним.

Необходимо отслеживать изменение прав доступа для учетных записей, особенно на критически значимых активах организации. При использовании в локальной сети контроллера домена можно отслеживать добавление пользователей в сетевые группы. Например, для операционной системы Windows события с event ID 4728, 4732, 4756, 4729, 4733, 4757. Для осуществления контроля и обеспечения информационной безопасности организации предоставление прав доступ пользователям должно быть согласовано с подразделением, отвечающем за информационную безопасность. Обнаружение событий изменения прав доступа учетных записей не в соответствии с согласованным доступом может указывать на действия нарушителя или халатность работников, создающую потенциальную уязвимость в локальной сети организации.

Несогласованные внутренние сканирования локальной сети могут являться попытками нарушителя изучить сетевую архитектуру, следовательно, можно настроить правила корреляции на их обнаружение. Например, можно отслеживать наличие сетевого трафика с одного IP-адреса на множество других, по определенному набору портов или по всем.

Для обеспечения безопасности корпоративной сети применяется технология ее сегментации. Следует отметить, что тестовые подсети также должны находиться в изолированном сетевом контуре. Можно настроить корреляционное правило, которое будет отслеживать исходящий (входящий) трафик из (в) тестовых подсетей. Если обнаруженные исходящие или входящие телекоммуникационные доступы не были согласованными, то это может быть признаком действий нарушителя или халатности

работников, создающей потенциальную уязвимость в локальной сети организации. Также необходимо отслеживать наличие несогласованных сетевых доступов во внешнюю сеть из внутренней сети или из изолированных сегментов, для которых такой доступ не предусмотрен.

Отслеживание изменений в конфигурации сетевого оборудования, в частности маршрутизаторов и межсетевых экранов, поможет своевременно выявить нарушение в регламентированных настройках сетевого оборудования или обнаружить предоставление сетевого доступа (изменение списков контроля доступа), которого быть не должно. После создания корреляционных правил необходимо отслеживать правильность их функционирования и, при необходимости, дорабатывать их, в том числе снижать количество ложноположительных сработок SIEM-системы. Для этого можно воспользоваться списками исключений и подбором более точных условий агрегации событий. Следует отметить, что ведение списков исключений представляет собой постоянный процесс.

Заключение

Системы класса SIEM играют важную роль в обеспечении информационной безопасности. Внедрение таких систем в информационную инфраструктуру организации значительно упрощает процесс мониторинга, а также повышает скорость обнаружения и реагирования на инциденты информационной безопасности. SIEM-система позволяет в режиме реального времени анализировать и коррелировать события информационной безопасности, приходящие с хостов, а также многочисленных средств защиты информации, таких как почтовые и хвостовые антивирусы, межсетевые экраны, WAF (Web Application Firewall), DLP-системы (Data Link Prevention), системы класса IDP/IPS и другие. Данный подход особенно актуален для организаций, обладающих большой информационной инфраструктурой, например, банковский сектор, где количество хостов исчисляется тысячами.

Список использованных источников

1. Gonzalez Granadillo G., Gonzalez Zarzosa S., Diaz R. (2021) Security Information and Event Management (SIEM). *ResearchGate*. 34 (2), 1–2.
2. Ertugrul A. (2016) Log correlation SIEM rule examples and correlation engine performance data. *ResearchGate*. 2 (2), 1–2.
3. Таблица Attack Mitre. – Текст: электронный // Mitre: официальный сайт. – 2025. – URL: https://attack.mitre.org/ (дата обращения: 15.02.2025).

References

1. Gonzalez Granadillo G., Gonzalez Zarzosa S., Diaz R. (2021) Security Information and Event Management (SIEM). *ResearchGate*. 34 (2), 1–2.
2. Ertugrul A. (2016) Log correlation SIEM rule examples and correlation engine performance data. *ResearchGate*. 2 (2), 1–2.
3. Attack Mitre Table. – Text: electronic // Mitre: official web-site. – 2025. – URL: https://attack.mitre.org/ (date of request: 15.02.2025).

Сведения об авторе

Алейникова Д.И., магистрант кафедры защиты информации, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alein.diana@yandex.ru

Information about the author

Aleinikova D., master student o fthe Department of Information Security, Belarusian State University of Informatics and Radio Electronics, alein.diana@yandex.ru.

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ПРИБОРОВ ОБНАРУЖЕНИЯ СКРЫТЫХ ПРОВОДОВ ТЕХНИЧЕСКИХ СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ

В.М. Алефиренко, А.Д. Денскевич, Е.Д. Зубрицкий
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Представлены результаты сравнительного анализа технических характеристик приборов обнаружения скрытых проводов, используемых для обнаружения несанкционированных средств получения информации, у которых питание, управление и съем информации осуществляется по проводам. Для сравнительного анализа использовался комплексный метод определения уровня качества на основе средневзвешенного арифметического показателя. В качестве единичных показателей брались такие технические характеристики приборов как максимальная глубина обнаружения, количество поисковых программ, время непрерывной работы, габаритные размеры, вес, максимальная и минимальная рабочая температура, гарантийный срок, вес, цена. Результаты анализа приведены в виде столбиковых диаграмм, которые могут использоваться для решения вопроса выбора лучшего прибора для систем защиты информации.
Ключевые слова: защита информации; скрытые провода; обнаружение; приборы; технические характеристики; комплексный показатель; сравнительный анализ; выбор приборов; система защиты.

COMPARATIVE ANALYSIS OF THE TECHNICAL CHARACTERISTICS OF HIDDEN WIRE DETECTION DEVICES FOR TECHNICAL MEANS OF UNAUTHORIZED INFORMATION ACQUISITION

V.M. Alefirenko, A.D. Denskevich, E.D. Zubritsky
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Annotation. The results of a comparative analysis of the technical characteristics of hidden wire detection devices used to detect unauthorized means of obtaining information, in which power supply, control and information retrieval are carried out via wires, are presented. For the comparative analysis, a comprehensive method was used to determine the quality level based on a weighted arithmetic mean. Such technical characteristics of the devices as the maximum detection depth, number of search programs, continuous operation time, overall dimensions, weight, maximum and minimum operating temperature, warranty period, weight, and price were taken as single indicators. The results of the analysis are presented in the form of bar charts, which can be used to decide on the choice of the best device for information security systems.
Keywords: information protection; hidden wires; detection; devices; technical characteristics; complex indicator; comparative analysis; selection of devices; protection system.

Введение

В системах защиты информации для поиска технических средств несанкционированного получения информации широко используются такие приборы, как индикаторы электромагнитного поля, сканирующие приемники, аппаратно-программные комплексы, обнаружители скрытых видеокамер, нелинейные локаторы и др. В эту систему целесообразно включить и приборы обнаружения скрытых проводов. Такие приборы позволяют обнаруживать скрытые провода, через которые осуществляется съем информации, питание и управление техническими средствами несанкционированного получения информации, например, такими как проводные микрофоны и стетоскопы, малогабаритные видеокамеры и другие устройства, управляемые по скрытно проложенным проводам. В связи с этим представляет интерес проведения сравнительного анализа технических характеристик этих приборов.

Основная часть

Для сравнительного анализа использовался комплексный метод определения уровня качества с использованием единичных показателей [1]. Комплексный метод оценки качества изделий предполагает использование комплексных показателей, в качестве одного из которых может использоваться средневзвешенный арифметический показатель, который определяется по формуле

(1)

где k_{Hi} – нормированный i-й единичный показатель; α_{Hi} – нормированный коэффициент, характеризующий вес (значимость, важность) i-го единичного показателя; m – количество единичных показателей, принятых во внимание.

Поскольку технические характеристики приборов обнаружения скрытых проводов имеют различные размерности, то для использования формулы (1) необходимо провести их нормировку, чтобы получить безразмерные значения. Нормировка проводится с помощью выражения

(2)

где k_i – исходное значение i-го единичного показателя; $k_{кр\,i}$ – критическое значение i-го единичного показателя; $k_{опт\,i}$ – оптимальное значение i-го показателя.

Исходные значения k_i должны лежат в пределах $k_{кр\,i} < k_i < k_{опт\,i}$, если увеличение значения показателя приводит к увеличению уровня качества, или $k_{опт\,i} < k_i < k_{кр\,i}$, если уменьшение значения показателя приводит к увеличению уровня качества. Таким образом, нормированные значения K_{Hi} будут лежать в пределах $0 < K_{Hi} < 1$.

Коэффициенты значимости α_{Hi} для формулы (1) должны выбираться таким образом, чтобы обеспечивалось условие

(3)

Для сравнения были выбраны восемь моделей приборов обнаружения скрытых проводов различных фирм: Bosch GMS 120 Professional, Bosch GMS 100 M Professional, ADA Instruments Wall Scanner 80, ADA Instruments Wall Scanner 50, ЗУБР Мастер DX-350, ЗУБР Профессионал DX-750, Laserliner CombiFinder Plus 080.955A, Wortex MD 3009.

В качестве единичных показателей брались следующие технические характеристики: максимальная глубина обнаружения, количество поисковых программ, время непрерывной работы, габаритные размеры, вес, максимальная и минимальная рабочая температура, гарантийный срок, вес, цена.

Расчет проводился с использованием средневзвешенного арифметического показателя качества [2].

Результаты расчетов, проведенные по формуле (1) с учетом выражений (2) и (3), в виде столбиковой диаграммы представлены на рис. 1. Как видно из рис. 1 наилучшие значения показателей качества были у модели *ADA Instruments Wall Scanner* 80 (0,65), на втором месте – *Bosch GMS 120 Professional* (0,64) и на третьем месте – *Bosch GMS 100 M Professional* (0,58), то есть значения показателей у приборов, занявших первые три места, близки между собой. Внешний вид этих приборов показан на рис. 2.

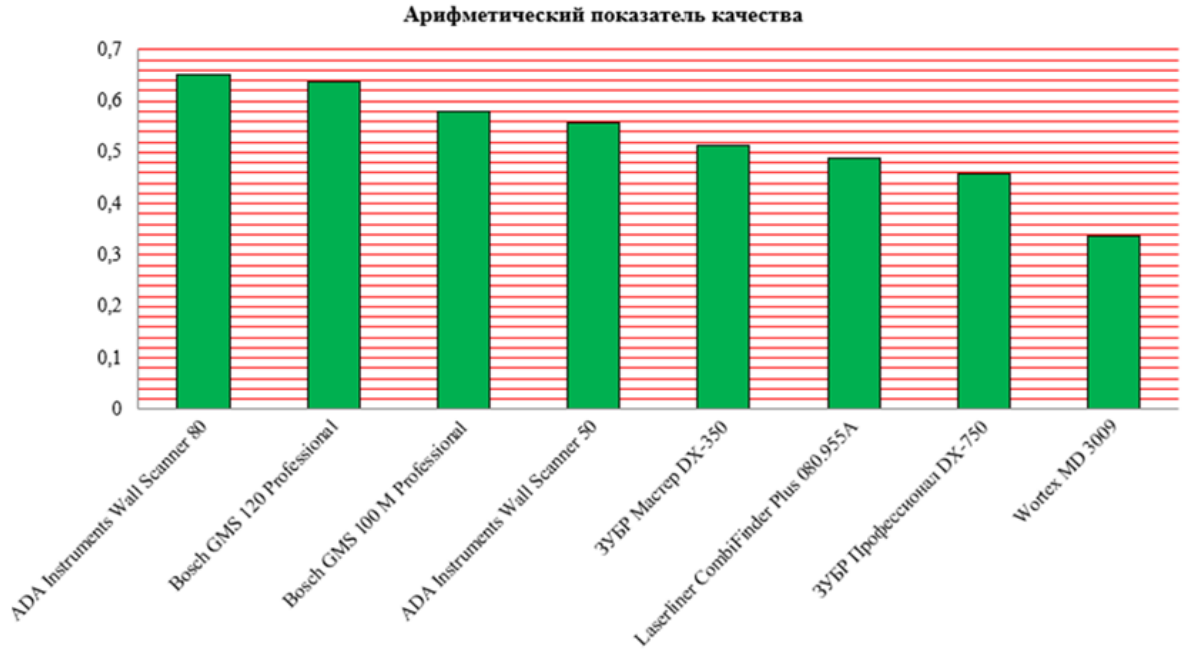


Рис. 1. Распределение комплексных арифметических показателей качества приборов обнаружения скрытых проводов
Fig. 1. Distribution of complex arithmetic quality indicators of hidden wire detection devices

a *b* *c*

Рис. 2. Внешний вид лучших приборов обнаружения скрытых проводов: *a* – ADA Instruments Wall Scanner 80; *b* – Bosch GMS 120 Professional; *c* – Bosch GMS 100 M Professional
Fig. 2. Appearance of the best hidden wire detection devices: *a* – ADA Instruments Wall Scanner 80; *b* – Bosch GMS 120 Professional; *c* – Bosch GMS 100 M Professional

Анализ полученных результатов показал также, что значения комплексного арифметического показателя качества для исследуемых приборов лежат в пределах от 0,65 (ADA Instruments Wall Scanner 80 до 0,34 (Wortex MD 3009), то есть максимальное и минимальное значения отличаются почти в два раза.

Заключение

Полученные результаты комплексного анализа уровня качества приборов обнаружения скрытых проводов с помощью средневзвешенного арифметического показателя, комплексно учитывающего значения технических характеристик, могут использоваться для решения вопроса выбора лучшего прибора для систем защиты информации.

Список использованных источников

1. Алефиренко, В.М. (2017) Выбор состава технических средств для систем обеспечения безопасности. *Доклады БГУИР*. 2 (104), 39–44.
2. Алефиренко В.М., Денскевич А.Д., Зубрицкий Е.Д. (2024) Анализ технических характеристик нелинейных локаторов с помощью комплексного арифметического показателя качества. *Журнал «Science Time»*. 12 (131). 82–86.

References

1. Alefirenko, V.M. (2017) Selection of the composition of technical means for security systems. *Reports of the BSUIR*. 2 (104), 39-44 (in Russian).
2. Alefirenko V.M., Denskevich A.D., Zubritskiy E.D. (2024) Analysis of the technical characteristics of nonlinear locators using a complex arithmetic quality indicator. *«Science Time» magazine*. 12 (131). 82–86 (in Russian).

Сведения об авторах

Алефиренко В.М., канд. техн. наук, доц., доцент кафедры информационно-компьютерных систем, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alefirenko@bsuir.by.
Денскевич А.Д., ассистент кафедры электронной техники и технологии, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», denskevichad@gmail.com.
Зубрицкий Е.Д., магистрант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», zzubritski@gmail.com.

Information about the authors

Alefirenko V.M., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Information and Computer-Aided Systems Design Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics".
Denskevich A.D., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", denskevichad@gmail.com.
Zubritskiy E.D., Master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", zzubrits-ki@gmail.com.

УДК 004.056.5

БЕЗОПАСНОСТЬ ДАННЫХ В ЦИФРОВОМ МИРЕ

О.Г. Аманова, А.А. Гелдиев, А.А. Мухамметныязов

Аннотация. Эта статья о развитии информационной безопасности в Туркменистане. Анализируются основные угрозы и вызовы, с которыми сталкиваются банки и государственные структуры в области информационной безопасности. Особое внимание уделяется мерам по защите информации и развитию кибербезопасности в контексте современных тенденций в области цифровизации.
Ключевые слова: банк, пластиковая карта, цифровизация, информационная безопасность, IT-отрасль.

DIGITAL SECURITY IN A NETWORKED WORLD

O.G. Amanova, A.A. Geldiyev, A.A. Muhammetniyazov

Abstract. This article is about the development of information security in Turkmenistan. The main threats and challenges faced by banks and government agencies in the field of information security are analyzed. Particular attention is paid to measures to protect information and develop cyber security in the context of modern trends in the field of digitalization.
Keywords: cyber security, bank, plastic cards, digitalization, information security, IT industry.

На фоне осуществляемого перехода от индустриального к информационному обществу повышается значимость умения ориентироваться в постоянно возрастающем

потоке информации, эффективно работая с ней. Сегодня возможности глобальной сети, активно используется во всех сферах общественной жизни. Основаны на информационных ресурсах, представляющих собой совокупность данных, которые организованы в информационных системах для получения достоверных сведений в различных областях знаний и практической деятельности. Однако одновременно с увеличением роли информации повышается и важность ее передачи и защиты, обеспечивающейся посредством инструментов информационной безопасности.

Целью работы является изучение особенностей информационной безопасности. Для ее достижения были использованы методы анализа и синтеза научных публикаций и литературных источников по рассматриваемой теме.

В статье рассмотрим два различных механизма защиты: смарт-карты и запоминающие карты с магнитной полосой. Определим, с какой картой будет более безопасно пользоваться смарт-картами с микропроцессором или картой с памятью магнитной полосой.

Информационная безопасность характеризуется способностью государства, общества, социальной группы, личности обеспечить защищенность информационных ресурсов для поддержания своей жизнедеятельности и жизнеспособности, противостоять информационным опасностям и угрозам, неблагоприятным информационным воздействиям на личное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации.

В Туркменистане приняты основополагающие законодательные акты Конституция Туркменистана, закон Туркменистана «Об информации и ее защите»,«О государственных секретах», «Об электронном документе и электронной цифровой подписи.

Наиболее распространенными случаями кибератак являются ботнеты: это сеть компьютеров, зараженных вредоносной программой, позволяющей злоумышленникам удаленно атаковать электронную систему платежей, управлять чужими пластиковыми картами без ведома их владельцев. С помощью ботнетов злоумышленники могут рассылать спам, распространять вирусы, атаковать компьютеры и серверы банков, а также совершать другие преступления.

Сегодня фишинг – один из самых распространенных в мире видов киберпреступлений, с помощью которого чаще всего похищают аккаунты и банковскую информацию.

Электронная система платежей, основанная на использовании смарт-карты, на которой ведется баланс средств. Их часто называют «stored-value cards» электронный бумажник. Некоторые такие карты уже опробованы на практике: система MasterCard, VisaCard.

Основная идея таких карт состоит в том, чтобы использовать ее в денежных расчетах. Специальные терминалы стали неотъемлемой частью нашей жизни: они появились в банках, в магазинах и присоединены к компьютерам, подключенным к Интернету. Такие карты обладают тем преимуществом, что они не обязательно должны работать в режиме онлайн, то есть находиться на связи с каким-либо центральным сервером. При использовании обычных платежных карточек торговый автомат обязан связаться с банковским компьютером в режиме реального времени. Их недостаток состоит в том, что утрата или повреждение карты означают потерю денег.

Как и всякая другая система электронных платежей, электронный бумажник имеет полный набор средств защиты. В их защите использует криптография, меры компьютерной безопасности, средства защиты от подделки и. т. д. Они обеспечивают необходимый уровень целостности данных, конфиденциальность и анонимность.

Мы не будем вдаваться в подробности, но рассмотрим, как используются карты двух различных типов.

Карты с магнитной полосой. Пользователь помещает карту в считывающее устройство и вводит PIN (личный идентификационный номер), пароль или код. Устройство считывает данные с магнитной полосы и использует PIN для расшифровки данных. Затем эти данные обрабатываются устройством для выполнения системой разнообразных действий, для которых она предназначена: вхождение в систему, подписывание электронного чека, плата за стоянку и т. п.

Смарт-карты. Пользователь помещает карту в различные считывающие устройства и вводит тот же личный идентификационный номер. Устройство посылает PIN в смарт-карту, которая расшифровывает данные. Затем они используются картой для выполнения системой нужных действий, а само устройство выполняет в системе функцию ввода-вывода данных.

В чем же различия? В обоих случаях примененное в преступных целях считывающее устройство в состоянии разрушить систему, так как это устройство является единственной связью карты с внешним миром. Как только станут известны секретные данные карты с магнитной полосой, устройство может делать все, что пожелает. Как только смарт-карта получит правильный PIN, считывающее устройство может заставить всех поверить всему, что оно захочет.

Основное различие между этими картами состоит в том, что смарт-карта умеет осуществлять некоторый контроль, так как имеет внутреннюю защиту. Например, если кто-нибудь украдет карту с магнитной полосой, он сможет грубыми приемами завладеть данными этой карты. Он может сделать это автономно, на компьютере, так что ее владелец даже не узнает о случившемся.

Смарт-карту нельзя взломать подобным образом, поскольку ее можно запрограммировать так, что она будет выключаться после нескольких неправильных вводов пароля подряд. Так, если кто-нибудь похитит смарт-карту, узнать пароль с легкостью у него не получится. Он получит возможность сделать только три попытки.

Другое существенное различие состоит в том, что смарт-карта не выдает свои секреты. Например, при использовании карт для подписи документов смарт-карта будет более безопасна, чем карта с магнитной полосой. Карта с магнитной полосой передает считывающему устройству функцию подписания документа, тем самым сообщая ему все секретные данные. В этом случае остается только надеяться на лучшее. Преступник с помощью устройства чтения может украсть шифр подписи. Смарт-карта же самостоятельно ставит подпись. Сканирующее устройство может загружать в карту для подписи подложные документы, но оно не получит шифр подписи.

Есть и другие, более тонкие различия. Смарт-карта позволяет опереться на некоторые основные правила выполнения действий. В принципе это можно использовать и в системе, которая обращается к базам данных, и для карт с магнитной полосой, но смарт-карты позволяют добиться лучшей реализации.

Известно, что смарт-карты распространены как платежное средство по всей Европе, но не в Туркменистане. Почему? Все объясняется особенностями телефонной связи. Система проверки туркменских карточек работает в режиме онлайн. Когда вы покупаете что-нибудь, продавец использует модем, чтобы убедиться в том, что ваша карточка действительна и вы платежеспособны. Двадцать лет назад эта система не могла бы работать ни в одной европейской стране. Плата за телефон была высока, многие магазины их даже не имели, а в Италии, например, их установки приходилось дожидаться год или два. Связь была дорогой и ненадежной. Создание онлайновой

системы в Европе было невыгодно, поэтому индустрия кредитных карт отдала предпочтение смарт-картам, позволявшим хоть как-то обезопасить сделки. Дело не в том, что смарт-карты защищены лучше, чем карты с магнитными полосами, просто туркменский способ борьбы с мошенничеством был менее практичным.

Моделируем угрозы и оценим риски пластиковых карт. Главные виды из преступлений против пластиковых карт это нарушение тайны частной жизни, вандализм и терроризм.

Нарушение тайны частной жизни происходит, когда кто-либо сообщает третьей стороне конфиденциальную информацию о некотором лице без его согласия. В зависимости от местного законодательства такие действия не везде считаются преступлением. Если разработчики пластиковых карт хотят, чтобы система распространилась по всему миру, имеет смысл составить перечень этих действий и не обращать на них внимания, если они считаются законными.

До тех пор, пока система не станет обладать средствами для предотвращения нарушения тайны частной жизни, банки будут иметь неограниченные возможности для получения информации о расходах клиентов. Этого можно избежать в некоторых случаях, если клиенты будут приобретать карты с фиксированной суммой денег на них, аналогично некоторым телефонным картам с предоплатой.

Продавец не сумеет непосредственно получить подобные сведения и узнать имя покупателя, однако с помощью других продавцов он может собрать информацию об использовании карты с известным ему идентификационным номером и, сопоставив данные, идентифицировать ее владельца.

Наконец, следует помнить и о возможности подслушивания: люди, вовсе не участвующие во взаиморасчетах, могут подслушивать и собирать информацию.

Следующий вид преступлений, вызывающих беспокойство, включает вандализм и терроризм. Эти правонарушения в первую очередь направлены против системы в целом, хотя могут совершаться и против отдельных владельцев карт, продавцов и банков. Главная цель таких преступлений –помешать правильному функционированию системы. То, что называется атаками, направленными на отказ в обслуживании, в этом случае может оказаться весьма любопытно.

Давайте рассмотрим в использовании системы для совершения преступлений, то есть о нарушениях закона с ее помощью. До сих пор мы рассматривали лишь возможность отмывания денег, но не менее заманчиво обсудить возможности других противозаконных действий.

Некоторые люди получают банковские карточки под вымышленными именами, но нетрудно склонить кого-либо к тому, чтобы он использовал свое настоящее имя. Несомненно, в мире найдется много желающих открыть банковский счет, который, как они понимают, будет контролироваться другими людьми и использоваться для отмывания денег, если им предложат несколько тысяч долларов. Если на такие карточки положить деньги, их можно использовать как компактное платежное средство, и не существует очевидного способа воспрепятствовать этому.

Обратите внимание на то, что решение вопросов морали и законности в этой сфере далеко не очевидно. Требования о предоставлении финансовой отчетности в государственные органы США и Великобритании. России, Белоруссии и Туркменистана могут причинять некоторые неприятности гражданам, но власти редко злоупотребляют этим. Во многих других странах, таких как Китай, Турция. Мексика или Сирия, дело принимает совсем другой оборот. Последнее обстоятельство чревато политическими и юридическими проблемами для тех компаний, которые

обязаны предоставлять такие сведения, и способно привести к большему распространению мошенничества в этих странах.

Сущность информационной безопасности заключается в формировании активной защиты в отношении приоритетных интересов, связанных с использованием информационных ресурсов, направленной на создание условий для нормального развития общества и экономики. Обеспечение информационной безопасности представляет собой комплексную задачу, что обусловлено сложностью и многоплановостью информационной среды. Если говорить кратко, то существует определенное различие между картами с магнитными полосами и смарт-картами, но насколько это важно зависит от их применения. Сопротивление вторжению в смарт-карту при достаточных затратах времени и средств, всегда может быть преодолено, поэтому не имеет смысла создавать систему, безопасность которой основана на средствах сопротивления вторжению. Большинство людей не способны взломать смарт-карту, потому что она более защищена. Но обе карты создавались в предположении, что считывающему устройству следует доверять, поэтому они могут пострадать от действия устройств, используемых злоумышленниками. И все же, смарт-карта лучше защищена от взлома. И до тех пор, пока сопротивление вторжению не преодолено, смарт-карта надежно хранит свои секреты.

Список использованных источников

1. Президент Туркменистана утвердил Концепцию цифровой образовательной системы. [Электронный ресурс]. – Режим доступа: https://turkmenistan.gov.tm/ – Дата доступа: 15.09.2017.

2. Смирнов А.Б. Кибербезопасность: основные принципы и методы защиты информации. – М.: Издательство НТЦ "Инфра-М", 2018.

3. Туркменский институт информационных технологий, "Отчет о состоянии проектного управления в IT-сфере", 2018.

References

1 The President of Turkmenistan approved the Concept of the digital educational system. [electronic resource]. – Access mode: https://turkmenistan.gov.tm / – Access date: 09/15/2017.

2. Smirnov A.B. Cybersecurity: basic principles and methods of information protection. Moscow: NTC Infra-M Publishing House, 2018.

3. Turkmen Institute of Information Technologies, "Report on the state of project management in the IT sphere", 2018.

Сведения об авторах

Аманова О.Г., преподаватель кафедры информационные технологи, Государственный энергетический институт Туркменистана, begob3824@gmail.com.
Гелдиев А.А., старший преподаватель кафедры общественных наук, Государственный энергетический институт Туркменистана, begob3824@gmail.com.
Мухамметныязов А.А., преподаватель кафедры электроэнергетических систем, Государственный энергетический институт Туркменистана, akmammetmuhammedow3@gmail.com.

Information about the authors

Amanova O.G., Lecturer, Department of Information Technology, State Energy Institute of Turkmenistan, begob3824@gmail.com.
Geldiyev A.A., Senior Lecturer, Department of Social Sciences, State Energy Institute of Turkmenistan, begob3824@gmail.com.
Muhammetniyazov A.A., Lecturer, Department of Electric Power Systems, State Energy Institute of Turkmenistan, akmammetmuhammedow3@gmail.com.

УДК 004.934.2

ПРОВЕРКА МУЗЫКАЛЬНЫХ ФАЙЛОВ НА НАЛИЧИЕ СКРЫТЫХ РЕЧЕВЫХ СООБЩЕНИЙ ПРИ ПОМОЩИ СПЕКТРОГРАММ

А.М. Асиненко, В.М. Алефиренко
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь

Аннотация. Представлен метод стеганофонии, использующий спектрограммы для проверки факта скрытия речевой информации в музыкальном файле. Алгоритм предполагает преобразование обоих аудиофайлов (речевого и музыкального) в спектрограммы, визуализирующие их частотный состав. Далее, речевая информация кодируется и встраивается в спектрограмму музыкального файла, например, путем модуляции амплитуды или частоты отдельных частотных составляющих. Полученная модифицированная спектрограмма затем обратно преобразуется в аудиосигнал. Для обнаружения скрытого сообщения сравниваются спектрограммы исходного музыкального файла и модифицированного. Различия, выявленные с помощью специального программного обеспечения, укажут на наличие скрытого сообщения. Программное обеспечение включает в себя модули для преобразования аудио в спектрограммы, алгоритмы встраивания/извлечения данных, и инструменты для анализа и сравнения спектрограмм. Эффективность метода зависит от выбранного алгоритма встраивания и устойчивости к шуму и искажениям.
Ключевые слова: спектрограмма; безопасность связи; защита информации; речевая информация; речевые файлы; музыкальные файлы; скрытая информация; обработка сигналов; преобразования Фурье; спектр сигналов.

CHECKING MUSIC FILES FOR HIDDEN ONES SPEECH MESSAGES USING SPECTROGRAMS

A. M. Asinenko, V. M. Alefirenko
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. A steganophony method is presented that uses spectrograms to verify that speech information is hidden in a music file. The algorithm involves converting both audio files (speech and music) into spectrograms that visualize their frequency composition. Further, speech information is encoded and embedded in the spectrogram of a music file, for example, by modulating the amplitude or frequency of individual frequency components. The resulting modified spectrogram is then converted back into an audio signal. To detect a hidden message, the spectrograms of the original music file and the modified one are compared. Differences detected using special software will indicate the presence of a hidden message. The software includes modules for converting audio into spectrograms, algorithms for embedding/extracting data, and tools for analyzing and comparing spectrograms. The effectiveness of the method depends on the chosen embedding algorithm and its resistance to noise and distortion.
Keywords: spectrogram; communication security; information protection; speech information; speech files; music files; hidden information; signal processing; Fourier transform; signal spectrum.

Введение

Значительная часть передаваемой по общедоступным каналам связи информации приходится на долю речевых сообщений. Такое положение дел сохранится и в будущем, поскольку такому универсальному инструменту человеческого общения как речь, обладающему уникальными признаками эффекта присутствия, эмоциональной окраски, аутентификации, информационной избыточности и другими, присущими только данному коммуникативному (переговорному) процессу, трудно найти какую-либо эквивалентную замену во многих системах связи и передачи информации. Вот почему задачи защиты речевой информации занимают одно из ведущих мест в решении общей проблемы информационной безопасности [1].

Для защиты информации могут использоваться специальные программные средства, применяющие в своей основе метод, основанный на использовании спектрограмм.

Основная часть

Спектрограмма – это визуальный способ представления уровня или «громкости» сигнала во времени на различных частотах, присутствующих в форме волны. Для вычисления спектрограммы дискретного сигнала его разбивают на сегменты. Для каждого сегмента находят его спектр в виде коэффициентов дискретного преобразования Фурье. Набор спектров и образует спектрограмму (рис. 1).

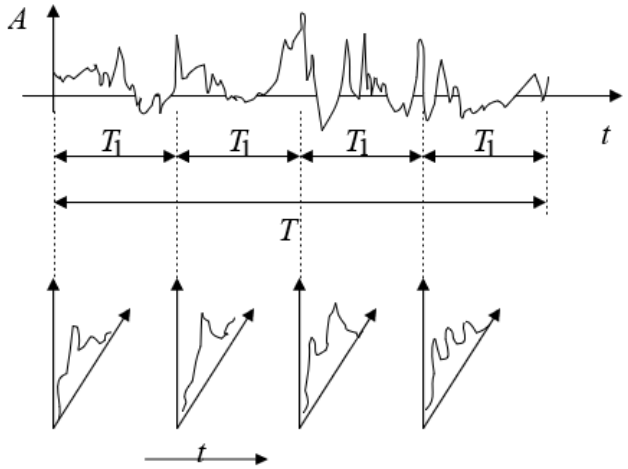


Рис. 1. Спектрограмма
Fig. 1. Spectrogram

В настоящее время существует большое количество хороших программных цифровых анализаторов и редакторов аудио сигналов, предназначенных для визуального анализа звуковых сигналов во временной (осциллограммы, графики уровня мощности сигнала и др.) и, конечно, частотной (сонограммы, кепстры и др.) областях. Среди импортных программных продуктов такого рода следует отметить Cool Edit Pro 1.2, Dart Pro, Sound Forge, Wave Lab, Wave Studio, Ocenaudio и др., среди отечественных – «SIS 5.2», «Win-Аудио», «Лазурь», Signal Quick Viewer 2 (SQV2), Signal Viewer (SV) и др. В ряде звуковых редакторов имеется возможность производить некоторые виды обработки аудио сигнала, которые можно применить и для решения ограниченного числа задач обеспечения безопасности речевых сигналов посредством компьютерных технологий [2]. Для проведения исследований использовалось программное средство Ocenaudio.

Возьмем музыкальный файл и запишем речевое сообщение, которое будет встроено в этот файл. В качестве исходного файла было взято музыкальное произведение длительностью около 3 минут, спектрограмма которого показана на рисунке 2. Речевое сообщение представляло собой короткую фразу произношения подряд нескольких цифр (цифровой пароль), спектрограмма которого показана на рисунке 3. На спектрограммах темным (черным) цветом показано отсутствие сигнала, а оттенками красного цвета – его наличие на соответствующих частотах по вертикальной оси.

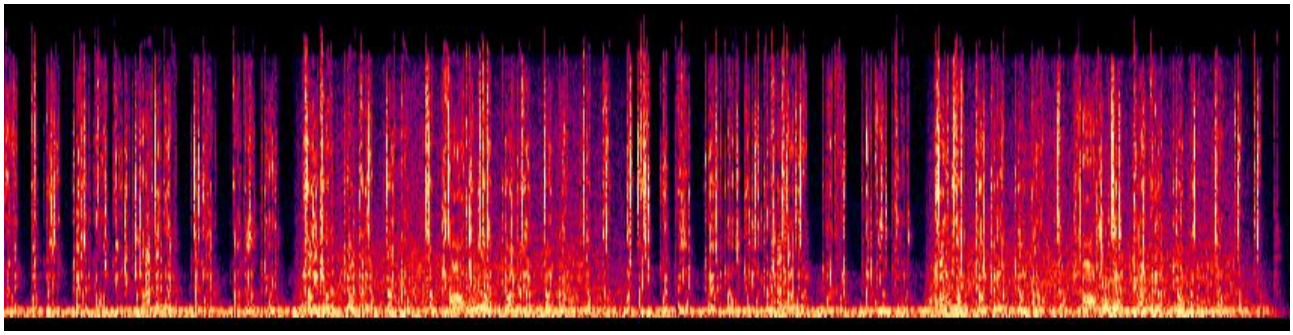


Рис. 2. Спектрограмма музыкального файла
Fig. 2. The spectrogram of the music file

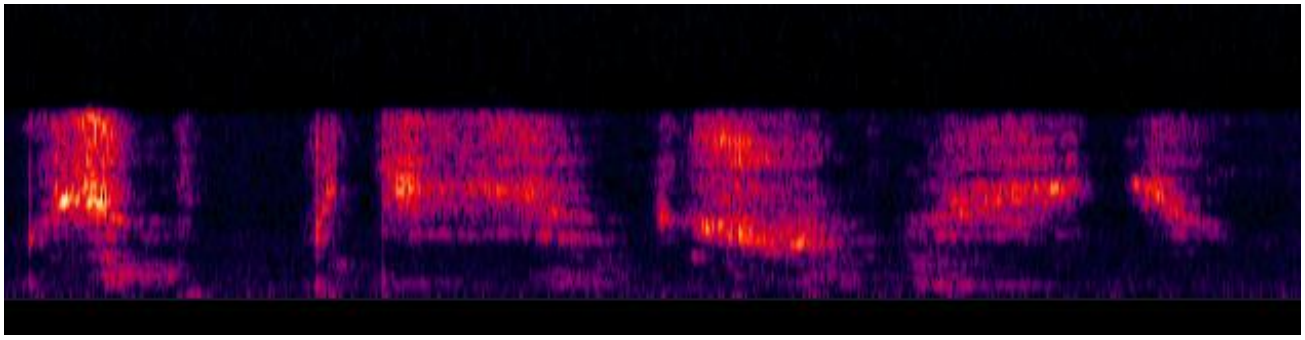


Рис. 3. Спектрограмма встраиваемого речевого файла
Fig. 3. Spectrogram of the embedded speech file

При объединении двух файлов в один получается спектрограмма, представленная на рис. 4. При сравнении исходной спектрограммы на рис. 2 и полученной спектрограммы на рис. 4 можно заметить небольшие различия на нижних частотах (выделены зеленым прямоугольником в левой нижней части), что свидетельствует о наличии скрытого сообщения. При прослушивании совмещенной спектрограммы различия не обнаруживаются.

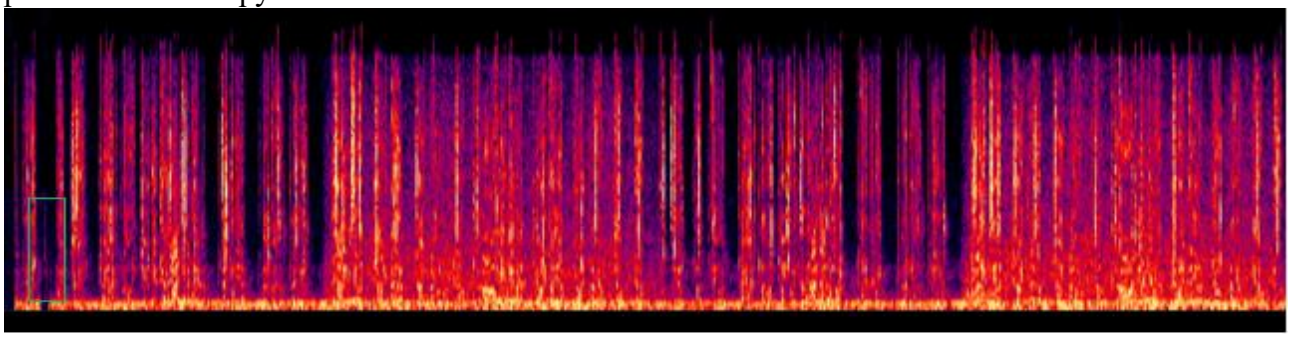


Рис. 4. Спектрограмма совмещенных звуковых файлов
Fig. 4. Spectrogram of combined audio files

Заключение

Прослушав музыкальный файл со скрытым сообщением, можно не заметить различия, отображенные на спектрограммах. Поэтому использование специальных программных средств позволяет определять наличие в различных файлах, в том числе музыкальных, скрытого сообщения.

Список использованных источников

1. Ахмад Х. М., Жирков В. Ф. (2007) *Введение в цифровую обработку речевых сигналов: учеб. пособие.* Издательство Владимирского государственного университета.
2. Асиненко, А. М. (2024) Использование спектрограмм для защиты речевой информации. *Электронные системы и технологии: сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР*, 46–48.

References

1. Akhmad Kh. M., Zhirkov V. F. (2007*) Introduction to digital processing of speech signals: textbook stipend*. Vladimir State University Publishing House (in Russian).
2. Asinenko, A.M. (2024) The use of spectrograms to protect speech information. *Electronic systems and Technologies: proceedings of the 60th Scientific Conference of graduate students, undergraduates and students of BSUIR*, 46-48 (in Russian).

Сведения об авторах

Асиненко А.М., ассистент кафедры электронной техники и технологии, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», asinenko2016@mail.ru.
Алефиренко В.М., канд. техн. наук, доц., доцент кафедры информационно-компьютерных систем, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alefirenko@bsuir.by.

Information about the authors

Asinenko A.M., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", asinenko2016@mail.ru.
Alefirenko V.M., Cand. Sci. (Tech.), Associate Professor, Associate Professor of Information and Computer-Aided Systems Design Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alefirenko@bsuir.by.

УДК 004.021

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

К.С. Барило, С.Н. Нестеренков, Е.В. Бегляк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Статья рассматривает криптографические методы защиты информации в сфере электронного документооборота. Основное внимание акцентируется на популярных криптографических методах защиты информации, таких как симметричное и асимметричное шифрование и хэширование в контексте обеспечения безопасности и целостности данных при обмене информацией через открытые каналы, такие как интернет. Описываются способы применения методов криптографической защиты информации для обеспечения конфиденциальности, целостности и доступности электронных документов. Также в данной статье уделяется внимание принципу работы и использованию цифровых подписей для обеспечения целостности данных и защиты авторских прав. В статье будут рассмотрены проблемы и ограничения современной криптографии. Также обсуждаются вызовы и перспективы развития криптографических технологий в сфере электронного документооборота, что делает материал актуальным для специалистов и организаций, работающих с электронными данными.
Ключевые слова: криптография; защита информации; электронный документооборот; безопасность данных; конфиденциальность; целостность; доступность; цифровизация; методы шифрования; доверие к системам.

CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION IN THE FIELD OF ELECTRONIC DOCUMENT MANAGEMENT

K. Barilo, S. Nesterenkov, E. Begliak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article examines cryptographic methods of information protection in electronic document management, focusing on symmetric and asymmetric encryption and hashing. Their applications for ensuring confidentiality, integrity, and accessibility of documents, as well as the importance of digital signatures, are described. The challenges and prospects for the development of cryptographic technologies in this area are also discussed, which makes the material relevant for specialists and organizations working with electronic data.
Keywords: cryptography, information security, electronic document management, data security, confidentiality, integrity, accessibility, digitalization, encryption methods, trust in systems.

Введение

В современном мире, где цифровизация проникает во все сферы жизни, электронный документооборот становится частью бизнес-процессов и взаимодействия между государственными органами и гражданами. С ростом объемов обрабатываемых данных возникают серьезные угрозы безопасности информации. Криптографические методы защиты являются ключевым инструментом для обеспечения конфиденциальности, целостности и доступности электронных документов.

Криптография, как наука о защищенной передаче и хранении информации, предоставляет мощные средства для защиты данных от несанкционированного доступа и изменений [1]. В данной статье будут рассмотрены основные криптографические методы, используемые для защиты информации в сфере электронного документооборота, а также их влияние на безопасность и эффективность процессов обмена документами.

Основная часть

Основными методами криптографической защиты информации являются:

1. Симметричное шифрование. Симметричное шифрование предполагает использование одного и того же ключа для шифрования и расшифровки данных. Данный метод защиты информации обеспечивает высокую скорость обработки данных и может быть применен для обработки больших объемов информации. Основным ограничением симметричного шифрования является необходимость безопасной передачи ключа между сторонами.

2. Ассиметричное шифрование. Асимметричное шифрование использует пару ключей: открытый и закрытый. Открытый ключ доступен всем участникам передачи данных, а закрытый хранится в секрете. Асимметричное шифрование обеспечивает более высокий уровень безопасности. Данный метод используется для создания цифровых подписей.

3. Хэширование. Хэширование – это процесс преобразования исходных данных в фиксированное значение, называемое хэшем. Хэширование позволяет проверить целостность данных: если изменится хотя бы один бит исходной информации, хэш также изменится. Хэширование широко применяется для хранения паролей и проверки целостности документов.

4. Цифровая подпись. Цифровая подпись используется для аутентификации и подтверждения целостности данных. Данный метод использует ассиметричное

шифрование так, что цифровая подпись создается с помощью закрытого ключа, а проверяется с помощью открытого ключа.

5. Протоколы обмена ключами. Протоколы обмена ключами обеспечивают безопасный обмен криптографическими ключами между сторонами. Примером такого протокола может быть протокол Диффи-Хеллмана [2].

6. Защита на основе атрибутов (Attribute-Based Encryption). Данный способ криптографической защиты информации предполагает шифрование данных с учетом определенных атрибутов, что обеспечивает гибкий доступ к информации.

7. Потоковое шифрование. Данный метод шифрования основан на шифровании данных по одному биту или байту за раз, что позволяет эффективно обрабатывать большие объемы данных. Примерами алгоритмов потокового шифрования являются алгоритмы RC4 и Salsa20 [3].

8. Блочное шифрование. При блочном шифровании данные разделяются на блоки фиксированного размера, после чего каждый блок шифруется отдельно. Примерами алгоритмов блочного шифрования являются алгоритмы AES и Blowfish [3].

9. Комбинированные методы шифрования. Приведенные выше методы могут использоваться в различных комбинациях для обеспечения надежной защиты информации в электронном документообороте.

Шифрование данных предотвращает их перехват и доступ к ним третьих лиц, что особенно важно в условиях передачи данных по открытым каналам связи, таким как интернет.

Хэширование используется для проверки целостности данных, что позволяет обнаружить любые несанкционированные изменения. Данный метод защиты информации активно применяется при хранении пользовательских данных и электронных документов на серверах.

Цифровые подписи, основанные на асимметричном шифровании, позволяют подтвердить авторство и целостность документов [5]. Подтверждение авторства и целостности электронного документа критически важно в юридической и финансовой сферах, где подделка документа может иметь серьезные последствия. Цифровая подпись обеспечивает юридическую значимость электронного документа, что делает его равнозначным бумажному.

Криптографические методы защиты информации также используются для защиты персональных данных в соответствии с законодательными нормами, такими как GDPR. Соблюдение законодательных норм позволяет организациям не только соблюдать правовые требования, но и укреплять доверие клиентов к своим услугам.

Одним из наиболее перспективных направлений развития криптографии является квантовая криптография. Квантовая криптография – направление криптографии, основанное на применении принципов квантовой механики для защиты информации. Квантовая криптография предлагает новые методы защиты, такие как квантовая распределенная ключевая система (QKD) [2]. Квантовая криптография в перспективе способна обеспечить абсолютную безопасность передачи информации.

Несмотря на значительные преимущества криптографических методов защиты информации, существуют сложности реализации безопасности. Примером сложности является обеспечение безопасной передачи ключа для симметричного шифрования по открытым каналам, таким как интернет. Следует учитывать, что с развитием технологий возникают новые угрозы безопасности, требующие постоянного обновления методов защиты.

Перспективы развития криптографических технологий в сфере электронного документооборота связаны с внедрением квантовой криптографии и развитием блокчейн-технологий [5], что обеспечит еще более высокий уровень безопасности.

Заключение

Криптографические методы защиты информации являются основным методом обеспечения безопасности электронного документооборота. Применение криптографии позволяет защитить данные от несанкционированного доступа и изменений, а также повысить доверие к электронным системам. В условиях цифровизации и роста объемов информации необходимость в эффективных методах защиты становится все более актуальной.

Дальнейшее развитие криптографических технологий, таких как квантовая криптография и технологии распределенного реестра, будет способствовать повышению уровня защищенности электронных документов. Исследования в этой области позволят создавать более надежные криптографические алгоритмы, устойчивые к современным угрозам.

Список использованных источников

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC.
3. Diffie, W., & Landau, S. (2007). Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press.
4. Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

References

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC.
3. Diffie, W., & Landau, S. (2007). Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press.
4. Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Сведения об авторах

Барило К.С., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kostabarilo12@gmail.com.
Нестеренков С.Н., кандидат технических наук, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.nesterenkov@bsuir.by.
Бегляк Е.В., инженер-программист 1 категории отдела сетевых технологий ЦИИР БГУИР, katarina@bsuir.by.

Information about the authors

Barilo K., student of the Department of Electronic Computing Machines at BSUIR, kostabarilo12@gmail.com.
Nesterenkov S., Candidate of Technical Sciences, Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.nesterenkov@bsuir.by.
Begliak E., software engineer of the 1st category of the Department of Network Technologies of CIID BSUIR, katarina@bsuir.by.

УДК 004.056.53

ПРИМЕНЕНИЕ МНОГОПОРТОВОГО S-ПАРАМЕТРИЧЕСКОГО АНАЛИЗА В РЕВЕРС-ИНЖИНИРИНГЕ ИНТЕГРАЛЬНЫХ СХЕМ ДЛЯ ДЕТЕКТИРОВАНИЯ СКРЫТЫХ ФУНКЦИИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ И АНОМАЛИЙ В ПЕРЕДАЧЕ СИГНАЛОВ

А.Б. Батыргалиев, А.А. Молганов
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан

Аннотация. Процесс проектирования интегральных микросхем в нынешнее время сопряжен с определенными технологическими нормами суть которых заключается в уменьшении подаваемой тока, уменьшении расстояния между структурными элементами и увеличения вычислительных мощностей на единицу площади. В связи с этим проведение инженерно-технического анализа на предмет наличия недекларированных возможностей представляется огромной проблемой как с технической точки зрения, так и с юридической – ввиду отсутствия конструкторской документации на интегральную микросхему. Интегральные микросхемы предназначенные для передачи информации с помощью радиочастотных структур имеют особое топологическое строение и поэтому реверс-инжиниринг данных микросхем затруднен из-за наличия фильтров и других помех блокирующих частей. Применение многопортового *S*-параметрического анализа позволяет провести топологический анализ скрытых цепей и портов, определить скрытые режимы работы и паразитных излучений.
Ключевые слова: интегральная микросхема; S-параметр; техническая защита информации; реверс-инжиниринг; печатная плата; инвазивные методы анализа; неинвазивные методы анализа.

APPLICATION OF MULTIPORT S-PARAMETRIC ANALYSIS IN REVERSE ENGINEERING OF INTEGRATED CIRCUITS TO DETECT HIDDEN FUNCTIONAL CAPABILITIES AND ANOMALIES IN SIGNAL TRANSMISSION

A.B. Batyrgaliev, A.A. Molganov
Satbayev Univeristy, Almaty, Republic of Kazakhstan

Abstract. The process of designing integrated circuits at the present time is associated with certain technological standards, the essence of which is to reduce the supplied current, reduce the distance between structural elements and increase computing power per unit area. In this regard, conducting an engineering and technical analysis for undeclared capabilities is a huge problem both from a technical point of view and from a legal one, due to the lack of design documentation for an integrated circuit. Integrated circuits designed to transmit information using radio frequency structures have a special topological structure, and therefore reverse engineering of these chips is difficult due to the presence of filters and other interference from blocking parts. The use of multiport *S*-parametric analysis allows for topological analysis of hidden circuits and ports, to determine hidden modes of operation and spurious emissions.
Keywords: integrated circuit; S-parameter; technical information protection; reverse engineering; printed circuit board; invasive methods of analysis; non-invasive methods of analysis.

Введение

Высокоскоростные радиочастотные интегральные схемы имеют внутреннее топологическое строение в виде много сегментных уровней с абсолютной уровнем металлизации и проявления в процессе производства, в следствие чего становится затруднительно с технической точки зрения провести комплексный и системный анализ на предмет наличия недекларированных возможностей интегральных микросхем с высокой степенью плотности. Анализ с помощью S-параметров позволяет исследовать характеристики передаваемого сигнала между интегральными микросхемами, расположенными на печатной плате, а также выявить паразитные связи между внутренними элементами и дать комплексную оценку влияния различных элементов на преднамеренное или умышленное искажение данных. Изучение

коэффициентов отражения и передачи сигнала помогает на этапе технической экспертизы или сертификации устройства, позволяет оценить потенциальные аппаратные закладки и недекларированные интерфейсы внутри интегральной микросхемы.

Основная часть

Современные системы на кристалле (SoC), в основе своей представляют несколько интегральных микросхем, объединенных высокоскоростным соединением с высокой степенью топологии, и включает в себя сложные многослойные структуры, состоящие из передатчиков, мостов, сетей и приемников. Для оценки характеристик передачи сигнала в таких системах широко применяется анализ S-параметров, который позволяет исследовать коэффициенты отражения и передачи на различных участках сигнальной передачи [1].

В эпоху глобализации и роста экспортного производства аппаратного обеспечения критической информационной инфраструктуры, вопросы информационной безопасности и аппаратного контроля за такими системами, становятся все более актуальными в связи с множественными случаями внедрения аппаратных закладок на этапе производства и упаковки интегральных микросхем. Таким образом, производители интегральных микросхем могут намеренно или якобы случайно оставлять дополнительные функциональные возможности, которые не задокументированы и нереализованны в технической документации или системном программном обеспечении, но могут влиять на работу системы с точки зрения информационной безопасности. Одним из подходов к выявлению таких возможностей является исследование характеристик рассеяния сигнала с помощью S-параметрического анализа. Этот метод позволяет обнаружить паразитные связи, неявные пути передачи данных и изменения в отклике системы, которые могут свидетельствовать о наличии аппаратных закладок или скрытых каналов связи внутри интегральной микросхемы или определенного участка топологии печатной платы.

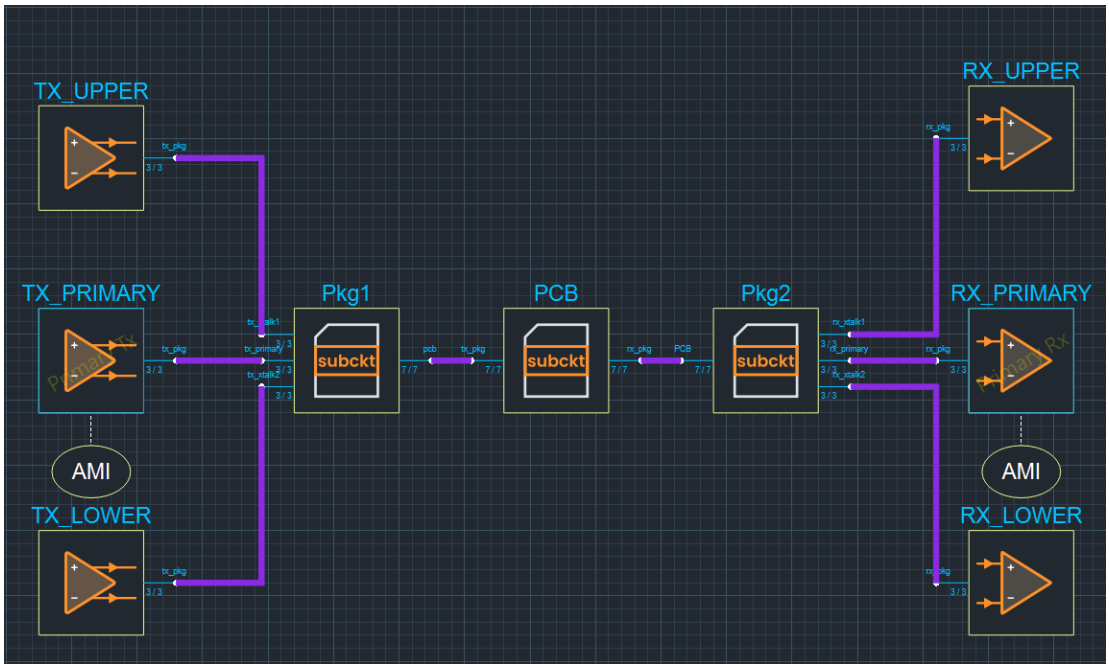


Рис. 1. Пример симуляционного стенда для анализа воздействия скрытых каналов связи
Fig. 1. Example of a simulation stand for analyzing the effects of hidden communication channels

На примере симуляционного виртуального стенда, выполненного в системе автоматизированного анализа Cadence Topology Workbench 2024.010, будет продемонстрировано применение многопортового S-параметрического анализа для выявления недекларированных возможностей на участке топологии печатной платы с двумя интегральными микросхемами [4].

На представленном выше изображении показана структурная схема передачи высокоскоростного сигнала через систему, состоящую из множества последовательно соединенных элементов между собой. Передающие устройства интегральной микросхемы №1 – TX_UPPER, TX_PRIMARY, TX_LOWER, генерируют сигнал, который проходит через соединительный слой интегральной микросхемы (Pkg1), затем передается на дорожку которая располагается на топологии печатной платы (PCB) и затем поступает в соединительный слой интегральной микросхемы №2 (Pkg2), после чего достигает приемных узлов – RX_UPPER, RX_PRIMARY и RX_LOWER.

Для обеспечения корректности симуляции и получения достоверных данных, передача сигнала в процессе симуляции, применяется AMI-модели (Algorithmic Modeling Interface), которые выполняют адаптивную обработку сигнала и компенсируют возникающие искажения путем фильтрации и различных преобразований сигнала. При этом на каждом этапе передачи, сигнал может подвергаться различным воздействиям, таким как потери, перекрестные наводки, отражения и паразитные резонансы. Вследствие этих факторов возможны изменения в характеристиках передачи, которые могут быть выявлены с помощью анализа *S*-параметров.

Signal Name	Data Rate (Gbps)	Baud Rate (GBaudPS)	Stimulus Pattern	Stimulus Offset (ns)	Leading Bits	Tx IO Model	Tx Jitter & Noise	Status
*	*	*	*	*	*	*	*	*
▼ ☑ Signal	5	5	PRBS(seed: 1, poly: 7)	0				
☑ pos	5	5	PRBS(seed: 1, poly: 7)	0		nmos_diff_tx		Signal
☑ neg	5	5	PRBS(seed: 1, poly: 7)	0		nmos_diff_tx		Signal

Рис. 2. Характеристики симулируемого сигнала
Fig. 2. Characteristics of the simulated signal

Для корректной симуляции, необходимо также задать физические величины и другие данные со следующими характеристиками:

1. *Передаваемый сигнал*:

– используется дифференциальный сигнал, состоящий из двух компонентов: положительного (pos) и отрицательного (neg);

– передача осуществляется со скоростью 5 Гбит/с (битрейт) и аналогичной символьной скоростью 5 Гбод/с (NRZ-кодирование).

2. *Структура передаваемых данных*:

– для моделирования используется псевдослучайная битовая последовательность (PRBS) с полиномом 7-го порядка (poly: 7, seed: 1). PRBS применяется для имитации реального трафика и оценки качества передачи сигнала;

– смещение сигнала во времени отсутствует (Stimulus Offset = 0 нс), что означает, что передача начинается без задержек.

3. *Модель передатчика*:

– передатчик использует NMOS-дифференциальный драйвер (Tx IO Model = nmos_diff_tx), что стандартизировано ввиду использования идентичной модели драйвера в современных высокоскоростных интерфейсах – PCIe, USB, SerDes.

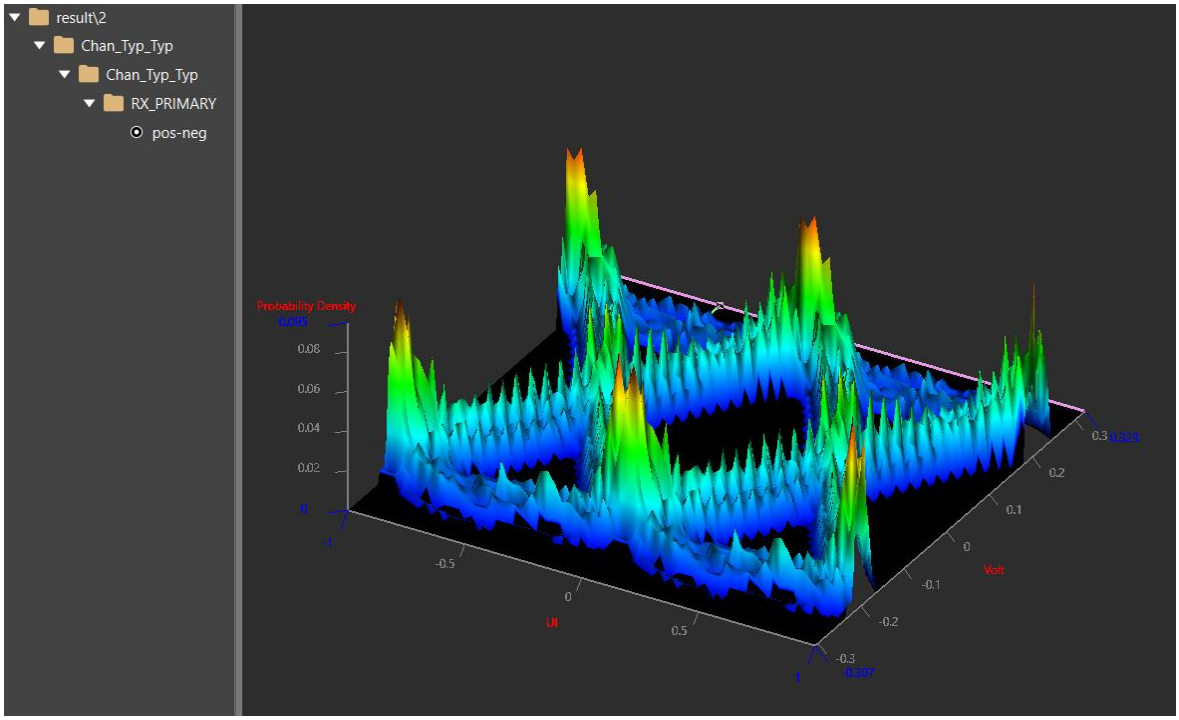


Рис. 3. Характеристики симулируемого сигнала
Fig. 3. Characteristics of the simulated signal

На представленном изображении показана трехмерная визуализация вероятностного распределения дифференциального сигнала, полученного в процессе моделирования высокоскоростного канала передачи данных. График демонстрирует зависимость плотности вероятности (Probability Density) от напряжения (Volt) и временного интервала (UI – Unit Interval), что позволяет оценить качество передаваемого сигнала от одной интегральной микросхемы к другой [5].

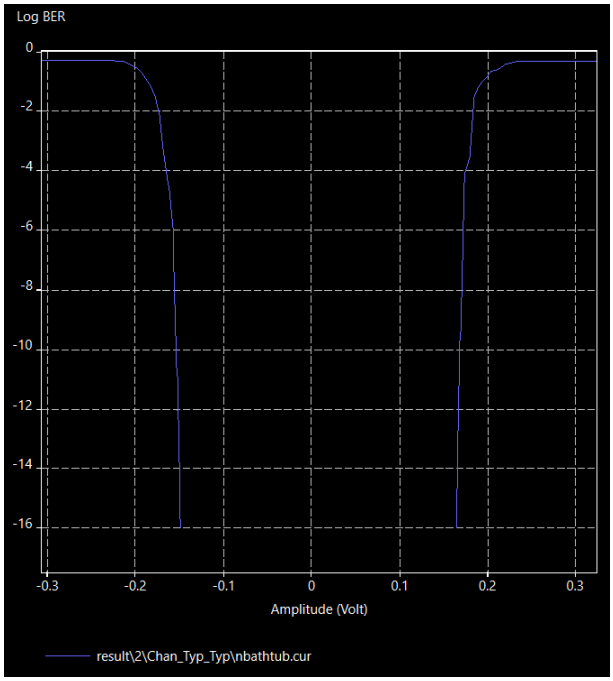


Рис. 4. График сигнала с помехами в приемнике интегральной микросхемы №2
Fig. 4. Graph of the signal with interference in the receiver of integrated circuit No. 2

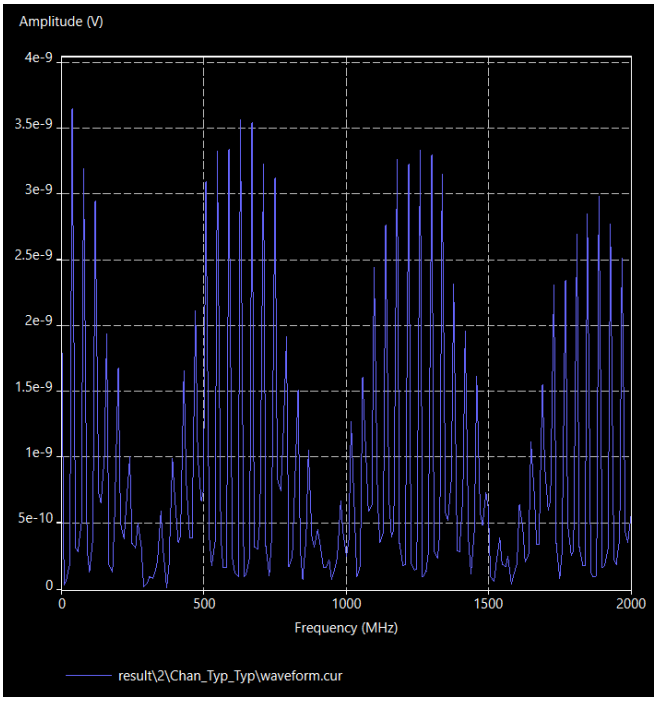


Рис. 5. График сигнала с помехами в приемнике интегральной микросхемы №2
Fig. 5. Graph of the signal with interference in the receiver of integrated circuit No. 2

Представленные графики с результатами симуляции, свидетельствует о наличии двух областей с высокой вероятностью ошибок (на краях амплитудного диапазона) и центральной зоны с минимальным уровнем BER-значения. Это типично для систем с разделением сигналов на дискретные уровни, таких как двоичные или многоуровневые модуляции (NRZ или PAM-4 модуляция). Минимизация ошибок в центральной зоне подтверждает эффективность используемых схем синхронизации, эквализации и кодирования коррекции ошибок. В то же время, резкие границы областей ошибок могут указывать на чувствительность системы к внешним помехам, фазовому шуму или дрожанию сигнала зависящих от внешнего источника генерации электромагнитных излучений [3].

Полученные результаты позволяют сделать несколько выводов. Во-первых, центральная область графика является ключевой для надежной передачи данных, и любые изменения параметров системы должны стремиться к расширению этой зоны. Во-вторых, высокая плотность ошибок на краях амплитудного диапазона указывает на необходимость оптимизации схем передачи и приема, в частности, улучшения тактового восстановления и фильтрации сигнала с помощью блоков ADC/DAC и умножителей/делителей. В-третьих, анализ формы кривой может помочь в калибровке параметров передатчика и приемника для достижения оптимального соотношения между мощностью сигнала и вероятностью ошибки [2].

Дополнительно, выявленные аномалии в распределении сигнальных ошибок, неожиданные искажения сигнала или нехарактерное поведение системы при определенных режимах работы могут указывать на наличие скрытых аппаратных закладок. Поэтому анализ кривых BER-значений позволяет выявить потенциальные отклонения, которые могут свидетельствовать о попытках несанкционированного вмешательства в работу интегральной микросхемы или системы на кристалле.

В заключении, можно сделать вывод что исследование представленных характеристик сигнала подтверждает важность использования логарифмического анализа BER-значений для проектирования, отладки и исследования цифровых систем

передачи данных. Данный вид анализа позволяет выявлять потенциальные проблемы на этапе исследования интегральной микросхемы на предмет наличия недекларированных возможностей.

Список использованных источников

1. Al-Meer, A., & Al-Kuwari, S. (2023). Physical Unclonable Functions (PUF) for IoT Devices. ACM Computing Surveys.
2. Liang, W., Xie, S., Zhang, D., Li, X., & Li, K.-C. (2022). A Mutual Security Authentication Method for RFID-PUF Circuit Based on Deep Learning. ACM Transactions on Internet Technology.
3. Nagata, M., Miki, T., & Niura, N. (2022). Physical Attack Protection Techniques for IC Chip Level Hardware Security. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems.
4. Hemavathy, S., & Bhaaskaran, V. S. K. (2023). Arbiter PUF - A Review of Design, Composition, and Security Aspects. IEEE Access.
5. Khichel, D., & Moradi, A. (2022). Low-Latency Hardware Private Circuits. Proceedings of the ACM Conference on Computer and Communications Security

References

1. Al-Meer, A., & Al-Kuwari, S. (2023). Physical Unclonable Functions (PUF) for IoT Devices. ACM Computing Surveys.
2. Liang, W., Xie, S., Zhang, D., Li, X., & Li, K.-C. (2022). A Mutual Security Authentication Method for RFID-PUF Circuit Based on Deep Learning. ACM Transactions on Internet Technology.
3. Nagata, M., Miki, T., & Niura, N. (2022). Physical Attack Protection Techniques for IC Chip Level Hardware Security. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems.
4. Hemavathy, S., & Bhaaskaran, V. S. K. (2023). Arbiter PUF - A Review of Design, Composition, and Security Aspects. IEEE Access.
5. Khichel, D., & Moradi, A. (2022). Low-Latency Hardware Private Circuits. Proceedings of the ACM Conference on Computer and Communications Security

Сведения об авторах

Батыргалиев А.Б., Доктор Ph.D., ассоциированный процессор, Кафедра Кибербезопасности, обработки и хранения информации, Институт автоматики и информационных технологий, Казахский национальный исследовательский технический университет имени К. И. Сатпаева, a.batyrgaliev@su.edu.kz
Молганов А.А., магистрант ОП «Комплексное обеспечение информационной безопасности», Кафедра Кибербезопасности, обработки и хранения информации, Институт автоматики и информационных технологий, Казахский национальный исследовательский технический университет имени К. И. Сатпаева, a.molganov@su.edu.kz

Information about the authors

Batyrgaliev A.B., Ph.D., Associate Professor, Department of Cybersecurity, Information Processing and Storage, Institute of Automation and Information Technology, Satbayev University, a.batyrgaliev@su.edu.kz.
Molganov A.A., Master's student in the Department of Integrated Information Security, Department of Cybersecurity, Information Processing and Storage, Institute of Automation and Information Technology, Satbayev University, a.molganov@su.edu.kz.

УДК 004.056.53

ЭВОЛЮЦИЯ УГРОЗ И УЯЗВИМОСТЕЙ WEB-САЙТОВ

Р.А. Божко[1], Т.А. Пулко[2]
[1]*Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь*
[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

Аннотация. Уязвимости в безопасности всегда являются актуальной проблемой, на исследование которой администраторы веб-сайтов тратят много времени в целях обеспечения безопасности их работы. Эти уязвимости позволяют хакерам использовать, атаковать, проникать и влиять на данные веб-сайтов любых компаний. Для стабильной, бесперебойной и безопасной работы веб-сайта необходимо знать основную информацию об уязвимостях в безопасности онлайн-платформ.
Ключевые слова: безопасность веб-сайтов; уязвимость; защита информации; код; программное обеспечение; сканирование уязвимостей безопасности; инъекция; скриптинг; утечка данных; аутентификация.

EVOLUTION OF THREATS AND VULNERABILITIES OF WEB SITES

P.A. Bozhko[1], T.A. Pulko[2]
[1]*Educational Institution "Belarusian State Academy of Communications", Minsk, Belarus*
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Security vulnerabilities are always a pressing issue that website administrators spend a lot of time researching to ensure the security of their work. These vulnerabilities allow hackers to exploit, attack, penetrate and influence the data of websites of any companies. For stable, uninterrupted and secure operation of a website, it is necessary to know the basic information about security vulnerabilities of online platforms.
Keywords: website security; vulnerability; information protection; code; software; security vulnerability scanning; injection; scripting; data leakage; authentication.

Введение

С ростом числа интернет-пользователей и развитием цифровой экономики вопрос обеспечения безопасности онлайн-платформ становится все более актуальным. Уязвимости веб-сайтов могут привести к краже конфиденциальной информации, взлому сайта или другим серьезным проблемам, поэтому обнаружение и устранение уязвимостей есть важная задача для владельцев веб-сайтов и специалистов по информационной безопасности [1]. Обеспечение безопасности веб-сайтов является сложной задачей, требующей постоянного мониторинга и реагирования на уязвимости [2].

Основная часть

Уязвимость веб-сайта – это дефект или ошибка программного кода, неправильная конфигурация системы или какая-либо другая слабость веб-сайта, веб-приложения или его компонентов и процессов. Уязвимости веб- приложений позволяют злоумышленникам получить несанкционированный доступ к системам, процессам или важнейшим активам компаний [3]. Имея такой доступ, злоумышленники могут организовывать атаки, захватывать приложения, участвовать в повышении привилегий для кражи данных, вызывать масштабные сбои в работе служб и т. д. Любой элемент технологии будет содержать уязвимости [4]. Конечно, не существует никаких указаний на то, сколько уязвимостей может иметь каждый из них. Однако очень грубый метод

определения количества возможных уязвимостей основан на количестве строк кода. Другими словами, чем больше строк кода, тем больше количество возможных уязвимостей [5, 6]. Известно, что языки программирования позволяют быстро устранять уязвимости безопасности веб- приложений. Кроме того, имеются такие методы проверки уязвимостей сайта, как: метод локальной проверки (обнаружени уязвимостей путем непосредственной проверки исходного кода устройства и приложения, проверки и чтения библиотек (двоичных), таких как файлы .exe и т.д.), метод удаленной проверки (удаленное обнаружение уязвимостей через сетевые протоколы, суть которого заключается в удаленном обнаружении уязвимостей). [7].

К основным уязвимостям относятся: инъекции (уязвимости, возникающие вследствие передачи не проверенных данных, которые пользователь ввел интерпретатору в целях выполнения: LDAP, XXE, OS и SQL); уязвимость XSS (Cross-Site Scripting или XSS функционирует в JavaScript -считается не опасной для сервера, однако представляет опасность для пользователя); уязвимости CSRF (атака Cross-Site Request Forgery или CSRF предоставляет злоумышленнику возможность вынудить браузер жертвы осуществить отправку в уязвимое приложение определенного HTTP запроса); применение элементов с уязвимостями (такие элементы, как фреймворки, библиотеки и прочие программные модули функционируют с такими же полномочиями, как и приложение); незащищенные API (большая часть современных приложений зачастую содержат в себе веб-приложения клиентов, а также богатые API интерфейсы, которые доступны из мобильных приложений и через JavaScript в браузере- они работают по протоколам GWT, RPC, REST/JSON, SOAP/XML и др).[8]

Самым надежным на данный момент является рейтинг топ 10 уязвимостей от проекта OWASP (Open Web Application Security Project) – это открытый проект обеспечения безопасности веб-приложений. На документ OWASP Top 10 часто ссылаются при упоминании наиболее распространенных недостатков безопасности веб приложений [9]:

A1 Внедрение кода. Инъекционные недостатки как SQL, NoSQL, OS и LDAP, возникают, когда ненадежные данные отправляются интерпретатору как часть команды или запроса.

A2 Некорректная аутентификация и управление сессией.

A3 Межсайтовый скриптинг. «Многие веб-приложения и API не защищают конфиденциальные данные, такие как финансовые, медицинские и PII.

A4 Нарушение контроля доступа. Многие старые или слабо сконфигурированные XML-процессоры оценивают ссылки на внешние сущности в документах XML. Внешние объекты могут быть использованы для раскрытия внутренних файлов с использованием обработчика URI файла, внутренних общих файлов, внутреннего сканирования портов, удаленного выполнения кода и атак типа отказ в обслуживании.

A5 Небезопасная конфигурация. Ограничения на то, что разрешено пользователям, прошедшим проверку подлинности, часто не выполняются должным образом.

A6 Утечка чувствительных данных. Наиболее часто встречающаяся проблема – это неправильная конфигурация системы. Обычно это результат небезопасных конфигураций по умолчанию, неполных или специальных конфигураций, открытого облачного хранилища, неправильно сконфигурированных заголовков HTTP и подробных сообщений об ошибках, содержащих конфиденциальную информацию.

A7 Недостаточная защита от атак (NEW). Ошибки XSS возникают, когда приложение включает не доверенные данные на новой веб-странице без правильной проверки или экранирования, или обновляет существующую веб-страницу

с предоставленными пользователем данными с помощью API-интерфейса браузера, который может создавать HTML или JavaScript.

A8 Подделка межсайтовых запросов. Небезопасная десериализация часто приводит к удаленному выполнению кода.

A9 Использование компонентов с известными уязвимостями. Компоненты как библиотеки, фреймворки и другие программные модули, работают с теми же привилегиями, как и приложение. Если уязвимый компонент используется, такая атака может облегчить серьезную потерю данных или захват серверов.

A10 Недостаточное журналирование и мониторинг. Недостаточная регистрация и мониторинг в сочетании с отсутствующей или неэффективной интеграцией с реагированием на инциденты позволяют атакующим продолжать атаковать системы, поддерживать постоянство, склоняться к большему количеству систем и подделывать, извлекать или удалять данные.

Проблемы, выделенные в отчетах OWASP, не просто статичны – они развиваются, и мы должны быть готовы к тому, что они будут видоизменяться и дальше. В таблице представлены уязвимости, наиболее актуальные в 2021 году и наиболее актуальные на 2025 год с учетом новых тенденций и прогнозов/

Эволюция уязвимостей
Evolution of vulnerabilities

уязвимость	2021	Прогноз 2025
API1	Нарушение контроля доступа	Расширенная авторизация на уровне сломанных объектов (BOLA)
API2	Сбои в криптографии	Атаки аутентификации, основанной на ИИ
API3	Внедрение кода	Сложные действия по свойствам объектов и манипулированию данными
API4	Небезопасное проектирование	Искусственное потребление ресурсов:
API5	Небезопасная конфигурация	Уязвимости BFLA (Broken Function Level Authorization) с использованием машинного обучения.
API6	Уязвимые и устаревшие компоненты	Несанкционированный доступ к данным на основе контекста.
API7	Ошибки идентификации и аутентификации	Усиленные SSRF-активности с использованием облачной альтернативы.
API8	Нарушение целостности данных программного обеспечения	Уязвимости из-за неправильной конфигурации безопасности в микросервисах.
API9	Ошибки мониторинга и недостаточное ведение журналов	Динамический контроль запасов API
API10	Подделка запросов со стороны сервера	Небезопасное использование API с использованием ИИ-ботов

Заключение

Обеспечение безопасности веб-сайтов требует постоянного мониторинга и реагирования на уязвимости. Продолжительность мониторинга и реагирования на уязвимости являются ключевыми факторами в обеспечении безопасности веб-сайтов. Эффективные методы обнаружения уязвимостей и соответствующие меры безопасности должны постоянно совершенствоваться и адаптироваться к новым угрозам для обеспечения эффективной защиты веб-ресурсов. Важно уделять внимание обучению персонала и его осведомленности о современных методах атак, чтобы поддерживать ресурс в защищенном состоянии.

Список использованных источников

1. Шакиров А.А. Зарипова Р.С. (2019) Современные тенденции web-разработки. Russian Journal of Education and Psychology. (3), 85-88.
2. Гибадуллин Р.Ф., Вершинин И.С., Глебов Е.Е. (2023) Разработка приложения для ассоциативной защиты файлов. Инженерный вестник Дона.
3. Юртаев В.В., Николаева С.Г. (2023) Базы данных как уязвимость организации. Технологический суверенитет и цифровая трансформация. Международная научно-техническая конференция. 256-260.
4. Gizatullin Z., Nuriev M. (2022) Modeling the electromagnetic compatibility of electronic means under the influence of interference through the power supply network.
5. Злыгостев Д.Д., Зарипова Р.С. (2017) Информационная безопасность как инструмент обеспечения экономической безопасности предприятий. Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов Международной научно-практической конференции. 23-25.
6. Gibadullin R.F., Nikonorov V.V. (2021) Development of the system for automated incident management based on open-source software.
7. Чудинов Н.В., Халидов А.А. (2022) Разработка программного комплекса для защиты программ от нелегального использования. Современные цифровые технологии: проблемы, решения, перспективы, национальная (с международным участием) научно-практическая конференция. 140-142.
8. Шутько Н.А. (2022) Теоретические понятия защиты web-приложений от уязвимостей. Международный научный журнал «ВЕСТНИК НАУКИ» . (11)
9. Алекперов З.А. (2019) Национальный Исследовательский Университет Информационных Технологий Механики и Оптики Россия, «Научно-практический электронный журнал Аллея Науки». (5)

References

1. Shakirov A.A. Zaripova R.S. (2019) Modern trends in web development. Russian Journal of Education and Psychology. (3), 85-88.
2. Gibadullin R.F., Vershinin I.S., Glebov E.E. (2023) Development of an application for associative file protection. Engineering Bulletin of the Don.
3. Yurtaev V.V., Nikolaeva S.G. (2023) Databases as an organization's vulnerability. Technological sovereignty and digital transformation. International scientific and technical conference. 256-260.
4. Gizatullin Z., Nuriev M. (2022) Modeling the electromagnetic compatibility of electronic means under the influence of interference through the power supply network.
5. Zlygostev D.D., Zaripova R.S. (2017) Information security as a tool for ensuring the economic security of enterprises. Innovations in information technology, mechanical engineering and motor transport: collection of materials of the International scientific and practical conference. 23-25.
6. Gibadullin R.F., Nikonorov V.V. (2021) Development of the system for automated incident management based on open-source software.
7. Chudinov N.V., Khalidov A.A. (2022) Development of a software package to protect programs from illegal use. Modern digital technologies: problems, solutions, prospects, national (with international participation) scientific and practical conference. 140-142.
8. Shutko N.A. (2022) Theoretical concepts of protecting web applications from vulnerabilities. International scientific journal "BULLETIN OF SCIENCE". (11)
9. Alekperov Z.A. (2019) National Research University of Information Technologies, Mechanics and Optics Russia, "Scientific and practical electronic journal Alley of Science". (5)

Сведения об авторах

Божко Р.А., начальник военной кафедры, учреждение образования «Белорусская государственная академия связи», vk@bsac.by
Пулко Т.А., канд. техн. наук, доц., доцент кафедры защиты информации факультета информационной безопасности учреждения образования «Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pulko@bsuir.by

Information about the authors

Bozhko R.A., Head of the Military Department, educational institution "Belarusian State Academy of Communications", vk@bsac.by
Pulko T.A., Cand. Sci. (Tech.)), Associate Professor, Associate Professor of the Department of Information Security, Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pulko@bsuir.by.

УДК 621.37

МНОГОСЛОЙНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ НА ОСНОВЕ ФОЛЬГИРОВАННЫХ МАТЕРИАЛОВ ДЛЯ ЗАЩИТЫ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ ОТ СВЧ- И ТЕПЛОВЫХ ПОМЕХ

О.В. Бойправ, В.В. Лобунов
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Представлена технология изготовления многослойных электромагнитных экранов с использованием фрагментов алюминий- или медьсодержащих фольгированных материалов. Приведены закономерности изменения температуры лицевых и оборотных поверхностей таких экранов в зависимости от соотношения между суммарной площадью участков поверхностей, покрытых такими фрагментами, и суммарной площадью участков поверхностей, не покрытых такими фрагментами. Согласно этим закономерностям, при увеличении с 50,0 до 75,0 % указанного соотношения температура лицевой поверхности рассматриваемых экранов, изготовленных с использованием фрагментов алюминийсодержащих фольгированных материалов, увеличивается с 45,0±1,0 °С до 50,0±1,0 °С, а оборотной – снижается с 36,0±1,0 °С до 34,0±1,0 °С (в условиях воздействия на такие экраны электромагнитного излучения ИК-диапазона длин волн, температура поверхности источника которого составляет 70,0±2,0 °С (температура воздуха – 20,0±1,0 °С)). У рассматриваемых экранов, изготовленных с использованием фрагментов медьсодержащих фольгированных материалов, при указанных условиях температура лицевой и оборотной поверхностей соответственно увеличивается с 43,0±1,0 °С до 47,0±1,0 °С и снижается с 35,0±1,0 °С до 33,0±1,0 °С. Показано, что исследованные экраны характеризуются значениями коэффициента передачи электромагнитного излучения в диапазоне частот 0,7–17,0 ГГц, изменяющимся в пределах от –30,0 до –40,0 дБ. Эти экраны представляются перспективными для использования в целях защиты средств обработки информации от воздействия СВЧ- и тепловых помех.

Ключевые слова: алюминийсодержащий фольгированный материал; медьсодержащий фольгированный материал; тепловая помеха; технология; электромагнитный экран.

MULTILAYER ELECTROMAGNETIC SHIELDS BASED ON FOILED MATERIALS FOR PROTECTING INFORMATION PROCESSING EQUIPMENT FROM UHF AND THERMAL INTERFERENCE

O.V. Boiprav, V.V. Lobunov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The technology of manufacturing multilayer electromagnetic shields using fragments of aluminum- or copper-containing foiled materials is presented. The regularities of temperature change of front and back surfaces of such shields are given depending on the ratio between the total area of surface sections covered by such fragments and the total area of surface sections not covered by such fragments. According to these regularities, with an increase from 50.0 to 75.0% of the specified ratio, the temperature of the front surface of the considered shields, manufactured using fragments of aluminum-containing foiled materials, increases from 45.0±1.0 °C to 50.0±1.0 °C, and the back surface temperature decreases from 36.0±1.0 °C to 34.0±1.0 °C (under conditions of exposure of such shields to electromagnetic radiation of the IR wavelength range, the surface temperature of the source of which is 70.0±2.0 °C (air temperature is 20.0±1.0 °C)). In the considered shields, manufactured using fragments of copper-containing foiled materials, under the specified conditions the temperature of the front and back surfaces increases from 43.0±1.0 °C to 47.0±1.0 °C and decreases from 35.0±1.0 °C to 33.0±1.0 °C, respectively. It's shown that the investigated shields are characterized by of the electromagnetic radiation transmission coefficient values in the frequency range of 0.7–17.0 GHz, varying within the limits from –30.0 to –40.0 dB. These shields appear promising for use in protecting information processing equipment from the effects of UNF and thermal interference.

Keywords: aluminum-containing foiled material; copper-containing foiled material; thermal interference; technology; electromagnetic shield.

Введение

Одним из мероприятий, реализуемых в целях обеспечения информационной безопасности, является защита средств обработки информации от внешних электромагнитных помех. Выделяют условно два подхода к реализации такого мероприятия:

1) размещение средств обработки информации от потенциальных источников помех на расстоянии, на котором амплитуда последних характеризуется значением, сопоставимым со значением амплитуды фонового электромагнитного излучения;

2) размещение между средством обработки информации и потенциальными источниками помех электромагнитного экрана.

Второй из вышепредставленных подходов на практике применяется чаще, чем первый. Это обусловлено тем, что потенциальные источники электромагнитных помех для средств обработки информации и сами такие средства располагаются в пределах одного помещения или в пределах смежных помещений, параметры границ которого (которых) меньше расстояния, удовлетворяющего условию, соответствующему первому из вышепредставленных подходов. Обозначенная особенность является одной из причин развития на высоком уровне исследований, посвященных разработке и совершенствованию технологий изготовления электромагнитных экранов [1].

Цель исследования, результаты которого представлены в статье, состояла в экспериментальном обосновании технологии изготовления многослойных электромагнитных экранов, обеспечивающих эффективное снижение энергии электромагнитного излучения СВЧ- и ИК-диапазонов длин волн. Основное преимущество таких экранов по сравнению с их аналогами заключается в том, что с их использованием можно обеспечивать защиту средств обработки информации и других радиоэлектронных средств не только от СВЧ-помех, но и от тепловых помех.

Основная часть

Разработанная технология включает в себя следующие операции.

1. Откраивание четырех однообразных фрагментов синтетического нетканого материала, размеры и форма которых соответствуют размерам и форме изготавливаемого электромагнитного экрана.

2. Откраивание фрагментов алюминий- или медьсодержащего фольгированного материала, длина и ширина которых не превышают соответственно 3,0 и 1,0 см, а суммарная площадь – 60,0 % от площади фрагментов, откроенных в результате реализации операции 1.

3. Равномерное хаотичное распределение фрагментов, откроенных в результате реализации операции 2, по поверхности одного из фрагментов, откроенных в результате реализации операции 1.

4. Расположение другого из фрагментов, откроенных в результате реализации операции 1, поверх фрагментов, распределенных в результате реализации операции 3.

5. Выдерживание конструкции, полученной в результате реализации операций 2–4, в термопрессе в течение 10,0 мин при температуре ~ 250,0 °С.

6. Повтор операций 2–5.

7. Ниточное соединение по периметру конструкции, полученной в результате реализации операций 2–5, и конструкции, полученной в результате реализации операции 6.

В соответствии с разработанной технологией были изготовлены шесть видов образцов экранов. Образцы каждого из вида отличались значением *C* и типом

фрагментов фольгированных материалов, с использованием которых они были изготовлены, где *C* – это соотношение между суммарной площадью участков поверхности образца, покрытых указанными фрагментами, и суммарной площадью участков поверхностей, не покрытых такими фрагментами, %. Характеристики изготовленных образцов экранов представлены в таблице 1.

Таблица 1. Характеристики изготовленных образцов экранов
Table 1. Characteristics of manufactured shields samples

Наименование образцов экранов	Тип фрагментов фольгированных материалов, с использованием которых были изготовлены образцы экранов	*C*, %
Образцы типа 1	Алюминийсодержащие фрагменты	50,0
Образцы типа 2		65,0
Образцы типа 3		75,0
Образцы типа 4	Медьсодержащие фрагменты	50,0
Образцы типа 5		65,0
Образцы типа 6		75,0

С использованием вышепредставленных образцов выполнены исследования, направленные на установление закономерностей изменения температуры лицевой и оборотной поверхностей экранов, изготовленных в соответствии с разработанной технологией, в зависимости от характерного для них значения *C*. Эти исследования выполнены согласно методике, представленной в работе [2]. Условия проведения исследований были следующими:

– температура поверхности использованного источника ИК-излучения– 70,0±2,0 °С;

– продолжительность воздействия ИК-излучения на образец – 60,0±1,0 мин.

– температура воздуха – 20,0±1,0 °С.

Полученные по результатам проведенных исследований графические зависимости представлены на рис. 1.

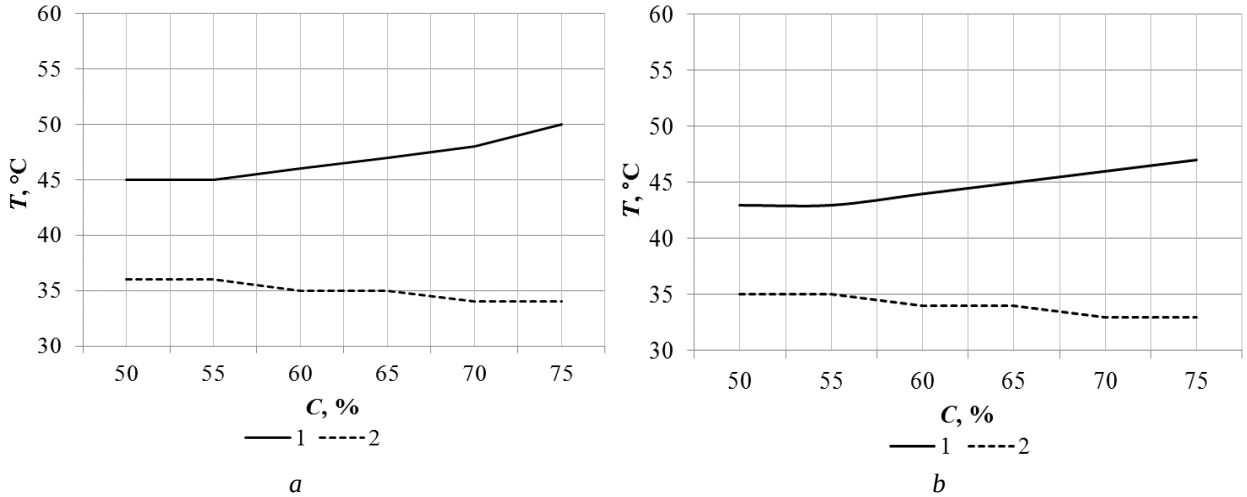


Рис. 1. Зависимости температуры лицевой (кривая 1) и оборотной (кривая 2) поверхностей образцов типов 1–3 (*a*) и образцов типов 4–6 (*b*) от соотношения *C*
Fig. 1. Dependences of the temperature of the front (curve 1) and back (curve 2) surfaces of the samples types 1–3 (*a*) and the samples types 4–5 (*b*) on the ratio *C*

Из рис. 1 следует, что в результате увеличения с 50,0 до 75,0 % значения *C*, характерного для электромагнитных экранов, изготовленных в соответствии с разработанной технологией с использованием фрагментов алюминийсодержащих

фольгированных материалов, температура их лицевой поверхности увеличивается с 45,0±1,0 °С до 50,0±1,0 °С, а оборотной – снижается с 36,0±1,0 °С до 34,0±1,0 °С при условиях, в которых проводились исследования. При аналогичных условиях температура лицевой и оборотной поверхностей электромагнитных экранов, изготовленных в соответствии с разработанной технологией с использованием фрагментов медьсодержащих фольгированных материалов, соответственно увеличивается с 43,0±1,0 °С до 47,0±1,0 °С и снижается с 35,0±1,0 °С до 33,0±1,0 °С.

В соответствии с методикой, представленной в работе [3], установлено, что электромагнитные экраны, изготовленные в соответствии с разработанной технологией, характеризуются значениями коэффициента передачи электромагнитного излучения в диапазоне частот 0,7–17,0 ГГц, изменяющимся в пределах от –30,0 до –40,0 дБ.

Заключение

Таким образом, электромагнитные экраны, изготовленные в соответствии с разработанной технологией, представляются перспективными для использования в целях защиты средств обработки информации от воздействия СВЧ- и тепловых помех. С применением таких экранов представляется рациональным изготавливать ширмы для зонирования помещений или для закрепления в дверных или оконных проемах последних.

Список использованных источников

1. Shi Y., Wu M., Ge S., Li J., Alshammari A.S., Luo J., et. al. (2024) Advanced Functional Electromagnetic Shielding Materials: A Review Based on Micro-Nano Structure Interface Control of Biomass Cell Walls. Nano- Micro Letters. 17, article number 3.

2. Бойправ О.В., Лобунов В.В., Лыньков Л.М., Аль-Машат Е.А.А. (2020) Исследование взаимодействия электромагнитного излучения инфракрасного диапазона длин волн с радиопоглотителями на основе металлсодержащих элементов. Авиационные материалы и технологии. 2 (59), 89–94.

3. Boiprav O., Ayad H., Abdaljlil S.A., Lynkou L., Abdulmawlay M. (2022) Charcoal- and Foil-Containing Materials for Radio Electronic Control Systems Protection from Electromagnetic Interferences. Proceedings of 2022 IEEE 21st International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, STA 2022. 299–304.

References

1. Shi Y., Wu M., Ge S., Li J., Alshammari A.S., Luo J., et. al. (2024) Advanced Functional Electromagnetic Shielding Materials: A Review Based on Micro-Nano Structure Interface Control of Biomass Cell Walls. Nano- Micro Letters. 17, article number 3.

2. Boiprav O.V., Lobunov V.V., Lynkov L.M., Al-Mashat E.A.A. (2020) Study of the interaction of electromagnetic radiation of the infrared wavelength range with radio absorbers based on metal-containing elements. Aviation Materials and Technologies. 2 (59), 89–94 (in Russian).

3. Boiprav O., Ayad H., Abdaljlil S.A., Lynkou L., Abdulmawlay M. (2022) Charcoal- and Foil-Containing Materials for Radio Electronic Control Systems Protection from Electromagnetic Interferences. Proceedings of 2022 IEEE 21st International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, STA 2022. 299–304.

Сведения об авторах

Бойправ О.В., канд. техн. наук, доц., зав. каф., учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», smu@bsuir.by.
Лобунов В.В., ст. преп., учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lobunov@bsuir.by.

Information about the authors

Boiprav O., Cand. Sci. (Tech.)), Associate Professor, Head of the Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", smu@bsuir.by.
Lobunov V.V., Senior Lecturer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lobunov@bsuir.by.

УДК 004.41

ЛОКАЛИЗАЦИЯ НЕКОТОРЫХ ЧАСТЕЙ КОММУНИКАЦИОННОГО ПРОТОКОЛА WIREGUARD

А.Г. Бокун
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассмотрена одна из составляющих механизма защиты информации в коммуникационном протоколе WireGuard. Во введении обозначена актуальность применения и локализации современных протоколов безопасной передачи данных с открытой спецификацией. В основной части была дана краткая характеристика частям механизма обеспечения аутентифицированного шифрования в Wireguard. Кроме этого было рассмотрено альтернативное решение на основе государственного стандарта Республики Беларусь СТБ 34.101.31. В заключении на основе проведенной оценки криптографических примитивов WireGuard и шифров из СТБ были сделаны выводы о целесообразности локализации именно этого протокола.
Ключевые слова: аутентифицированное шифрование; блочный шифр; функция генерации имитовставки; протокол сетевого уровня; криптографические примитивы; шифротекст.

LOCALIZATION OF SOME PARTS OF THE WIREGUARD COMMUNICATION PROTOCOL

A.G. Bokun
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article considers one of the components of the information protection mechanism in the WireGuard communication protocol. In the introduction the relevance of application and localization of modern protocols of secure data transmission with an open specification is outlined. In the main part a brief characterization of parts of the mechanism of providing authenticated encryption in Wireguard was given. In addition, an alternative solution based on the state standard of the Republic of Belarus STB 34.101.31 was considered. In conclusion, based on the evaluation of cryptographic primitives of WireGuard and ciphers from STB, conclusions were made about the expediency of localization of this protocol.
Keywords: authenticated encryption; block cipher; message authentication code; network layer protocol; cryptographic primitives; ciphertext.

Введение

Современные тренды в области защиты средств связи делают ставку на легкие и производительные протоколы. Манифестацией этого тренда стал выпущенный в 2015 г. протокол сетевого уровня TCP/IP WireGuard. Сильными сторонами этого протокола являются скорость, применение современных криптографических моделей и компактная кодовая база. Исходя из этого считаем рациональным рассмотреть варианты адаптации данного протокола под стандарты Республики Беларусь и его дальнейшую эксплуатацию.

Основная часть

Одним из ключевых аспектов криптографической защиты информации в протоколе WireGuard является алгоритмическая система аутентифицированного шифрования с дополнительными данными (AEAD). В спецификации протокола указано, что в качестве AEAD используется стек ChaCha20-Poly1305. Он состоит из двух алгоритмов – поточного шифра ChaCha20 и кода аутентификации сообщений Poly1305. Актуальным стандартам, регламентирующим работу данного стека, является RFC 8439.

Существует несколько вариантов реализации алгоритма ChaCha: на 8 раундов, на 12 раундов и на 20 раундов. В документе RFC 8439 описывается реализация на 20 раундов, соответственно, WireGuard также использует именно этот вариант.

Суть механизма шифрования заключается в циклическом вызове блок-функции ChaCha20 с одинаковым ключом и вектором инициализации, при этом последовательно увеличиваются параметры счетчика блоков. Затем ChaCha20 сериализует полученное состояние, записывая числа в порядке little-endian, создавая блок потока ключей. Поток ключей образуется через конкатенацию релевантных значений из последовательных блоков. Далее алгоритм выполняет операцию исключающего ИЛИ (XOR) над потоком ключей и исходным текстом. В качестве более оптимизированной альтернативы данному шагу: операцию XOR можно выполнять с каждым блоком потока ключей по отдельности, выбирая для этого соответствующий блок исходного текста.

Стоит помнить, что для исходного текста нет никаких требований по части размера (то есть ему необязательно быть целым кратным 512 битам). Но некоторые конкретные протоколы могут требовать, чтобы открытый и шифрованный текст имели определенную длину.

В спецификации также указано, что если после последнего блока остался лишний ключевой поток, то он отбрасывается. Входными данными для шифра ChaCha20 являются:

– 256-битный ключ;
– 32-битный начальный счетчик, обычно это ноль или единица;
– 96-битный вектор инициализации;
– исходный текст произвольной длины.

В результате работы получается зашифрованное сообщение, той же длины, что и исходный.

Расшифровка выполняется аналогичным образом. Блок-функция ChaCha20 используется для расширения ключа в поток ключей. Далее проводится операция исключающего ИЛИ с зашифрованным текстом, что позволяет получить исходный текст.

Poly1305 является одноразовым аутентификатором. Этот примитив принимает на вход исходные данные и 32-байтный одноразовый ключ, отдает же 16-байтную подпись. Эта подпись может быть использована для проверки подлинности и целостности сообщения.

Poly1305 – это полиномиально-оценочная функция генерации имитовставки. Такие функции представляют каждое сообщение как одномерный многочлен над конечным полем, а затем оценивает этот многочлен на ключе. Полиномиально-оценочные имитовставки сочетают в себе несколько привлекательных в контексте производительности особенностей: не ресурсоемкую генерация коротких ключей и быструю аутентификацию сообщений.

Функция выработки имитовставки Poly1305 представлена в следующей формуле: $Poly1305_r(m, AES_k(n))$, где m – сообщение, k – ключ AES, r – дополнительный ключ, n – синхропосылка. Из формулы создания имитовставки можно понять, что AES здесь используется только для шифрования синхропосылки и получения 128-битной уникальной строки. При этом в стандарте Poly1305 никак не закреплено использование именно AES. Это одновременно делает алгоритм крайне безопасным (его безопасность напрямую зависит от безопасности AES или другого используемого шифра) и гибким, так как AES можно будет заменить любым другим шифром того же класса. Например, в схеме AEAD AES будет заменен шифрованием ChaCha20.

Независимо от способа генерации ключ делится на две части, называемые *r* и *s*. Пара (*r*, *s*) должна быть уникальной и непредсказуемой для каждого обращения (именно поэтому изначально она была получена путем шифрования синхропосылки), в то время как r быть константным. Таким образом, входные данные для функции генерации имитовставки *Poly*1305 будут следующими:

– 256-битный одноразовый ключ;

– некоторое сообщение произвольной длины.

На выходе же будет 128-битный код аутентификации.

AEAD (Authenticated Encryption with Additional Data) является конструкцией, которая представляет собой единый стек из ChaCha20 и Poly1305. AEAD необходим для реализации схемы аутентифицированного шифрования (AE). Существует несколько подходов к реализации AE:

– Шифрование до MAC (EtM) – этот подход предполагает шифрование исходного текста и дальнейшее получение имитовставки через функцию генерации.

– Шифрование и MAC (E&M) – здесь шифрование и получение имитовставки происходят независимо на одном и том же входном тексте.

– MAC до шифрования (MtE) – в данном сценарии первоначально происходит получение имитовставки, после чего имитовставка и входной текст шифруются вместе.

В стеке ChaCha20-Poly1305 реализован первый вариант – шифрование до получения имитовставки. Сначала ChaCha20 шифрует исходный текст, а потом, уже на шифре, получается имитовставка. Общая схема работы ChaCha20-Poly1305 представлена на рис. 1.

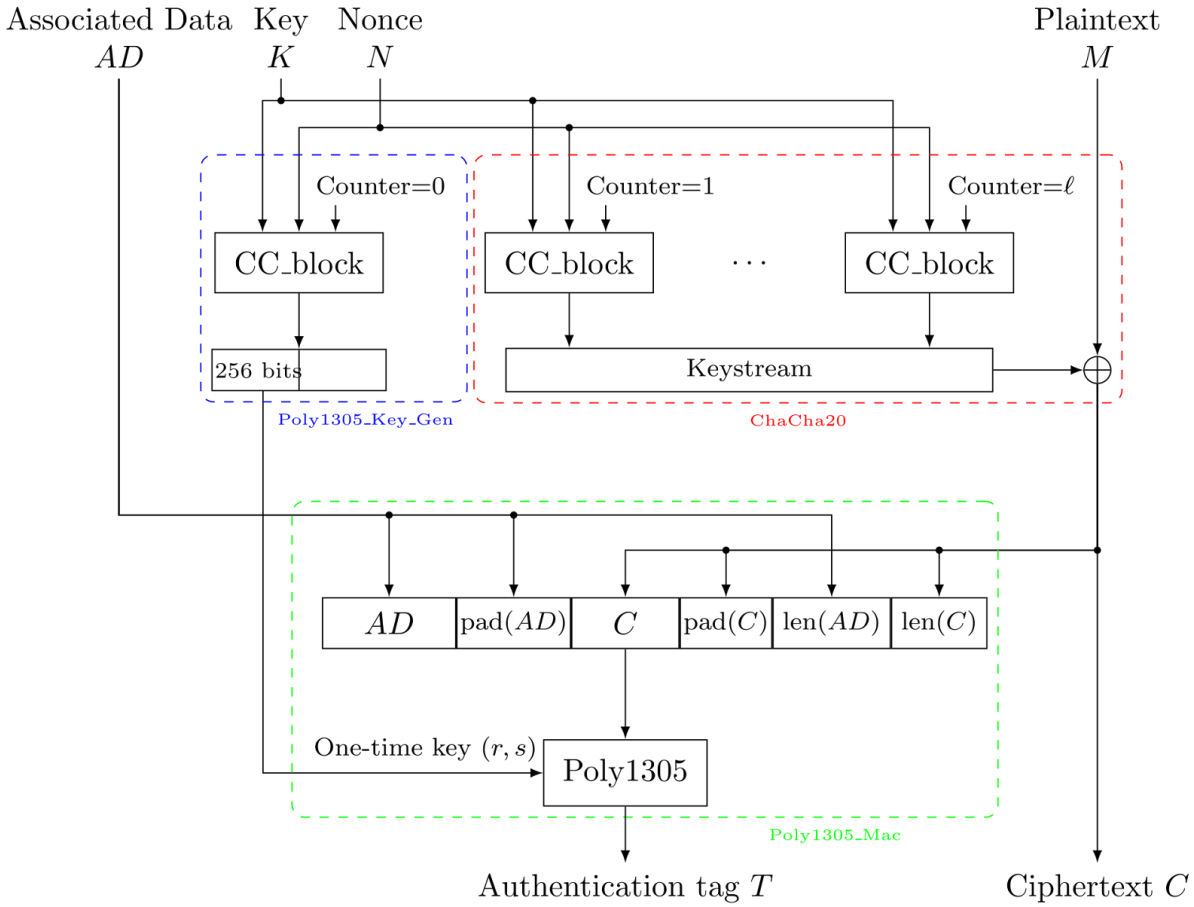


Рис. 1. Общая схема работы AEAD ChaCha20-Poly1305
Fig. 1. General operating scheme of AEAD ChaCha20-Poly1305

Расшифровка сообщения выполняется обратным ходом ChaCha20, при этом Poly1305 все еще применяется на зашифрованном сообщении так как необходимо проверить целостность сообщения.

Имея представление о принципах работы этой части системы шифрования Wireguard можно подобрать алгоритм, который сможет заменить AEAD, определенный в RFC 8439, на подходящий стек криптографических примитивов, соответствующих СТБ.

Наиболее подходящим для задачи интеграции AEAD шифром, который стандартизирован в Республике Беларусь, является алгоритм BelT. BelT – блочный шифр, который описан в СТБ 34.101.31. AEAD был представлен во второй (belt-dwp) и третьей (belt-che) версиях стандарта, от 2011-го и 2020-го годов соответственно. Оба алгоритма (belt-dwp и belt-che) являются актуальными схемами аутентифицированного шифрования и присутствуют в последних редакциях стандарта.

Для использования в локализованной версии Wireguard предлагается вариант belt-dwp, так как режим DWP у AEAD является аналогом режима GCM, но более защищенным, режим же GCM в свою очередь активно используется в традиционных VPN-протоколах вроде OpenVPN. В спецификации belt-dwp указаны следующие входные данные:

– сообщение произвольной длины;
– дополнительные (ассоциированные данные);
– ключ (256 байт);
– синхропосылка (128 байт).

Размерность входных данные соответствуют (за исключением размера синхропосылки) спецификации AEAD ChaCha20-Poly1305, что значительно упростит процесс интеграции.

Заключение

Wireguard является крайне производительным и удобным для расширения протоколом, что делает его локализацию крайне полезной и важной задачей. В статье было продемонстрировано, что государственные стандарты Республики Беларусь могут предоставить криптографические примитивы, которые способны стать аналогами нестандартизированных решений и обеспечить верифицированную безопасность коммуникации. Кроме этого соответствие алгоритмов из СТБ внешним интерфейсам родных шифров Wireguar делает интеграцию довольно удобной, а работы в этой области перспективными.

Список использованных источников / References

1. Bernstein, D.J. (2008) ChaCha, a Variant of Salsa20. Journal of Software Engineering and Applications. 16 (12), 24-30.

2. Bernstein, D.J. (2005) The Poly1305-AES Message-Authentication Code. Lecture Notes in Computer Science. 3557, 32-49.

3. Y. Nir, A. Langley (2018) RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. USA, RFC Editor.

Сведения об авторе

Бокун А.Г., ассистсент кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.bokun@bsuir.by.

Information about the author

Bokun A.G, Assistant at the Department of Informatics, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.bokun@bsuir.by.

УДК 621.382.33–027.45

ЭФФЕКТИВНОСТЬ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ МЕТОДОМ ПРЕОБРАЗОВАНИЯ ИНФОРМАТИВНЫХ ПАРАМЕТРОВ В ТРОИЧНЫЙ КОД

С.М. Боровиков
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Прогнозирование готовых и прошедших выходной контроль изделий электронной техники с точки зрения класса их надежности для заданной наработки может быть выполнено в начальный момент времени методами, использующими информативные параметры. Для целей практики интерес представляет прогнозирование с разделением выборки изделий для заданной наработки на два класса: класс надежных и класс потенциально ненадежных экземпляров. Для прогнозирования используют модели, которые получают заблаговременно с помощью предварительных исследований определенной выборки изделий интересующего типа. В классических методах прогнозирования (потенциальных функций, статистических решений), модель прогнозирования получают, используя непрерывные значения информативных параметров. Автором был предложен метод, в котором информативные параметры преобразовывают в двоичные или троичные кодовые сигналы, что упрощает получение модели прогнозирования, которая в конечном итоге может быть представлена простой логической таблицей, показывающей связь комбинаций кодовых сигналов с классом надежности изделия. На примере выборок мощных полевых транзисторов исследована эффективность моделей прогнозирования, получаемых новым методом.
Ключевые слова: информативные параметры; класс надежности изделий; индивидуальное прогнозирование надежности; достоверность прогнозирования.

EFFICIENCY OF A MODEL FOR FORECASTING THE RELIABILITY OF ELECTRONIC PRODUCTS BY TRANSFORMING INFORMATIVE PARAMETERS INTO A TERNARY CODE

S.M. Borovikov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Forecasting of finished and final-tested electronic products in terms of their reliability class for a given service life can be performed at the initial time using methods that use informative parameters. For practical purposes, forecasting with division of a sample of products for a given service life into two classes is of interest: a class of reliable and a class of potentially unreliable specimens. For forecasting, models are used that are obtained in advance using preliminary studies of a certain sample of products of the type of interest. In classical forecasting methods (potential functions, statistical solutions), the forecasting model is obtained using continuous values of informative parameters. The author proposed a method in which informative parameters are transformed into binary or ternary code signals, which simplifies obtaining a forecasting model, which can ultimately be represented by a logical table showing the relationship of code signal combinations with the reliability class of the product. Using samples of powerful field-effect transistors as an example, the efficiency of prediction models obtained by the new method is investigated.
Keywords: informative parameters; product reliability class; individual reliability forecasting; forecasting reliability.

Введение

Применение методов прогнозирования с разделением выборки готовых изделий электронной техники на классы надежности для заданной наработки основано на измерении информативных параметров у конкретного экземпляра в начальный момент времени с последующей обработкой результатов измерений этих параметров [1] Для

практических применений интерес представляет разновидности метода, при использовании которых экземпляры интересующей выборки ИЭТ классифицируют с точки зрения работоспособности для заданной наработки на два класса:

– класс надежных экземпляров, которые для заданной наработки $t_н$ сохраняют работоспособность (далее обозначен как класс K_1);

– класс потенциально ненадежных экземпляров; это те экземпляры, которые потеряют работоспособность раньше заданной наработки $t_н$ по причине возникновения постепенного или внезапного отказа (далее класс обозначен через K_2).

Решение о классе экземпляра принимают по модели прогнозирования

$$\begin{cases} j \in K_1, \text{если } F\left[x_1^{(j)},...,x_k^{(j)}\right] \geq P_0, \\ j \in K_2, \text{если } F\left[x_1^{(j)},...,x_k^{(j)}\right] < P_0, \end{cases} \quad (1)$$

где j – символ, используемый для обозначения конкретного экземпляра; $x_1{}^{(j)}$, …, $x_k{}^{(j)}$ – значения информативных параметров, измеренные для j-го экземпляра в момент времени $t = 0$; k – количество используемых информативных параметров (обычно $k = 2$–5); $F[x_1{}^{(j)}, …, x_k{}^{(j)}]$ – значение прогнозирующей функции, подсчитанное для j-го экземпляра; P_0 – порог разделения классов, определяемый экспериментально, исходя из условия лучшего разделения классов надежности ИЭТ обучающей выборки.

Модель прогнозирования (1) получают один раз с помощью предварительных исследования определенной выборки (примерно 30…100 экземпляров) ИЭТ интересующего типа. Эти исследования называют обучающим экспериментом, а исследуемую при этом выборку – обучающей. Полученную модель применяют для прогнозирования класса надежности других однотипных экземпляров, которые не использовались в обучающем эксперименте. Основу модели составляет прогнозирующая функция F, значение которой находят при прогнозировании конкретного экземпляра путем подстановки в нее результатов измерения информативных параметров x_1, …, x_k этого экземпляра.

Основная часть

Интерес для практических применений представляет метод построения модели прогнозирования, основанный на принципах пороговой логики с преобразованием измеренных значений информативных параметров в троичные кодовые сигналы τ, принцип получения которых иллюстрируется рис. 1 на примере электрического параметра $U_{КЭнас}$ (напряжение насыщения коллектор-эмиттер) биполярных транзисторов большой мощности КТ872А.

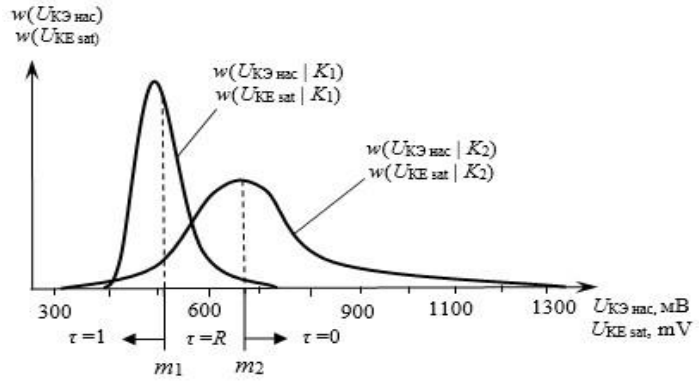


Рис. 1. Преобразование информативного параметра $U_{КЭнас}$ в троичный код
Fig. 1. Transformation of the informative parameter U_{KEsat} into a ternary code

На рис. 1 приняты следующие обозначения: m_1, m_2 – средние значения (математические ожидания) параметра $U_{КЭнас}$ в начальный момент времени, полученные обработкой отдельно экземпляров классов K_1 и K_2 обучающей выборки ИЭТ; τ – троичный кодовый сигнал.

Для области, находящейся между средними значениями информативного параметра в классах K_1 и K_2, присваивается код $\tau_i = R$ (от англ. Range – диапазон), означающий высокую степень неопределенности класса работоспособности рассматриваемого экземпляра (единицы ИЭТ). За пределами указанного диапазона от m_1 до m_2 код $\tau_i = 1$ присваивается значениям информативного параметра, которые в основном соответствуют экземплярам класса K_1, код $\tau_i = 0$ – экземплярам класса K_2.

Практический интерес представляет модель прогнозирования, в которой прогнозирующая функция строится с учетом понятия частная информация о принадлежности j-го экземпляра к классам K_1 и K_2, содержащаяся в сообщении о том, что i-й троичный сигнал τ_i для этого экземпляра принял конкретное значение $\tau_i^{(j)} = \varepsilon$ ($\varepsilon = 1$, либо 0, либо R). В этом случае функция $F^{(j)}$ модели (1) может быть представлена в виде [2]

$$F^{(j)}(\tau_1,...,\tau_k) = \sum_{i=1}^{k} \log_2 \left[\frac{P\left(K_1 \middle| \tau_i^{(j)}\right)}{P(K_1)} \right] - \sum_{i=1}^{k} \log_2 \left[\frac{P\left(K_2 \middle| \tau_i^{(j)}\right)}{P(K_2)} \right], \text{ дв.ед.,} \qquad (2)$$

где j – индекс, означающий, что рассматриваемая величина относится к конкретному экземпляру ИЭТ; $\tau_i^{(j)}$ –троичный кодовый сигнал, полученный для j-го экземпляра; $P(K_1 | \tau_i^{(j)})$, $P(K_2 | \tau_i^{(j)})$ – условная вероятность принадлежности экземпляра соответственно к классам K_1 и K_2 при условии, что в результате преобразования информативного параметра $x_i^{(j)}$ j-го экземпляра в кодированный сигнал $\tau_i^{(j)}$ последний принял конкретное значение ε ($\varepsilon = 1, 0, R$); $P(K_S)$ – начальная вероятность принадлежности любого экземпляра рассматриваемой выборки к классу K_S ($S = 1, 2$).

Первая сумма выражения (2) представляет собой частную информацию, получаемую для j-го экземпляра от набора троичных кодовых сигналов $\tau_1^{(j)}$, ..., $\tau_k^{(j)}$ о классе K_1, а вторая (вычитаемое) – частную информацию о классе K_2. Результатом вычисления $F^{(j)}$ по выражению (2) является число, показывающее, как выполнять прогноз класса работоспособности j-го экземпляра:

а) при $F^{(j)} \geq 0$ должно приниматься решение о классе K_1;

б) при $F^{(j)} < 0$ должно приниматься решение о классе K_2.

Достоверность модели прогнозирования, использующей функцию (2), сравнивалась с моделями прогнозирования, получаемыми методом статистических решений (МСР) и методом потенциальных функций (МПФ) на примере полевых транзисторов большой мощности КП744А как группы ИЭТ.

Для получения моделей прогнозирования был выполнен обучающий эксперимент. Заданная нормированная наработка транзисторов, составляющая $t_н = 80\,000$ ч для обычных нормальных условий работы, обеспечивалась проведением ускоренных форсированных испытаний по типовым методикам с использованием высокотемпературной и электрической нагрузок. Суммарный коэффициент ускорения испытаний имел значение $K_у \approx 160$. Объем обучающей выборки составлял 172 экземпляра, из которых для наработки $t_н = 80\,000$ ч 79 экземпляров оказались работоспособными, следовательно, представителями класса K_1, а 93 экземпляра – представителями класса K_2.

В качестве критерия оценки эффективности моделей прогнозирования использована вероятность принятия правильных решений $P_{прав}$ о классе надежности транзисторов для заданной наработки $t_н$.

В табл. 1 приведены условия получения кодовых сигналов, в табл. 2 – оценки условных вероятностей класса надежности, в табл. 3 – результаты эффективности рассматриваемых моделей прогнозирования.

Таблица 1. Условия получения кодовых сигналов
Table 1. Conditions for creating code signals

Информативный параметр	Пояснение параметра	Условие получения троичного кодового сигнала		
		$\tau = 1$	$\tau = R$	$\tau = 0$
$U_{ЗИ.пор}$, В	Пороговое напряжение затвор–исток, В	> 3,013	$2{,}694 \le U_{ЗИ.пор} \le 3{,}013$	< 2,694
$C_{ЗС}$, пФ	Емкость затвор–сток, пФ	< 773,3	$773{,}3 \le C_{ЗС} \le 795{,}2$	> 795,2
$C_{ЗИ}$, пФ	Емкость затвор–исток, пФ	< 462,3	$462{,}3 \le C_{ЗИ} \le 473{,}3$	> 473,3

Таблица 2. Оценки условных вероятностей класса надежности
Table 2. Estimates of conditional probabilities of reliability class

Способ преобразования информативного параметра	Обозначение условной вероятности	Оценка условной вероятности для:		
		$x_1 \rightarrow \underline{U}_{ЗИ.пор}$	$x_2 \rightarrow C_{ЗС}$	$x_3 \rightarrow C_{ЗИ}$
В троичные сигналы τ_i	$P(K_1 \mid \tau_i = 1)$	0,927	0,900	0,920
	$P(K_1 \mid \tau_i = 0)$	0,045	0,071	0,053
	$P(K_1 \mid \tau_i = R)$	0,448	0,455	0,369
	$P(K_2 \mid \tau_i = 1)$	0,073	0,100	0,080
	$P(K_2 \mid \tau_i = 0)$	0,955	0,929	0,947
	$P(K_2 \mid \tau_i = R)$	0,552	0,545	0,631

Таблица 3. Эффективность моделей прогнозирования
Table 3. Performance of forecasting models

Описание прогнозирующей функции $F^{(j)}$	Номер выражения функции $F^{(j)}$ или источник	Значение порога P_0	Вероятность правильных прогнозов класса работоспособности, $P_{прав}$	
			Обучающая выборка	Контрольная выборка
Использование частной информации о классах K_1 и K_2	(2)	0 бит	0,913	0,906
МСР, гипотеза о нормальном распределении информативных параметров в классах K_1 и K_2	[1]	1	0,901	0,894
Метод потенциальных функций	[1]	0	0,890	0,888

Заключение

Из табл. 3 следует, что модель прогнозирования, основанная на преобразования информативных параметров в троичный код, с использованием прогнозирующей функции, учитывающей частную информацию, содержащуюся в полученном наборе троичных сигналов, обеспечивает достоверность прогнозирования, не уступающую МСР (в предположении нормального распределения информативных параметров в классах надежности K_1 и K_2) и МПФ. Модель прогнозирования может быть представлена логической таблицей. При прогнозировании однотипных экземпляров

отпадает необходимость выполнения расчетов функции вида (2) для каждого прогнозируемого экземпляра.

Список использованных источников

1. Боровиков С.М. (2013) *Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники*. Москва, Издательство «Новое знание».

2. Казючиц В.О., Боровиков С.М., Батура М.П., Шнейдеров Е.Н. (2023) Прогнозирование класса надежности изделий электронной техники методом преобразования информативных параметров в дискретный код. *Доклады ТУСУР*. 26(1), 91–97.

References

1. Borovikov S.M. (2013*) Statistical Forecasting for Rejection of Potentially Unreliable Electronic Products*. Moscow, New Knowledge Publishing House (in Russian).

2. Kaziuchyts V.O., Borovikov S.M., Batura M.P., Shneiderov E.N. (2023) Prediction of the class of reliability of electronic equipment by the method of converting informative parameters into a discrete code. *TUSUR reports*. 26(1), 91–97 (in Russian).

Сведения об авторе

Боровиков С.М., канд. техн. наук, доц., доцент кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bsm@bsuir.by.

Information about the author

Borovikov S.M., Cand. Sci. (Tech.), Associate professor of the Department of Information and Computer Systems Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", bsm@bsuir.by.

УДК 621.382.33-0.27.45

ПРОГНОЗИРОВАНИЕ ЭЛЕКТРИЧЕСКИХ ФУНКЦИОНАЛЬНЫХ ПАРАМЕТРОВ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ ДЛЯ ДЛИТЕЛЬНЫХ НАРАБОТОК

С.М. Боровиков, Е.В. Жук
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В работе на примере мощных биполярных транзисторов КТ872А показана возможность прогнозирования функциональных параметров биполярных транзисторов для длительных наработок путем использования электрических воздействий, в частности тока коллектора, в качестве имитационного фактора. Прогнозирование возможного значения электрического функционального параметра транзистора (например, коэффициента усиления) для длительной наработки в данном методе сводится к измерению в начальный момент времени у прогнозируемого экземпляра значения его электрического функционального параметра при значении тока коллектора (или обратного напряжения на коллекторе), соответствующим имитационному уровню для заданной наработки. Уровни рассчитывают по функции связи имитационного тока коллектора (или обратного напряжения) с заданной наработкой. Функцию связи получают с помощью предварительных исследования выборки транзисторов рассматриваемого типа. Использование тока или напряжения в качестве имитационных воздействий заметно уменьшают длительность процедуры прогнозирования электрического функционального параметра транзисторов в сравнении с использованием температуры в качестве имитационного воздействия. Предложенный метод не требует сложного и дорогостоящего оборудования, необходимого для получения имитационной температуры и поддержания ее постоянной при измерении функционального параметра прогнозируемого экземпляра.

Ключевые слова: биполярный транзистор; индивидуальное прогнозирование электрического функционального параметра; имитационное воздействие; ток коллектора.

FORECASTING ELECTRICAL FUNCTIONAL PARAMETERS OF BIPOLAR TRANSISTORS FOR LONG-TERM OPERATING TIME

S.M. Borovikov, Y.V. Zhuk
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The paper uses the example of powerful bipolar transistors KT872A to demonstrate the possibility of predicting the functional parameters of bipolar transistors for long-term operation by using electrical effects, in particular, the collector current, as a simulation factor. Predicting the possible value of the electrical functional parameter of a transistor (for example, the gain) for a long-term operation in this method comes down to measuring the value of the electrical functional parameter of the predicted specimen at the initial moment of time at the value of the collector current (or reverse voltage on the collector) corresponding to the simulation level for the specified operation. The levels are calculated using the coupling function of the simulation collector current (or reverse voltage) depending on the specified operating time. The coupling function is obtained using preliminary studies of a sample of transistors of the type under consideration. Using current or voltage as simulation effects significantly reduces the duration of the procedure for predicting the electrical functional parameter of transistors in comparison with using temperature as a simulation effect. The proposed method does not require complex and expensive equipment necessary for obtaining the simulated temperature and maintaining it constant when measuring the functional parameter of the predicted specimen.
Keywords: bipolar transistor; individual prediction of electrical functional parameter; simulation effect; collector current.

Введение

Прогнозирование постепенного отказа полупроводникового прибора (ППП) основано на информации о возможном значении его электрического функционального параметра для интересующей заданной наработки. Эффективным подходом к получению этой информации является использование метода имитационных воздействий, при котором возможные необратимые изменения электрического параметра для заданной, обычно длительной наработки, воспроизводятся обратимыми изменениями параметра, вызываемыми имитационным воздействием. Традиционно в качестве такого воздействия рассматривают температуру. Однако температура, как имитационное воздействие, имеет недостатки, наиболее существенными из которых являются длительность процедуры индивидуального прогнозирования значения электрического параметра конкретного экземпляра из-за необходимости нагрева или охлаждения прогнозируемого экземпляра до имитационной температуры, соответствующей заданной наработке, а также техническая сложность поддержания имитационного уровня температуры постоянным при измерении значения электрического функционального параметра прогнозируемого экземпляра (единицы ППП). Результат измерения электрического параметра при имитационной температуре рассматривается в качестве прогноза электрического параметра для заданной наработки.

Актуальным является выбор и экспериментальное подтверждение возможности использования других имитационных факторов, позволяющих более эффективно, нежели использование температурных воздействий, выполнять в начальный момент времени индивидуальное прогнозирование значений электрического параметра конкретного экземпляра и, следовательно, надежности этого экземпляра по постепенному отказу для интересующей наработки.

Основная часть

В отличие от традиционных методов, использующих в качестве имитационных воздействий высокие и/или низкие температуры или радиацию, предложенный подход ориентирует на использование электрических воздействий, такие как ток коллектора или обратное напряжение, которые могут имитировать (вызывать изменения) электрические функциональные параметры при длительной наработке ППП. Электрические функциональные параметры транзисторов заметно реагируют на изменение тока коллектора или обратное напряжение, прикладываемое к коллекторному переходу. При этом, изменения электрических параметров являются обратимыми, не сопровождаются их деградацией. Выполненные ранее исследования [1] подтвердили наличие статистической аналогии между обратимыми изменениями электрического функционального параметра, обусловленные сменой тока коллектора биполярных транзисторов, с одной стороны, и необратимыми изменениями (деградацией) электрического параметра, вызываемые наработкой транзисторов, с другой стороны. Это позволяет по значению электрического функционального параметра (обозначим через Y), измеренному при определенном токе коллектора делать вывод о прогнозном значении электрического параметра и, следовательно, о постепенном отказе транзистора по этому параметру для заданной наработки. Для определения имитационного тока коллектора $I_{\text{Ким}}$, соответствующего заданной наработке необходимо иметь функцию пересчета заданной наработки t на имитационное значение тока коллектора $I_{\text{Ким}}$ (будем эту функцию называть имитационной моделью наработки для рассматриваемого электрического параметра Y):

$$I_{\text{Ким}} = f(t), \tag{1}$$

где f – символ функциональной связи между наработкой t и имитационным током коллектора $I_{\text{Ким}}$.

Для получения имитационной модели (1) вначале необходимо для транзисторов интересующего типа выполнить предварительные исследования, называемые обучающим экспериментом, а используемую при этом выборку – обучающей выборкой. Суть обучающего эксперимента: вначале необходимо выяснить, как электрический параметр Y выборки транзисторов рассматриваемого типа в среднем изменяется от тока коллектора $I_{\text{К}}$. В данном случае изменения электрического параметра Y являются обратимыми. Затем, выполняя ускоренные, обычно форсированные испытания, выясняют, как параметр Y этой же выборки в среднем изменяется от наработки t. В этом случае изменения Y являются необратимыми из-за деградации материалов и свойств транзисторов. Имея результаты обучающего эксперимента, получают две следующие модели:

$$Y_{\text{ср}} = f_1(I_{\text{К}}), \tag{2}$$

$$Y_{\text{ср}} = f_2(t), \tag{3}$$

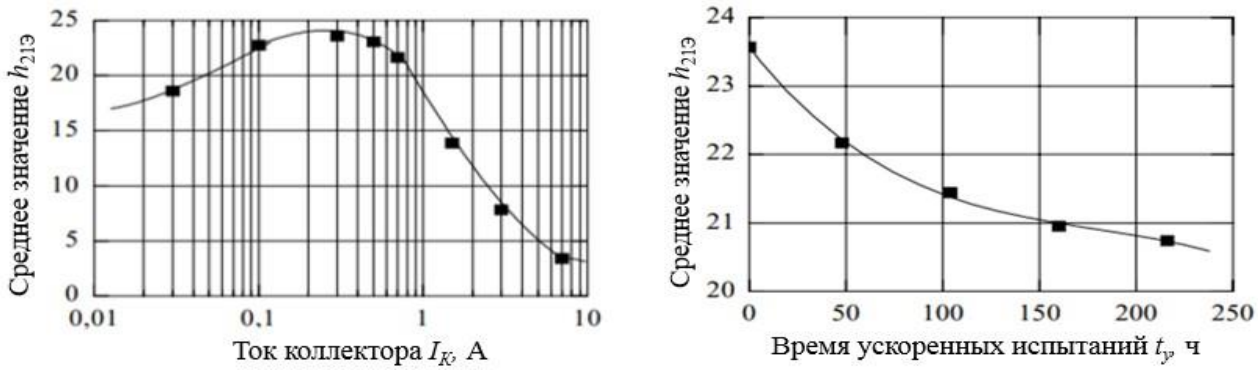
где f_1 и f_2 – символы функциональной связи.

Процедура решения задачи по прогнозированию электрического функционального параметра транзисторов включает следующие этапы [1]: получение математических моделей (2) и (3) для интересующего функционального электрического параметра Y, используя данные экспериментальных исследований; построение имитационной модели (1) на основе полученных моделей (2) и (3); проверка пригодности имитационной модели для прогнозирования значений параметра Y

и, следовательно, постепенных отказов транзисторов по электрическому параметру *Y* для заданных наработок.

Возможность и эффективность прогнозирования значений электрического параметра ППП для заданных наработок с использованием новых имитационных воздействий была исследована на примере биполярных транзисторов большой мощности типа КТ872А. В качестве электрического функционального параметра *Y*, по значению которого принималось решение о постепенном отказе транзисторов, рассматривался коэффициент передачи тока базы в схеме с общим эмиттером ($h_{21Э}$) при рабочем токе коллектора $I_К$ = 0,1 А. В качестве имитационного воздействия (фактора) использовался ток коллектора $I_К$.

Для выполнения обучающего эксперимента из партии транзисторов типа КТ872А случайным образом была взята выборка из 100 транзисторов. Для каждого экземпляра этой выборки при комнатной температуре (20±5 °*C*) измерялся коэффициент $h_{21Э}$ при различных значениях тока коллектора в диапазоне 0,03–7 А. Далее экземпляры обучающей выборки подвергались ускоренным форсированным испытаниям на надежность, проводимым по типовым методикам. Коэффициент ускорения испытаний примерно был равен 80. В процессе испытаний в определенные моменты времени измерялись значения $h_{21Э}$ каждого транзистора обучающей выборки. На рис. 1 приведены графики зависимости среднего значения $h_{21Э}$ для экземпляров обучающей выборки от тока коллектора $I_К$ (*a*) и от времени ускоренных испытаний $t_у$ (*b*).



а *б*

Рис. 1. Зависимость среднего значения коэффициента $h_{21Э}$ от параметров:
a – от тока коллектора; *b* – от временит ускоренных испытаний
Fig. 1. Dependence of the average value of the coefficient h_{21E} on the parameters:
a – on the collector current; *b* – on the time of accelerated tests

Для аналитического описания изменения среднего значения $h_{21Э}$ от тока $I_К$ и от наработки *t*, рассчитанной по времени ускоренных испытаний $t_у$ с учетом коэффициента ускорения испытаний, получены следующие модели:

$$h_{21Э.ср} = \frac{1}{0{,}022 I_К + 0{,}037}, \quad (4)$$

$$h_{21Э.ср} = \frac{1}{3{,}4 \cdot 10^{-7} t + 0{,}043}, \quad (5)$$

где *t* – значение заданной наработки, ч; размерность $I_К$ – А.

На основе моделей (4) и (5) получена функция пересчета (имитационная модель наработки для электрического параметра $h_{21Э}$):

$$I_{Ким} = 1{,}545 \cdot 10^{-5} \cdot t + 0{,}273, \text{ мА}. \quad (6)$$

Индивидуальное прогнозирование электрического параметра $h_{21Э}$ для заданной наработки t выполняется с использованием полученной имитационной модели (6). Процедура включает следующие действия. Вначале по модели (6) для заданной наработки t определяется имитационный ток $I_{Ким}$. Затем у экземпляра (конкретной единицы транзистора), электрическим параметром которого интересуются для наработки t, измеряется $h_{21Э}$ при токе коллектора, равном рассчитанному значению $I_{Ким}$. Полученное значение $h_{21Э}$ (результат измерения при токе $I_К = I_{Ким}$) принимается в качестве прогнозного значения $h_{21Э}$ для наработки t.

Используя имитационную модель (6), можно убедится, что для наработки t = 1000 ч имитационный ток $I_{Ким}$ = 0,288 А, а для t = 20 000 ч – $I_{Ким}$ = 0,582 А. Это соответствует изменению тока коллектора примерно на 300 мА в диапазоне наработок 1000–20000 ч при рабочем токе $I_К$ = 0,1 А. Погрешность поддержания $I_{Ким}$ в пределах ±5 мА приводит к ошибке в выборе прогнозируемой наработки не более 300 ч в указанном диапазоне, что более, чем в 8 раз меньше, нежели в случае использования имитационной температуры $T_{им}$ при погрешности ее поддержания ±1,5…1,8 °*C*. Кроме того, использование тока коллектора в качестве имитационного воздействия значительно сокращает время процедуры прогнозирования в сравнении с использованием температуры в качестве имитационного воздействия.

Заключение

Предложенный метод прогнозирования электрических функциональных параметров биполярных транзисторов и, следовательно, возможных постепенных отказов для заданных наработок, с использованием электрических имитационных воздействий является более эффективным, нежели использование температуры в качестве имитационного воздействия. Значительно уменьшается длительность самой процедуры прогнозирования и не требуются дополнительные затраты на покупку специального оборудования, обеспечивающего получение имитационных воздействий.

Список использованных источников

1. Боровиков С.М. (2013) *Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники*. Москва, Издательство «Новое знание».

2. Боровиков С.М., Шнейдеров Е.Н., Плебанович В.И, Бересневич А.И., Бурак И.А. (2017) Экспериментальное исследование деградации изделий электронной техники. *Доклады БГУИР*. 2 (104), 45–52.

References

1. Borovikov S.M. (2013) *Statistical Forecasting for Rejection of Potentially Unreliable Elec-tronic Products*. Moscow, New Knowledge Publishing House (in Russian).

2. Borovikov S.M., Shneiderov E.N., Plebanovich V.I., Beresnevich A.I., Burak I.A. (2017) Experimental study of degradation of electronic products. *BSUIR Reports*. 2 (104), 45–52 (in Russian).

Сведения об авторах

Боровиков С.М., канд. техн. наук, доц., доцент кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bsm@bsuir.by.
Жук Е.В., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», zegor091@gmail.com.

Information about the authors

Borovikov S., Cand. Sci. (Tech.), Associate Professor of the Department of Information and Computer Systems Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", bsm@bsuir.by
Zhuk Y., Student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", zegor091@gmail.com.

УДК 004.056

О СПЕЦИФИКЕ ПРЕПОДАВАНИЯ ОСНОВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ПРОГРАММЕ ПРИКЛАДНОЙ МАТЕМАТИКИ В ВОЕННОЙ АКАДЕМИИ

Е.В. Валаханович
Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

Аннотация. В настоящее время информация стала одним из ключевых ресурсов государства. Вместе с ростом значимости информации возрастают и риски, связанные с несанкционированным доступом и кибератаками. В этих условиях подготовка квалифицированных специалистов в области защиты информации становится одной из приоритетных задач для всех сфер деятельности.
Ключевые слова: защита информации; информационная безопасность; шифрование; кодирование; алгоритм; математические методы.

ON THE SPECIFICS OF TEACHING THE FUNDAMENTALS OF INFORMATION SECURITY ACCORDING TO THE APPLIED MATHEMATICS CURRICULUM OF THE MILITARY ACADEMY

E.V. Valakhanovich
The Military Academy of the Republic of Belarus, Minsk, the Republic of Belarus

Abstract. Currently, information has become one of the key sovereign resources. However, risks associated with an unauthorized access and cyberattacks surge as the value of information increases. In view of the above, training of qualified information security specialists has become one of the priorities for all areas of activity.
Keywords: data protection; information security; encryption; coding; algorithm; mathematical methods.

Введение

Сегодня, в эпоху цифровой трансформации, информация стала одним из ключевых ресурсов, определяющих успех как отдельных отраслей деятельности, так и государств в целом. Однако вместе с ростом значимости информации возрастают и риски, связанные с несанкционированным доступом и кибератаками. В этих условиях подготовка квалифицированных специалистов в области защиты информации становится одной из приоритетных задач для всех сфер деятельности.

Основная часть

Специалисты по информационной безопасности необходимы практически во всех отраслях: от финансов и здравоохранения до энергетики и обороны. Они обеспечивают защиту данных, предотвращают утечки информации, разрабатывают системы шифрования и мониторинга, а также участвуют в создании нормативно-правовой базы, регулирующей вопросы информационной безопасности.

Учитывая специфику деятельности Вооруженных Сил, многоуровневая система управления должна обеспечить слаженную работу разнородных подразделений, выполняющих задачи на различных направлениях, в режиме реального времени. При этом противник не должен вскрыть или подавить прохождение информации по каналам связи. Это означает, что в военном деле решение вопросов защиты информации должно быть организовано с наивысшим приоритетом. Неправомерное искажение, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи, могут привести к серьезным последствиям.

В связи с вышеизложенным, современный военный инженер должен обладать высоким профессиональным уровнем базовой подготовки в сфере защиты информации, включающим твердое владение специальными математическими методами и навыками по их использованию.

В настоящее время в учреждении образования «Военная академия Республики Беларусь» на изучение курса высшей математики отводится 360 часов. Вне всякого сомнения, этого объема часов по высшей математике недостаточно для выполнения требований по обеспечению базовой подготовки инженера, которые предъявляет современный уровень развития материально-технической базы Вооруженных Сил. Обучение высшей математике должно включать в себя не только базовый курс, но и изучение специальных прикладных разделов математики с учетом будущей профессиональной деятельности курсантов.

Выпускники ряда специальностей должны обладать профессиональными теоретическими знаниями по передаче, хранению и защите информации, как от помех, так и от несанкционированного доступа, а также практическими навыками применения современных алгоритмов криптографической защиты информации.

Для их специальной подготовки разработана учебная программа по дисциплине «Прикладная математика» в объеме 76 часов, включающая в себя лекции, практические занятия, лабораторные и контрольную работу по теме «Алгоритмы криптографической защиты информации» и дифференцированный зачет.

В ходе изучения «Прикладной математики» курсанты овладевают основными математическими методами теории чисел, теории групп, колец и полей, конечных полей для их последующего использования в защите и цифровой обработке информации, в помехоустойчивом кодировании и в ряде других важных задач, решаемых в военно-инженерной деятельности; основными алгоритмами современной криптографической защиты информации; математическими методами формирования и обработки помехоустойчивых кодов.

Особенности преподавания курса «Прикладная математика» в УО «ВА РБ» состоят в существенном использовании информационных технологий из области программирования и в индивидуальном подходе к курсантам.

В криптографических алгоритмах ведется работа с числами длиной от нескольких до десятков и сотен десятичных знаков, вычисления с которыми отнимают много времени и сил. Даже простейшие теоретико-числовые алгоритмы становятся непреодолимыми для точной обработки их вручную. Это составляет существенную проблему в реализации любого курса математических основ защиты информации.

В связи с этим преподаватели кафедры высшей математики УО «ВА РБ» разработали цикл из 11 лабораторных работ. Если в первой из них рассматриваются алгоритмы вычисления наибольшего делителя двух целых чисел, то в последней из них декодируются двукратные ошибки в примитивных двоичных БЧХ-кодах с конструктивным расстоянием 5 решением квадратных уравнений в поле Галуа – поле

определения рассматриваемого БЧХ-кода. Данные ЛР снабжены множеством разного рода алгоритмов, подпрограмм и мини-программ. В частности, алгоритмами решения линейных и квадратных уравнений в полях Галуа, адаптированными алгоритмами для решения систем линейных уравнений в кольцах классов вычетов как по простому, так и по составному модулю.

Для практического освоения лабораторных занятий курсанты распределены на три подгруппы в зависимости от их уровня подготовки. Исходя из качества выполнения заданий, возможен переход из одной подгруппы в другую.

Курсанты первой подгруппы выполняют упрощенные задачи с применением готового программного продукта.

Для курсантов второй подгруппы подбираются задания базового уровня, а также задания с дополнительными условиями, которые требуют не только умения использовать готовое программное обеспечение, но и разрабатывать свои индивидуальные алгоритмы для решения поставленной задачи.

Курсантам третьей подгруппы предлагаются задания, требующие хорошей математической подготовки, самостоятельного поиска решения, исследовательской деятельности и навыков разработки мини-программ. Курсанты именно третьей подгруппы максимально усваивают преподаваемый материал, проходят все этапы осмысления курса, именно они способны к самостоятельному творчеству.

Важным аспектом данного подхода является то, что для реализации конкретной задачи при помощи программных средств курсантам необходимо мыслить в нескольких направлениях: какой алгоритм нужен, как реализовать этот алгоритм математически, как сделать нужный алгоритм понятным для компьютера. Такой метод, как правило, значительно сокращает время решения поставленной задачи. И главное, развивает творческую инициативу курсантов.

В большинстве случаев алгоритмы реализованы «на скорую руку» в консоле, в них не обработаны исключения и нет привычного для пользователей ПК интерфейса, т.к. они предназначены для личного пользования. Данные мини-программы не реализуют алгоритм шифрования, а лишь облегчают определенные этапы вычислений.

Конечным результатом изучения дисциплины «Прикладная математика» является умение курсантов вскрывать классические криптографические тексты, вскрывать учебные, современные криптограммы, работать с линейными помехоустойчивыми кодами, кодами Хемминга, БЧХ-кодами.

В ходе обучения дисциплине «Прикладная математика» применяется практикум «Защита информации» [1]. Книга отражает с практической точки зрения темы «Основы теории чисел», «Классы вычетов», «Историческая криптография», «Современные криптографические системы: криптосистема RSA и криптосистема Эль Гамаля», позволяет практически освоить материал пособия [2].

Кроме того, в настоящее время коллективом авторов разработано и передано для издания учебно-методическое пособие «Прикладная математика. Лабораторные работы. Практикум» по прикладной математике, включающее в себя 12 лабораторных работ: одна работа посвящена древнейшим криптосистемам, которые как нельзя лучше показывают становление современной криптографии: переход от буквенных шифров к математическим основам защиты информации; три последующие – теории чисел, в частности, теории классов вычетов, которая является основой для освоения криптосистемы RSA и Рабина; работы по теории групп, колец и полей связаны с криптосистемой Эль Гамаля, теорией норм синдромов, полями Галуа. Данный комплекс лабораторных работ будет готовить обучающихся к изучению стандарту шифрования, требующего более сложной математики – криптосистеме AES.

Заключение

Знание математических основ защиты информации в автоматизированных системах обработки информации необходимо для действенного усвоения всего спектра алгоритмов и сути современных криптосистем, с которыми придется столкнуться в своей практической деятельности будущим специалистам-инженерам.

Подготовка специалистов в области защиты информации – важнейшая задача, от решения которой зависит безопасность данных, конфиденциальность и устойчивость современных систем. Для успешной реализации задачи по подготовке специалистов в области защиты информации требуется системный подход, учет современных тенденций и активное внедрение инновационных технологий в образовательный процесс.

Список использованных источников

1. Липницкий В. А., Михайловская Л. В., Валаханович Е. В. (2012) *Защита информации: практикум*. Минск: ВА РБ.

2. Липницкий В. А. (2006) *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа*. Минск: БГУИР.

References

1. Lipnitski V. A., Mikhailovskaya L. V., Valakhanovich E. V. (2012) *Information protection: workshop*. Minsk: MA RB.

2. Lipnitski V. A. (2006) *Modern applied algebra. Mathematical foundations for protecting information from interference and unauthorized access.* Minsk: BSUIR.

Сведения об авторах

Валаханович Е. В., старший преподаватель, Учреждение образования «Военная академия Республики Беларусь», ekat.valah@gmail.com.

Information about the authors

Valakhanovich E. V., senior lecturer, The Military Academy of the Republic of Belarus, ekat.valah@gmail.com.

УДК 621.391

АСПЕКТЫ ВЫБОРА ПОМЕХОУСТОЙЧИВОГО КОДА ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Г.А. Власова

Институт информационных технологий
Белорусского государственного университета информатики и радиоэлектроники,
Минск, Республика Беларусь

Аннотация. Рассмотрены задачи, возникающие при обеспечении контроля целостности информации методами помехоустойчивого кодирования. Систематизированы критерии для оценки эффективности выбора кода, контролирующего ошибки. Помимо классических критериев, к которым относятся кратность контролируемых ошибок, скорость кода, использование пошаговых либо параллельных методов обработки, предлагается рассматривать и другие параметры. Добавочные преимущества позволяет получить использование дополнительных возможностей по контролю ошибок, в том числе группирующихся, без значительного увеличения аппаратных затрат. Особенности реализации устройств обработки в интегральном исполнении либо на дискретных элементах также требуют выбора кода и алгоритма декодирования с определенными параметрами. Коды с однородной структурой и разделение ошибок на классы позволяют обеспечить высокое быстродействие и наращиваемость устройств обработки. На примере кодов Боуза-Чоудхури-Хоквингема и их модификаций показаны этапы проектирования устройств контроля ошибок в сообщениях.

Ключевые слова: целостность информации; коды, контролирующие ошибки; кратность ошибки; коды Боуза-Чоудхури-Хоквингема; модификации кодов; дополнительные корректирующие возможности; пошаговое декодирование; параллельное декодирование; аппаратная сложность; быстродействие.

ASPECTS OF SELECTING A NOISE-RESISTANT CODE FOR INFORMATION INTEGRITY CONTROL

G. A. Vlasova
Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The tasks that arise in ensuring information integrity control by noise-resistant coding methods are considered. The criteria for evaluating the effectiveness of error control code selection are systematized. In addition to the classical criteria, which include the multiplicity of controlled errors, the code speed, the use of step-by-step or parallel processing methods, it is proposed to consider others. Using additional error control capabilities, including clustering errors, without significantly increasing hardware costs allows you to get additional advantages. The features of the implementation of processing devices in integrated design or on discrete elements also require the choice of a code and a decoding algorithm with certain parameters. Codes with a uniform structure and dividing errors into classes allow for high processing speed and extensibility of processing devices. Using the example of Bose-Chaudhuri-Hocquenghem codes and their modifications, the design stages of devices for error control in the message are shown.
Keywords: information integrity; error control codes; error order; Bose-Chaudhuri-Hocquenghem codes; codes modifications; additional error correction possibilities; step-by-step decoding; parallel decoding; hardware complexity; processing speed.

Введение

Согласно Закону Республики Беларусь «Об информации, информатизации и защите информации» под защитой информации понимается комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Целостность и сохранность необходимо обеспечить в условиях действия помех при передаче, обработке, распределении и хранении информации. Эффективным методом обнаружения, идентификации и коррекции ошибок в передаваемых сообщениях является помехоустойчивое кодирование. Однако задача выбора помехоустойчивого кода, алгоритма его обработки и аппаратной реализации является сложной многопараметрической задачей.

Основная часть

Теория и аппаратная реализация кодов, контролирующих ошибки, характеризуются тем, что разработка кодов и алгоритмов их обработки исследовались, как правило, алгебраистами; в то время как устройства проектируют инженеры [1–3]. В результате построены коды с высокими корректирующими возможностями и малой вносимой избыточностью, близкими к теоретически достижимым значениям. Однако их практическое использование ограничено сложностью устройств обработки. В то же время, коды с хорошими, но не предельно достижимыми параметрами, и приемлемыми аппаратными и временными затратами на декодирование находят широкое применение на практике [2, 3].

При проектировании устройств обработки кодов следует искать компромисс между противоречивыми задачами (см. рисунок). Так, необходимость сокращения времени обработки кода ведет к росту аппаратных затрат и, соответственно, размеров устройства и его стоимости. Увеличение требований к достоверности информации, а, следовательно, к числу контролируемых кодом ошибок, также ведет к росту затрат

на его обработку. Затраты на декодирование зависят и от выбора алгоритма обработки кода.

Рассмотрим возможную последовательность этапов выбора кода, контролирующего ошибки, с учетом требований к его практическому использованию.

Во-первых, следует оценить помеховую обстановку и определить требования к кратности обнаруживаемых, идентифицируемых и корректируемых кодом ошибок. Поскольку помехоустойчивое кодирование основано на введении в информационное сообщение избыточности, одной из основных характеристик кода является скорость R, то есть отношение числа информационных символов k к общей длине последовательности n. Возможности кода по контролю ошибок определяет кодовое расстояние d (минимальное расстояние Хемминга). Геометрически расстояние Хэмминга – это число ребер в n-мерном кубе между i-м и j-м кодовыми словами. В теории помехоустойчивого кодирования построены оценки зависимости скорости кода от кодового расстояния. Код считается хорошим, если его параметры лежат выше нижней границы Варшамова–Гильберта и ниже верхней границы Хэмминга [1]. Например, одними из лучших кодов, контролирующих независимые ошибки, являются коды Боуза-Чоудхури-Хоквингема (БЧХ) [2].

Критерии выбора помехоустойчивого кода и метода его обработки
Criteria for selecting a noise-resistant code and its processing method

Следующим этапом является оценка допустимых значений аппаратных и временных затрат на контроль ошибок. В зависимости от этих критериев выбирается параллельная (с минимальными временными затратами) либо последовательная (с минимальными аппаратными затратами) обработка [2]. В [4] рассмотрены варианты пошагового декодирования БЧХ-кодов. Показано, что известный декодер Меггитта [2] возможно использовать не только для низкоскоростных, но и для классических кодов БЧХ. Причем время декодирования при коррекции одиночных и двойных ошибок возможно уменьшить с $3n$ до $2{,}5n$ тактов, то есть увеличить быстродействие на 16 % по сравнению с известными устройствами без увеличения аппаратных затрат. В случае, когда требуется увеличить быстродействие устройства декодирования, обработка кода проводится по параллельным алгоритмам. Основной задачей при этом является минимизация сложности селектора (устройства, которое по виду синдрома принятой последовательности определяет вид ошибки). Сократить в n раз сложность селектора

для циклических кодов, к которым относятся коды БЧХ, без значительного увеличения временных затрат позволяет разделение ошибок на классы [5, 6].

В классических трудах теории помехоустойчивого кодирования рассматриваются коды, корректирующие определенный вид ошибок: независимые либо группирующиеся в модули и пакеты [1-3]. Однако проведенные исследования показали, что осуществимо расширить корректирующие возможности кодов. Так модифицированный код, полученный перестановкой в лексикографическом порядке столбцов в проверочной матрицы реверсивного БЧХ-кода, корректирующего двойные независимые ошибки, позволяет дополнительно исправлять модульные ошибки длины четыре и пакетные ошибки длины три [7]. Перестановка столбцов проверочной матрицы эквивалентна перестановке разрядов в кодовом слове и не влияет на сложность устройства. Дополнительные элементы, вводимые в устройство для коррекции группирующихся ошибок, составляют порядка 5% аппаратных затрат на коррекцию независимых ошибок [6, 8] и не влияют на быстродействие устройства. Поэтому при выборе помехоустойчивого кода необходимо исследовать его дополнительные возможности по контролю ошибок, что позволит получить конкурентные преимущества.

При проектировании следует учитывать также, будет ли устройство разрабатываться на дискретных элементах, либо в интегральном исполнении. Реализация на дискретных элементах позволяет разрабатывать оригинальные устройства с максимальным учетом требований заказчика. Кроме того, подобная реализация позволяет минимизировать не декларируемые возможности при эксплуатации [4]. Устройства в интегральном исполнении, напротив, должны быть унифицированы и иметь возможность наращивания для увеличения длины корректирумой последовательности либо кратности контролируемых ошибок. Это позволит обеспечить рентабельность производства подобных схем. Разделение ошибок на классы дает возможность проектировать устройства с регулярной однородной структурой на вентильных матрицах, быстродействие которых не зависит от длины кодового слова и кратности корректируемых ошибок [8]. Высокая скорость обработки достигается за счет уменьшения числа последовательно соединенных элементов по сравнению с известными решениями. Благодаря однородной структуре при интегральном исполнении устройство будет занимать значительно меньшую площадь кристалла. Кроме того, обеспечена возможность наращиваемости: в случае возникновения необходимости увеличения кратности исправляемых ошибок, в устройство вводятся дополнительные блоки (вентильные матрицы).

Заключение

Выбор помехоустойчивого кода для контроля целостности информации является компромиссным решением. Так увеличение скорости декодирования ведет к росту аппаратных затрат, а, следовательно, размеров и стоимости устройства обработки. Необходимость увеличения кратности корректируемых ошибок также приводит к дополнительным аппаратным и временным затратам. Для решения данной проблемы необходим комплексный системный подход. Следует оценить кратность корректируемых ошибок, допустимые аппаратные и временные затраты, особенности исполнения устройств обработки кода, а также возможности модификации кода для получения дополнительных корректирующих возможностей.

Список использованных источников

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. (1979) *Теория кодов, исправляющих ошибки.* Москва, Издательство «Связь».

2. Блейхут Р. (1986) *Теория и практика кодов, контролирующих ошибки.* Москва, Издательство «Мир».

3. Морелос-Сарагоса Р. (2005) *Искусство помехоустойчивого кодирования: методы, алгоритмы, применение.* Москва, Издательство «Техносфера».

4. Власова Г. А. (2022) Устройства пошагового декодирования кодов Боуза-Чоудхури-Хоквингема. *Восьмой Белорусский космический конгресс.* Том 1, 141–144.

5. Власова Г. А. (2024) Проектирование устройств обработки модификаций кодов Боуза-Чоудхури-Хоквингема на основе разделения ошибок на классы. *Компьютерное проектирование в электронике.* 60–62.

6. Власова Г. А. (2021) Устройство декодирования реверсивных кодов Боуза-Чоудхури-Хоквингема с дополнительными корректирующими возможностями для контроля целостности информации. *Комплексная защита информации.* 240-242.

7. Липницкий В. А., Конопелько В. К., Власова Г. А., Осипов А. Н.. (2000) Двоичные реверсивные коды для контроля байтовых ошибок. *Известия национальной академии наук Беларуси. Серия физико-математических наук*. (1), 127-131.

8. Власова Г. А., Конопелько В. К. (1998) Параллельное декодирование БЧХ-кодов с идентификацией ошибок. *Цифровая обработка сигналов и ее применения.* Том II, II-75–II-78.

References

1. Mac Williams E. J., Sloane N. J. A. (1979) *The Theory of Error-Correcting Codes.* Moscow, Svyaz Publishing House (in Russian).

2. Blahut R. E. (1986) *Theory and Practice of Error Contril Codes.* Moscow, Tekhnosfera Publishing House (in Russian).

3. Morelos-Zaragoza R. (2005) *The Art of Error Correcting Coding.* Moscow, Mir Publishing House (in Russian).

4. Vlasova G. A. (2022) Devices for step-by-step decoding of Bose-Chaudhuri- Hocquenghem codes. *The eighth Belarusian Space Congress.* Vol 1, 141–144 (in Russian).

5. Vlasova G. A. (2024) Design of devices for processing Bose-Chaudhuri- Hocquenghem codes modifications based on dividing errors into classes. *Electronic Design Automation.* 60–62 (in Russian).

6. Vlasova G. A. (2021) A Device for Decoding Reverse Bose-Chaudhuri- Hocquenghem codes with Additional Correction Capabilities for Information Integrity Control. *Comprehensive Information Protection.* 240-242 (in Russian).

7. Lipnitsky V. A., Konopelko V. K., Vlasova G. A., Osipov A. N. Binary Reverse Codes for Byte Error Control. *Proceedings of the National Academy of Sciences of Belarus.* (1), 127-131 (in Russian).

8. Vlasova G. A., Konopelko V. K. (1998) Decoding of BCH Codes with Error Identification. *Digital signal processing and its applications.* Vol. II-E, II-E-55–II-E-58.

Сведения об авторе

Власова Г.А., канд. техн. наук, доц., доцент кафедры информационных систем и технологий, Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, g.vlasova@bsuir.by.

Information about the author

Vlasova G.A., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Systems and Technologies, Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", g.vlasova@bsuir.by.

УДК 004.056:621.311.1

КИБЕРАТАКИ НА КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С.Ю. Воробьев, Е.А. Ханчевский
РУП «Белэнергосетьпроект», Минск, Беларусь

Аннотация. Энергетика является одной из наиболее важных отраслей национальной экономики государства. Кибератаки на энергетические объекты могут привести к сбоям в подаче электроэнергии, авариям, значительному экономическому ущербу, человеческим жертвам. В данной статье рассмотрена тенденция государств к созданию киберподразделений в составе национальных вооруженных сил, проведению в киберпространстве учебных и боевых операций, сделан акцент на внимании, уделяемом руководством Республики Беларусь вопросам кибербезопасности и защиты критически важной инфраструктуры от кибератак, приведены кейсы зафиксированных инцидентов на объектах энергетики вследствие применения кибероружия. Перечислены основные нормативные правовые акты, регулирующие вопросы информационной безопасности и защиты информации, в том числе по вопросам организации противодействия кибератакам. В качестве примера описаны мероприятия организационного, правового и технического характера, осуществленные на одном из предприятий ГПО «Белэнерго» Министерства энергетики Республики Беларусь.
Ключевые слова: кибератака; кибербезопасность; защита информации; информационная безопасность; энергетика; объекты энергетики; жизнеобеспечение; критически важный объект; критически важный объект информатизации; гибридная война.

CYBER ATTACKS ON CRITICAL ENERGY INDUSTRY FACILITIES

S.Yu. Vorobyov, E.A. Khanchevsky
RUE «Belenergosetproekt», Minsk, Belarus

Abstract. Energy is one of the most important sectors of the national economy of the state. Cyber attacks on energy facilities can lead to power outages, accidents, significant economic damage, and casualties. This article examines the tendency of states to create cyber units as part of national armed forces, conduct training and combat operations in cyberspace, emphasizes the attention paid by the leadership of the Republic of Belarus to issues of cybersecurity and protection of critical infrastructure from cyber attacks, and provides cases of recorded incidents at energy facilities due to the use of cyber weapons. The main regulatory legal acts governing information security and information protection issues, including those related to organizing counteraction to cyber attacks, are listed. As an example, organizational, legal and technical measures implemented at one of the enterprises of the State Production Association «Belenergo» of the Ministry of Energy of the Republic of Belarus are described.
Keywords: cyber attack; cyber security; information protection; information security; energy; energy facilities; life support; critical facility; critical information facility; hybrid war.

Введение

Республика Беларусь на современном этапе развития представляет собой состоявшееся правовое, демократическое и суверенное государство, которое проводит миролюбивую внешнюю и социально ориентированную внутреннюю политики и вместе с тем в силу своего географического положения и открытости в полной мере подвержена большинству геополитических процессов, происходящих в мире. Среди прочих перед государством стоит масштабная задача по развитию, поддержанию и совершенствованию системы обеспечения кибербезопасности.

Основная часть

Тенденцией последних двух десятилетий явилась «милитаризация» киберпространства. Военно-политический блок НАТО в 2016 году на Варшавском саммите официально объявил киберпространство новой сферой проведения операций –

наряду с воздушной, сухопутной и морской [1]. Менее чем в 800 км от Минска в Таллине функционирует Центр передового опыта по совместной киберзащите НАТО, на базе которого проходят многочисленные учения и тренировки, в том числе флагманские ежегодные учения НАТО по действиям в киберпространстве «Кибер Коалиция».

Следует отметить, что Соединенные Штаты – одна из немногих стран, государственная политика которых рассматривает киберпространство как поле боя, а потому направлена на полный контроль этой сферы при наличии средств и возможностей на осуществление этого контроля [2]. При этом в США циркулирует концепция так называемой «дешевой войны» (War on the Cheap), сторонники которой утверждают, что один миллион долларов и 20 человек, проводя компьютерные атаки, могут обеспечить успех, сопоставимый с действиями многотысячной группировки войск [3].

Кратно вырос круг государств, создавших или создающих в составе национальных вооруженных сил подразделения информационной безопасности, включая кибервойска, задачей которых является проведение кибероперации. Реальный практический «боевой» опыт в киберпространстве имеют подразделения вооруженных сил США, Китая, КНДР, Ирана и др. Подразделение радиоэлектронной разведки «8200» Армии обороны Израиля известно не только участием в успешных кибератаках на иранские объекты атомной энергетики, но и тем, что выходцы из «8200» являются зачинателями многочисленных прибыльных стартапов в сфере информационной безопасности, например, Check Point Software Technologies Ltd.

Особый интерес представляет тот факт, что Министерство энергетики Соединенных Штатов наряду с такими спецслужбами, как ЦРУ, ФБР, АНБ, РУМО, входит в состав разведывательного сообщества США. В составе Министерства энергетики США действует Управление разведки и контрразведки, основными задачами которого являются научно-техническая разведка в ядерной области и защита ядерных секретов. В феврале 2016 года Министерство энергетики США официально объявило о создании Управления по кибербезопасности, энергетической безопасности и экстренному реагированию (структурно вошло в состав Управления разведки и контразведки) [4]. Необходимо отметить, что Соединенные Штаты со всей серьезностью относятся к защите электроэнергетической системы от киберугроз в связи с чрезвычайной значимостью энергетического сектора национальной инфраструктуры.

Президент Республики Беларусь неоднократно обращал внимание на особую опасность, такого элемента гибридной войны, используемого против Республики Беларусь, как кибератаки, их направленность на экономические объекты, предприятия, банковскую систему, основные пункты жизнеобеспечения, отмечал, что целью кибератак является нанесение максимального ущерба экономике и дестабилизация общества.

Глубокое проникновение энергетики во все отрасли экономики и в социальную сферу определяет ее особую роль в сфере безопасности. Система управления энергосистемой должна быть устойчивой к кибервоздействиям. Достигшая поставленных целей кибератака с высокой вероятностью нанесет урон сопоставимый с применением ядерного оружия: отключение важных инфраструктурных объектов мгновенно введет в хаос крупные мегаполисы и целые регионы [5]. Среди зафиксированных кибератак наибольший интерес вызывают следующие:

– инцидент на Игналинской АЭС (Литва) в 1994 году;

– совместная операция «Олимпийские игры» спецслужб США и Израиля по выведению из строя объектов атомной энергетики Ирана с применением

компьютерного вируса Stuxnet (данный вредонос был обнаружен в 2010 году белорусской антивирусной компанией);

– внедрение вредоносного программного обеспечения в информационные системы Korea Hydro & Nuclear Power Co., Ltd в 2014 году и немецкой АЭС «Gundremmingen» в 2015 [6].

Защита критически важной инфраструктуры является одной из наиболее важных задач обеспечения национальной безопасности любой страны. В целях обеспечения национальных интересов в Республике Беларусь на нормативном уровне осуществляется выделение и регламентирование функционирования критически важных объектов информатизации на основании критериев социальной, экономической, экологической и информационной значимости.

В целях повышения уровня защиты национальной инфраструктуры от внешних и внутренних угроз Президентом Республики Беларусь 14.02.2023 подписан Указ № 40 «О кибербезопасности», регулирующий основные принципы создания и функционирования национальной системы обеспечения кибербезопасности, который по сути является правовым фундаментом национальной системы обеспечения кибербезопасности, и направленный на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности. В рамках реализации данного указа Оперативно-аналитическим центром при Президенте Республики Беларусь 25.07.2023 был издан приказ № 130, а Совет Министров Республики Беларусь 23.02.2024 принял постановление № 120.

Обеспечение надлежащего уровня безопасности достигается путем выполнения комплекса организационных, правовых и технических мероприятий. В качестве примера приведем обстановку, сложившуюся по состоянию на текущий момент времени на предприятии, структурно входящем в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее - Предприятие). Так, на Предприятии осуществлено:

– создание подразделения информационной безопасности в структуре Предприятия;

– разработка и актуализация локальных правовых актов (ЛПА), регулирующих вопросы информационной безопасности и защиты информации;

– проведение на постоянной основе инструктажей с работниками Предприятия, имеющими доступ с автоматизированных рабочих мест к ресурсам сети Интернет и почтовым сервисам;

– повышение квалификации руководителей структурных подразделений и работников Предприятия на тематических курсах, семинарах, конференциях и иных обучающих мероприятиях, посвященных вопросам информационной безопасности и защиты информации;

– получение лицензии на деятельность по технической и (или) криптографической защите информации в части проектирования систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

– запланировано к приобретению и внедрению сертифицированная в Республике Беларусь система предотвращения утечек конфиденциальной информации (DLP-система).

В целях совершенствования нормативного правового регулирования защиты информации и обеспечения кибербезопасности были подготовлены и направлены предложения в адрес регулятора.

В рамках проектирования строительства (реконструкции) объектов энергосистемы, предусматривающего, в том числе создание (модернизацию) информационных систем, осуществляется разработка соответствующего раздела «Информационная безопасность».

В настоящее время на Предприятии осуществляется разработка и внедрение системы менеджмента информационной безопасности на соответствие требованиям СТБ ISO/IEC 27001 (запланировано получение сертификата в Национальной системе подтверждения соответствия Республики Беларусь на систему менеджмента информационной безопасности).

Заключение

Слабым местом растущей цифровизации энергосистемы является «чувствительность» последней к кибератакам. Последние, при надлежащей подготовке, выборе цели, приложении сил и средств, теоретически могут вывести из строя энергетическую сеть целой страны. В Республике Беларусь на государственном уровне уделяется внимание вопросам кибербезопасности и организации противодействия кибератакам, осуществляется поддержка и поощрение к применению лучших практик применения кибербезопасности. Действующая нормативная правовая база, регулирующая вопросы информационной безопасности и защиты информации, позволяет реализовывать Предприятию комплекс правовых, организационных и технических мероприятий, в том числе с запланированной сертификацией системы менеджмента информационной безопасности в Национальной системе подтверждения соответствия Республики Беларусь.

Список использованных источников

1. Белоус А. И., Солодуха В. А. (2021) *Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения.* Москва, Издательство «Техносфера».

2. Харрис Ш. (2020) *Кибервойна@: Пятый театр военных действий*. Москва, Издательство «Альпина нон-фикшн».

3. Бартош А. А. (2023) *Гибридная война.* Москва, Издательство «КНОРУС».

4. Белоус А. И. (2020) *Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения.* Москва; Вологда, Издательство «Инфра-Инженерия».

5. Белоус А. И. (2020) *Кибероружие и кибербезопасность. О сложных вещах простыми словами.* Москва; Вологда, Издательство «Инфра-Инженерия».

6. Воробьев С. Ю., Ханчевский Е. А. (2024) Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности. *Энергетическая стратегия*. (6), 33–36.

References

1. Belous A. I., Solodukha V. A. (2021) *Fundamentals of Cybersecurity. Standards, Concepts, Methods and Means of Support.* Moscow, Technosfera Publishing House (in Russian).

2. Harris S. (2020) *Cyberwar@: The Fifth Theater of Military Operations.* Moscow, Alpina Non-Fiction Publishing House (in Russian).

3. Bartosh A. A. (2023) *Hybrid War*. Moscow, KNORUS Publishing House (in Russian).

4. Belous A. I. (2020) *Cybersecurity of fuel and energy complex facilities. Concepts, methods and means of support.* Moscow; Vologda, Infra-Engineering Publishing House (in Russian).

5. Belous A. I. (2020) *Cyberweapons and cyber security. About complex things in simple words.* Moscow; Vologda, Infra-Engineering Publishing House (in Russian).

6. Vorobyov S. Yu., Khanchevsky E. A. (2024) Cyberattacks on critical energy facilities as a source of threats to national security. *Energy strategy.* (6), 33–36 (in Russian).

Сведения об авторах

Воробьев С. Ю., магистр техн. наук, заведующий сектором информационной безопасности отдела информационных технологий,
РУП «Белэнергосетьпроект», s.varabyou@besp.by.
Ханчевский Е. А., начальник отдела информационных технологий,
РУП «Белэнергосетьпроект», zh@besp.by.

Information about the authors

Vorobyov S.Yu., Master of Engineering. Sciences, Head of the Information Security Sector of the Information Technology Department,
RUE «Belenergosetproekt», s.varabyou@besp.by.
Khanchevsky E.A., Head of Information Technology Department, RUE «Belenergosetproekt», zh@besp.by

УДК 537.874.6

ДИЭЛЕКТРИЧЕСКАЯ И МАГНИТНАЯ СОСТАВЛЯЮЩИЕ РАДИОПОГЛОЩАЮЩЕГО НАНОКОМПОЗИТА НА ОСНОВЕ УГЛЕРОДНЫХ НАНОТРУБОК

Ю. Ву, С.Л. Прищепа
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Рассматривается радиопоглощающий материал на основе углеродных нанотрубок с инкорпорированными наночастицами ферромагнитного металла. Эффективность поглощения электромагнитного излучения в этом случае определяется не только диэлектрической проницаемостью, но и магнитной составляющей нанокомпозита. Предлагается модельная структура для описания свойств подобных нанокомпозитов. С учетом экспериментальных данных учитывается возможность окисления поверхности ферромагнитных наночастиц. В силу этого каждая наночастица представляется в виде сложной структуры типа ядро/оболочка. Приводятся выражения, описывающие вклад магнитной и диэлектрической составляющих в экранирующие свойства нанокомпозита. При этом уравнения записаны в удобной для расчетов форме и включают в себя необходимые материальные параметры. Это позволит в будущем оценить коэффициент распространения плоской электромагнитной волны в нанокомпозите на основе УНТ, коэффициенты поглощения и отражения, что даст возможность моделировать эффективность экранирования электромагнитного излучения в широком диапазоне частот.
Ключевые слова: радиопоглощающие материалы; нанокомпозиты; углеродные нанотрубки; ферромагнетики; наночастицы; магнитная проницаемость; диэлектрическая проницаемость; структура ядро/оболочка; разупорядоченная структура; проводимость.

DIELECTRIC AND MAGNETIC COMPONENTS OF A RADIO-ABSORBING NANOCOMPOSITE BASED ON CARBON NANOTUBES

Y. Wu, S.L. Prischepa
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. A radio-absorbing material based on carbon nanotubes with embedded ferromagnetic metal nanoparticles is considered. The efficiency of electromagnetic radiation absorption in this case is determined not only by the permittivity, but also by the magnetic component of the nanocomposite. A model structure is proposed to describe the properties of such nanocomposites. Taking into account experimental data, the possibility of oxidation of the surface of ferromagnetic nanoparticles is taken into account. Due to this, each nanoparticle is represented as a complex core/shell structure. Expressions are given that describe the contribution of the magnetic and dielectric components to the shielding properties of the nanocomposite. The equations are written in a form convenient for calculations and include the actual material parameters. This will make it possible to estimate the propagation coefficient of a plane electromagnetic wave in a CNT-based nanocomposite, the absorption and reflection coefficients, which will subsequently make it possible to model the efficiency of shielding electromagnetic radiation in a wide frequency range.
Keywords: radio-absorbing materials; nanocomposites; carbon nanotubes; ferromagnets; nanoparticles; magnetic permeability; permittivity; core/shell structure; disordered structure; conductivity.

Введение

Радиопоглощающие материалы (РПМ) находят широкое применение в радиолокационной технике и различных средствах технической защиты информации. В последние годы большое значение уделяется наноструктурированным композитам, способным обеспечивать высокую степень поглощения и/или экранирования электромагнитного излучения на различных частотах. К таковым можно отнести нанометаллы и сплавы, нанооксиды, наноферриты, нанографит, нано-SiC, нано-SiN, наноструктурированные проводящие полимеры и углеродные нанотрубки (УНТ). Среди перечисленных наноструктурированных материалов УНТ являются весьма перспективными компонентами РПМ [1,2]. Они обладают высокой прочностью, а также электро- и теплопроводностью. Исследования поглощения СВЧ излучения нанокомпозитами на основе УНТ получили большой импульс благодаря особенностям их синтеза. УНТ формируются методом химического парофазного осаждения (ХПО) с применением катализатора на основе ферромагнитных 3d металлов. Поглощающие свойства нанокомпозитов на основе УНТ в первую очередь определяются омическими и диэлектрическими потерями. Однако интеркаляция магнитных наночастиц в матрицу УНТ приводит к увеличению поглощающих свойств нанокомпозитов из-за магнитных потерь. Эффективность экранирования материала при этом возрастает [3,4].

В данной работе проведена адаптация метода Грановского и др. [5] для описания поглощающих свойств нанокомпозита на основе УНТ с инкорпорированными наночастицами ферромагнетика.

Результаты

Рассмотрим разупорядоченную структуру, содержащую магнитные проводящие наночастицы в проводящей среде. Схематически модельный образец представлен на рисунке 1. Каждая наночастица представляет собой структуру типа металлическое ядро/диэлектрическая оболочка. Индексы 1 на рисунке 1 относятся к материалу матрицы (в данном случае УНТ), индексы 2 – к материалу ферромагнитной наночастицы, индексы 3 – к оболочке.

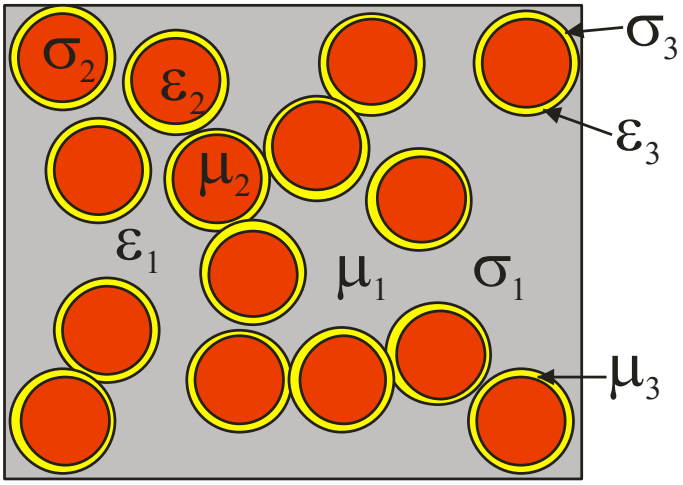


Рис. 1. Схематическое представление модельного образца
Fig. 1. Schematic representation of the model sample

Исходное уравнение для разупорядоченной структуры нанокомпозита в форме, удобной для вычисления значений магнитной проницаемости запишется как

$$-2Q_{\mu}\mu^{2}(\omega)+\mu(\omega)\left[(3c_{V}-1)-\mu_{1}Q_{\mu}(3c_{V}-2)\right]+\mu_{1}=0, \quad (1)$$

где параметр Q_{μ} характеризует воздействие свойств наночастицы и ее оболочки на магнитную проницаемость,

$$Q_{\mu}=\frac{1}{\mu_{2}}-\frac{i\omega\cdot a\mu_{0}}{2\rho_{s}}. \quad (2)$$

Уравнение (1) получено адаптируя результаты работы [5] для нанокомпозита, состоящего из проводящей матрицы с хаотично расположенными ферромагнитными наночастицами со структурой типа ядро/оболочка. В уравнениях (1) и (2) μ_1 – относительная магнитная проницаемость среды УНТ, μ_2 – относительная магнитная проницаемость наночастиц, μ_0 – магнитная проницаемость вакуума, а – характерный размер наночастиц, $\rho_S=\rho_{S0}(1+ik\omega_0/\omega)$ – поверхностное сопротивление оболочки, которая окружает проводящую наночастицу, ρ_{S0}– сопротивление этой оболочки на постоянном токе, ω – циклическая частота электромагнитного излучения, ω_0 – циклическая частота квазимагнитного резонанса в упорядоченной структуре, *k* – отношение мнимой части ρ_S к ее реальной части на частоте ω_0. Как правило, величина k зависит от свойств среды УНТ и включенных наночастиц.

Решение уравнения (1) запишем в виде, содержащем функцию только одного параметра, что представляет удобство для проведения практических расчетов,

$$\mu(\omega)=\sqrt{\mu_{1}/2Q_{\mu}}\,\eta\phi(\eta), \quad (3)$$

где функция

$$\phi(\eta)=\left(1+\sqrt{1+\eta^{-2}}\right) \quad (4)$$

зависит от параметра

$$\eta=\frac{[(3c_{V}-1)-\mu_{1}Q_{\mu}(3c_{V}-2)]}{\sqrt{8\mu_{1}Q_{\mu}}}. \quad (5)$$

Для диэлектрический проницаемости получено следующее уравнение,

$$\varepsilon(\omega)=\sqrt{\varepsilon_{1}\left(1+\beta M^{2}\right)/2Q_{\varepsilon}}\,\xi\phi(\xi), \quad (6)$$

где функция $\phi(\xi)$ определяется уравнением (4) и параметр ξ выражается как

$$\xi=\frac{(3c_{V}-1)-\varepsilon_{1}(1+\beta M^{2})Q_{\varepsilon}(3c_{V}-2)}{\sqrt{8\varepsilon_{1}\left(1+\beta M^{2}\right)Q_{\varepsilon}}}. \quad (7)$$

Характерной особенностью полученных уравнений (3) и (6) является наличие материальных параметров нанокомпозита, которые определяют его диэлектрическую и магнитную проницаемости. В частности, из уравнений (1) – (7) следует, что магнитная

и диэлектрическая проницаемости магнитного нанокомпозита сложным образом зависят от концентрации и размеров наночастиц, диэлектрической и магнитной проницаемостей среды УНТ и наночастиц, а также сопротивления оболочки наночастиц.

Заключение

Проведенный анализ позволяет оценить коэффициент распространения плоской электромагнитной волны в нанокомпозите на основе УНТ, коэффициенты поглощения и отражения, что в последующем даст возможность моделировать эффективность экранирования электромагнитного излучения в широком диапазоне частот.

References

1. Gupta S., Tai N. (2019) Carbon Materials and their Composites for Electromagnetic Interference Shielding Effectiveness in X-band. *Carbon*. 152, 159–187.

2. Wu G., Chen Y., Zhan H., Chen H.T., Lin J.H., Wang J.N., et al. (2020) Ultrathin and Flexible Carbon Nanotube/Polymer Composite Films with Excellent Mechanical Strength and Electromagnetic Interference Shielding. *Carbon*. 158, 472–480.

3. Labunov V. A., Danilyuk F. L., Prudnikava A. L., Komissarov I., Shulitski B. G., Speisser C., et al. (2012) Microwave Absorption in Nanocomposite Material of Magnetically Functionalized Carbon Nanotubes. *Journal of Applied Physics*, 112 (2), 024302.

4. Çakmakçı N., Kim G., Song H., Shin M., Jung Y., Jeong Y. (2023) Ferrite-decorated Ultrathin and Lightweight Carbon Nanotube Film for Electromagnetic Interference Shielding. *ACS Applied Nano Mater*ials. 6 (19), 18229–18237.

5. Granovsky A. B., Bykov I. V., Ganshina E. A., Gushchin V. S., Inoue M., Kalinin Yu. E., et al. (2003) Magnetorefractive Effect in Magnetic Nanocomposites. *Journal of Experimental and Theoretical Physics.* 96 (4), 1104–1112.

Сведения об авторах

Ву Ю., магистрант кафедры защита информации, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР), ilmsiaoms@gmail.com.
Прищепа С.Л., д-р физ.-мат. наук, проф., проф. кафедры защита информации БГУИР, prischepa@bsuir.by.

Information about the authors

Wu Y., Master Student, Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics" (BSUIR), ilmsiaoms@gmail.com.
Prischepa S.L., Dr. of Sci. (Phys. and Math.), Professor, Professor at the Department of Information Security, BSUIR, prischepa@bsuir.by.

УДК 614.841

ТЕХНИЧЕСКИЕ СРЕДСТВА ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ ПАРКИНГА

В.Е. Галузо, А.И. Пинаев
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Перспективы применения воздушных завес и струйной вентиляции в системах противодымной защиты паркингов (гаражей стоянок). Воздушные завесы над проемами со стороны помещения хранения транспортных средств посредством настильных воздушных струй от сопловых аппаратов рекомендованы техническими нормативно-правовыми актами (ТНПА). Однако, эти технические средства не нашли широкого применения из-за отсутствия в ТНПА конкретных рекомендаций по проектированию, что обусловлено недостаточным изучением их использования. Целью работы стало выявление недостатков противопожарного нормирования использования воздушных завес

в системе противодымной защиты, а также поиск возможных путей дальнейших исследований в данной области. В частности, предложено строить системы противодымной защиты паркингов на основе струйных систем вентиляции, включающих в себя воздушные завесы. Конкретные практические рекомендации по их проектированию в виду сложности проведения натурных испытаний могут быть разработаны на основе трехмерного математического CFD (Computational Fluid Dynamics - вычислительная гидрогазодинамика) моделирования.
Ключевые слова: пожарная безопасность; паркинг; противодымная защита; противодымная вентиляция; воздушная завеса; струйные системы вентиляции; CFD моделирование.

PARKING FIRE PROTECTION TECHNICAL MEANS

V.E. Galuzo, A.I. Pinaev
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Prospects for the use of jet ventilation air curtains in smoke protection systems for parking lots (parking garages). Air curtains over openings on the side of the vehicle storage room using flat air jets from nozzle devices are recommended by technical regulations (TNLA). However, these technical means have not been widely used due to the lack of specific design recommendations in TNLA, which is due to insufficient study of their use. The purpose of the work was to identify the shortcomings of fire safety regulations for the use of air curtains in the smoke protection system, as well as to find possible ways for further research in this area. n particular, it is proposed to build smoke protection systems for parking lots based on jet ventilation systems that include air curtains. Specific practical recommendations for their design, due to the complexity of conducting full-scale tests, can be developed on the basis of three-dimensional mathematical CFD (Computational Fluid Dynamics) modeling.
Keywords: fire safety; parking; smoke protection; smoke ventilation; air curtain; jet ventilation systems; CFD modeling.

Введение

Паркингам уделяется особое внимание в нашей стране. Это подтверждается тем, что их строительство, а также работы по проектированию, монтажу, наладке и техническому обслуживанию систем обеспечения жизнедеятельности паркингов освобождены от налога на добавленную стоимость.

С целью благоустройства территорий, прилегающих к жилым, административным, торгово-развлекательным и другим объектам, паркинги строятся под этими объектами, что также обусловлено и снижением стоимости их строительства.

Согласно техническим нормативно-правовым актам (ТНПА) паркинги, и особенно, закрытые, что как правило имеет место при их расположении под объектами должны быть оборудованы системами противопожарной защиты (ППЗ). То обстоятельство, что эти паркинги встроены в объекты с массовым пребыванием людей накладывает особый отпечаток на надежность функционирования систем ППЗ в них.

В соответствии с актуальными ТНПА на закрытых паркингах должны быть системы пожаротушения, оповещения о пожаре и противодымной защиты (ПДЗ). Системам ПДЗ уделяется самое пристальное внимание, что подтверждается тем, что это единственные системы противопожарной защиты, которые должны испытываться аккредитованными при Госстандарте испытательными лабораториями. Кроме того, за последние десять лет были разработаны пять новых ТНПА в области проектирования и испытания систем ПДЗ.

Основная часть

Согласно СН 2.02.07-2020 из помещений для хранения автомобилей закрытых гаражей-стоянок (паркингов) необходимо предусматривать удаление продуктов горения при пожаре системами вытяжной противодымной вентиляции (дымоудаления). Дымоудаление осуществляется через клапаны, установленные на вентиляционных шахтах, размещенных в пространстве паркинга.

В случае многоэтажных паркингов въезд на каждый этаж с рампы (пандуса) осуществляется через въездные противопожарные ворота (проемы).

В соответствии с СН 3.02.03-2019 в противопожарных стенах и перекрытиях 1-го типа гаражей-стоянок заполнения проемов следует предусматривать по СН 2.02.05-2020 и (или) путем устройства воздушной завесы над проемами со стороны помещения хранения транспортных средств посредством настильных воздушных струй от сопловых аппаратов со скоростью истечения воздуха не менее 10 м/с при начальной толщине струи не менее 0,03 м и ширине струи не менее ширины защищаемого проема. Объемный расход воздуха, подаваемого сопловым аппаратом, при ширине ворот 4 м составляет 4320 м^3/ч.

Это положение почти дословно заимствовано из СП 154.13130.2013, в котором в отличие от СН 3.02.03-2019 четко сказано, что воздушная завеса располагается над противопожарными воротами 1-го типа. В обоих ТНПА не учитывается угол выпуска струи завесы к плоскости проема, который как показано в [1] существенно влияет на эффективность работы воздушных завес для защиты проемов в условиях пожара.

В проведенных в Академии ГПС МЧС исследованиях [2] было показано, что при некоторых параметрах струи через защищаемый проем вдоль пола возможно истечение горячих газов (смесь продуктов горения и воздуха) в соседнее защищаемое помещение. Например, при больших скоростях воздушной струи (более 10 м/с) вероятен захват ею дыма из припотолочного слоя и распространения его по помещению как очага пожара, так и защищаемого (при открытом проеме) после соприкосновения (удара) струи с полом помещения. Таким образом, подчеркивается то, что вертикальная завеса неэффективна.

В пространстве паркинга согласно СН 2.02.07-2020 должно осуществляться дымоудаление вентиляционными системами с механическим побуждением. Для компенсации удаляемой газодымовой смеси из дымовой зоны помещения паркинга в объеме равном приблизительно 45000 м^3/ч (согласно расчету, приведенному в СН 2.02.02-2023) должен быть обеспечен приток воздуха, который на практике осуществляется через открытые ворота въезда на паркинг. А это означает, что через ворота, защищаемые завесой с производительностью 4320 м^3/ч дует ветер компенсирующей подачи воздуха при включенном дымоудалении в 10 раз (45000 м^3/) превышающий производительность завесы, который тем более не пустит дым из паркинга на рампу.

То, что воздушная завеса в паркингах не часто реализуема из-за отсутствия понятных практических рекомендаций по ее проектированию, подтверждается тем фактом, что рекомендована она в строительных нормах 2019 года, а методика их испытаний предложена только в последней редакции НПБ 23-2010, вступившей в силу в 2025 году. Причем эта методика не соответствует ГОСТ 12.3.018-79, на который сделана ссылка в НПБ.

Зона действия для дымоприемного отверстия согласно СН 2.02.07-2020 не должна превышать 1 000 м^2. Это приводит к тому что в паркингах большей площади необходимо проектировать несколько шахт дымоудаления или от одной шахты прокладывать в пределах этажа паркинга сеть воздуховодов большого сечения.

В паркинге при пожаре должна быть обеспечена незадымляемая зона, достаточная по высоте для безопасной эвакуации людей и работы пожарных. Наличие воздуховодов приводит к увеличению высоты помещений паркинга. Кроме того, как было сказано выше для нераспространения пожара и продуктов горения из помещения паркинга в другие помещения рекомендуется использовать воздушные завесы. Все это повышает стоимость системы ПДЗ.

Одним из возможных выходов из сложившейся ситуации является использование струйных вентиляторов [3,4]. На рис.1 приведена схема системы струйной вентиляции, поясняющая ее работу. В качестве приточной вентиляции могут использоваться сопловые аппараты, используемые для воздушных завес, рассмотренных выше. Струйная вентиляция будет выполнять как функцию защиты проемов на выезде из этажа паркинга на рампу, так и дымоудаления.

Струйная продольная противодымная вентиляция обеспечивает удержание нижней границы распространения дыма в течение времени, необходимого для эвакуации людей. Для продольной системы противодымной вентиляции высота потолка не является фактором риска [5].

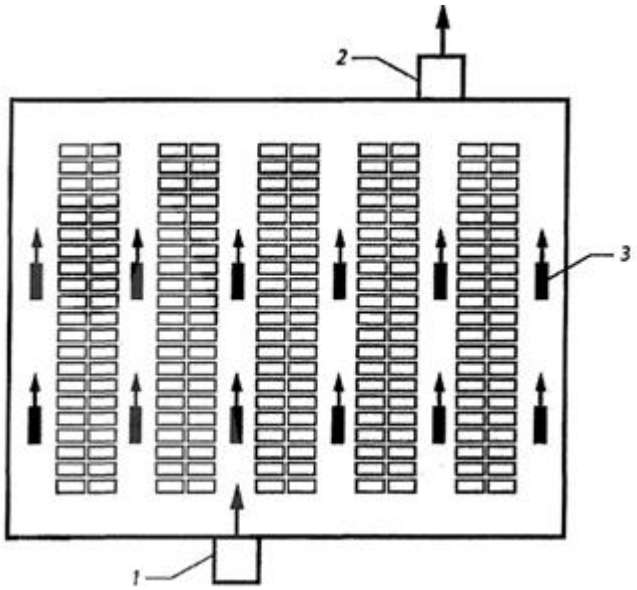


Рис. 1. Схема системы струйной вентиляции: *1* - приточная вентиляция; *2* – вытяжная вентиляция*;* *3* –струйный вентилятор

Fig. 1. Scheme of the jet ventilation system: 1 – supply ventilation; 2 – exhaust ventilation; 3 – jet fan

Проектирование струйной системы противодымной вентиляции паркинга должно быть основано на численном CFD-моделировании процессов воздухораспределения, которое можно назвать аэродинамическими испытаниями вентиляции методами вычислительной гидродинамики. CFD-модель позволяет проверить проектные решения и, если надо, внести в проект изменения.

Заключение

На основе анализа технических нормативно-правовых актов и работ в области проектирования противодымной защиты закрытых гаражей-стоянок (паркингов) сделан вывод о недостаточном исследовании эффективности воздушных завес, что ограничивает их применение.

Предлагается использовать для реализации систем противодымной защиты закрытых паркингов системы струйной вентиляции, которые удаляя газодымовую смесь при пожаре обеспечивают незадымляемую зону в течение времени, необходимого для эвакуации людей. Кроме того, системы струйной вентиляции будут выполнять функцию защиты проемов на выезде из этажа паркинга на рампу вместо отдельных воздушных завес.

Проектирование струйной системы противодымной вентиляции паркинга должно быть основано на численном CFD - моделировании процессов воздухораспределения.

Список использованных источников

1. Xing Yu, Fang Liu, Tarek Beji, Miao-Cheng Weng, BartMerci (2018) Experimental study of the effectiveness of air curtains ofvariable width and injection angle to block fire-induced smoke in atunnel configuration International. *Journal of Thermal Sciences.* (*134), 13–26.*

2. Пузач С. В., Панов М. В. (2001) Закономерности тепломассообмена в помещении в условия пожара при защите проема воздушной завесой. *Проблемы пожарной безопасности в строительстве. Материалы науч.-практ. конф. М.: Академия ГПС МВД России.*

3. Есин В.М., Калмыков С.П. (2006) Использование струйных вентиляторов в системах дымоудаления автостоянок. *Инженерные системы зданий. Журнал АВОК (2), 60.*

4. Есин В.М., Калмыков С.П. (2007) Обоснование основных параметров, обеспечивающих эффективную работу системы дымоудаления и вентиляции автостоянки закрытого типа при помощи струйных вентиляторов. *Журнал Пожаровзрывобезопасность, 16 (3), 54-62.*

5. Свердлов А. В., Волков А. П., Рыков С. В., Волков М. А., Барафанова Е. Ю. (2019) Моделирование процессов дымоудаления в подземных сооружениях транспортного назначения. *Вестник Международной академии холода, (1), 3–10.*

References

1. Xing Yu, Fang Liu, Tarek Beji, Miao-Cheng Weng, BartMerci (2018) Experimental study of the effectiveness of air curtains ofvariable width and injection angle to block fire-induced smoke in atunnel configuration International. *Journal of Thermal Sciences.* (*134), 13–26.*

2. Puzach S.V., Panov M.V. (2001) Regularities of heat and mass transfer in a room under fire conditions when protecting the opening with an air curtain. Problems of fire safety in construction. Scientific and practical materials. conf. M.: Academy of State Fire Service of the Ministry of Internal Affairs of Russia.

3. Esin V.M., Kalmykov S.P. (2006) Use of jet fans in car park smoke removal systems. Engineering systems of buildings. ABOK Journal (2), 60.

4. Esin V.M., Kalmykov S.P. (2007) Justification of the main parameters ensuring the effective operation of the smoke removal and ventilation system of a closed parking lot using jet fans. Journal of Fire and Explosion Safety, 16 (3), 54-62.

5. Sverdlov A. V., Volkov A. P., Rykov S. V., Volkov M. A., Barafanova E. Yu. (2019) Modeling of smoke removal processes in underground transport structures appointments. Bulletin of the International Academy of Refrigeration, (1), 3–10.

Сведения об авторах

Галузо В.Е., канд. техн. наук, доц., доцент, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», valga51@yandex.ru.

Пинаев А.И., канд. техн. наук, доц., доцент, Белорусский государственный университет информатики и радиоэлектроники, info@avsm.by.

Information about the authors

Galuzo V.E., Ph.D. tech. Sciences, Associate Professor, Associate Professor, Belarusian State University of Informatics and Radio Electronics, valga51@yandex.ru.

Pinaev A.I., Ph.D. tech. Sciences, Associate Professor, Associate Professor, Belarusian State University of Informatics and Radio Electronics, info@avsm.by.

.

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ АКТИВАЦИИ ПОДПИСИ В СИСТЕМЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В.А. Герасимов
Государственное предприятие «Научно-исследовательский институт технической защиты информации», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается система электронной цифровой подписи на основе виртуальной инфраструктуры и ее преимущества перед традиционными решениями. Внедрение такой системы позволяет пользователям избежать необходимости хранения личных ключей, однако связано с таким риском информационной безопасности, как взлом сервера. Для минимизации этого риска предложен протокол активации подписи, который обеспечивает контроль над использованием личного ключа. Автор статьи анализирует реализации протокола активации подписи, основывающиеся на различных методах аутентификации. Представлены ключевые характеристики и проект разработанного протокола активации подписи, направленный на повышение уровня безопасности. В результате исследования определены уязвимости и векторы атак, что позволяет в дальнейшем совершенствовать протоколы активации подписи и повысить доверие пользователей к системе электронной цифровой подписи на основе виртуальной инфраструктуры.
Ключевые слова: облачная электронная цифровая подпись на основе виртуальной инфраструктуры; данные активации подписи; протокол активации подписи.

COMPARATIVE ANALYSIS OF SIGNATURE ACTIVATION PROTOCOLS IN AN ELECTRONIC DIGITAL SIGNATURE SYSTEM BASED ON A VIRTUAL INFRASTRUCTURE

V.A. Herasimov
Scientific production republican unitary enterprise "Research institute for technical protection of information", Minsk, Republic of Belarus

Abstract. The article discusses an electronic digital signature system based on a virtual infrastructure and its advantages over traditional solutions. The implementation of such a system allows users to avoid the need to store private keys, however, it is associated with such an information security risk as hacking the server. To minimize this risk, a signature activation protocol has been proposed that provides control over the use of a private key. The author of the article analyzes the implementation of the signature activation protocol based on various authentication methods. The key characteristics and draft of the developed signature activation protocol aimed at increasing the security level are presented. As a result of the study, vulnerabilities and attack vectors were identified, which makes it possible to further improve signature activation protocols and increase user confidence in an electronic digital signature system based on a virtual infrastructure.
Keywords: cloud-based electronic digital signature based on virtual infrastructure; signature activation data; signature activation protocol.

Введение

Система электронной цифровой подписи на основе виртуальной структуры (далее – облачная ЭЦП) имеет очевидные преимущества для пользователей по сравнению с традиционными решениями использования электронной цифровой подписи, основанными на использовании USB-токенов или специальных SIM-карт (далее – ЭЦП).

Несмотря на обозначенное преимущество системы облачной ЭЦП, следует отметить, что ее эксплуатация сопряжена со следующими рисками информационной безопасности:

– взлома сервера [1];

– компрометация сервера

Для минимизации указанных рисков необходимо применять протокол активации подписи (далее – ПАП). Этот протокол реализуется между двумя сторонами: клиентской программой пользователя (далее – КПП) и сервером подписи (далее – СП). Основная задача протокола заключается в том, чтобы сервер получил разрешение от пользователя на использование его ключа для подписи определенного документа.

Консорциум облачной подписи (Cloud Signature Consortium, далее – CSC) [2] представляет собой объединение компаний и научных учреждений, занимающееся разработкой технических стандартов в сфере облачной ЭЦП. На данный момент ключевым документом, созданным в рамках CSC, является спецификация, которая описывает программный интерфейс (API) для взаимодействия со службами облачной подписи, а также шаги, необходимые для получения электронного документа.

В рамках анализа уязвимостей ПАП, а также анализа векторов атак на существующие системы, использующие ПАП, были выполнены следующие задачи:

– определены ключевые характеристики и особенности различных протоколов активации подписи;

– проанализированы преимущества и недостатки каждого протокола с точки зрения безопасности, производительности и удобства использования;

– сформирован проект ПАП, который опирается на данные [3], полученные при анализе.

Наиболее значимые результаты проведенного исследования представлены далее.

Основная часть

В настоящее время существует несколько реализаций ПАП [2], которые предоставляют возможность создания электронного документа с использованием технологии облачной ЭЦП использующих либо один из видов аутентификации из перечня или же их комбинацию:

– базовая аутентификация (Basic Authentication) (рис. 1, а);

– OAuth2 аутентификация (OAuth2 with Authentication Code flow) (рис. 1, б);

– аутентификация с использованием PIN (credenal protected by a PIN) (рис. 2, а);

– аутентификация с использованием OTP (credenal protected by an «online» OTP (based on SMS)) (рис. 2, б);

– аутентификация с использованием PIN и OTP (credenal protected by a PIN and an «online» OTP (based on SMS)) (рис. 3).

В общем виде, любой из ПАП разделяется на блоки.

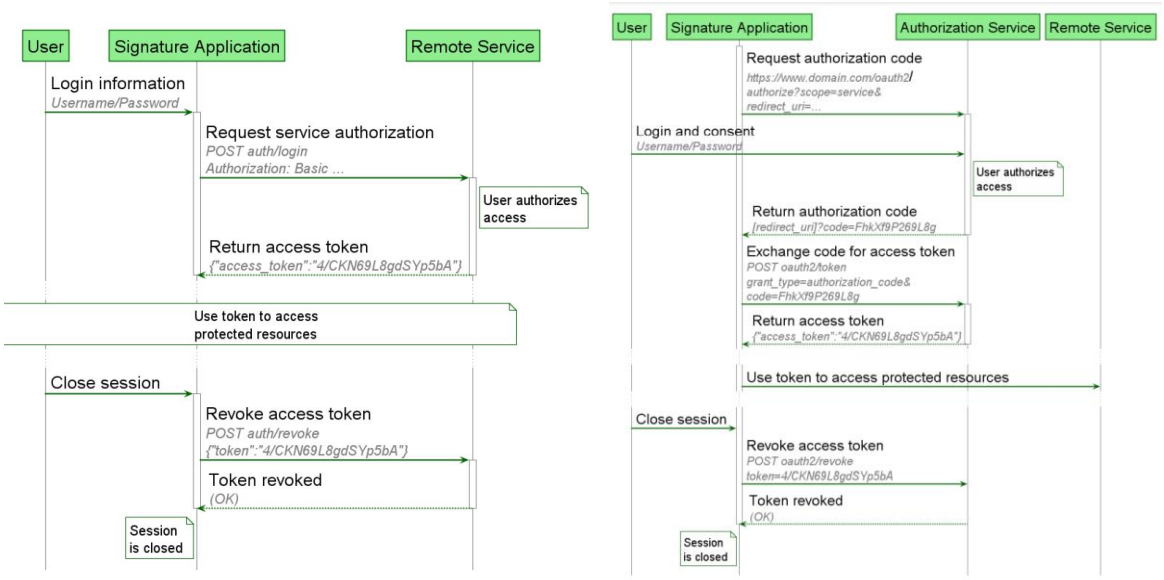
1. Блок SysAuth - пользователь проходит аутентификацию как субъект системы электронного документооборота.
2. Блок Submit: пользователь инициирует подпись документов без атрибутов.
3. Блок CredAuth1: начало аутентификации пользователя на доступ к личному ключу.
4. Блок AddSignedAttrs: добавление подписываемых атрибутов.
5. Блок Confirm: пользователь дает согласие на подпись документов.
6. Блок CredAuth2: завершение аутентификации пользователя на доступ к личному ключу.
7. Блок IssueDAP: выпуск данных активации подписи (далее – ДАП).
8. Блок Sign: подпись документов.
9. Блок AddUnsignedAttrs: добавление неподписываемых атрибутов.

Разработанный в рамках исследования ПАП опирается на протоколы, использующие PIN-код к личному ключу пользователя и OTP-пароль, а также дополнительные механизмы защиты информации [3].

Разработанный ПАП может противостоять следующим атакам.

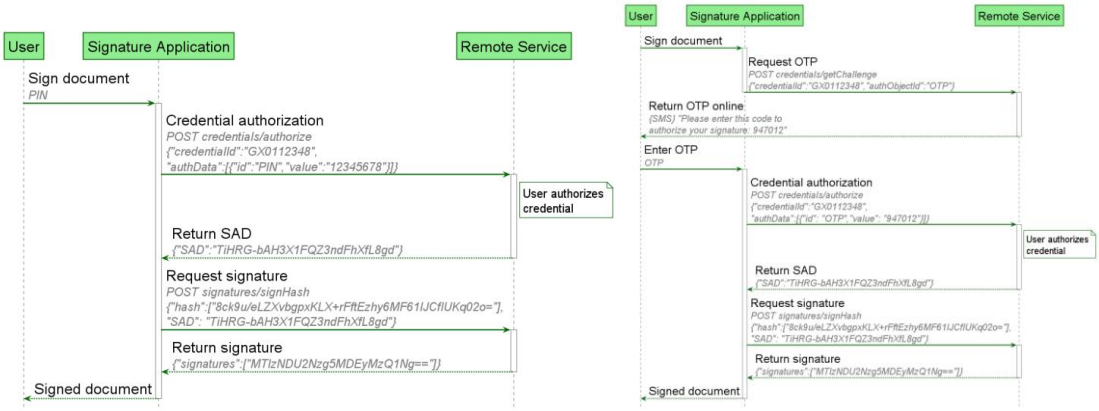
1. Перехват аутентификатора, при котором противник перехватывает аутентификаторы в момент их ввода пользователем и определяет по ним будущие аутентификаторы.
2. Угадывание аутентификатора, когда противник угадывает аутентификатор в ходе выполнения протокола аутентификации.
3. Подбором аутентификатора, при котором противник в последовательных сеансах аутентификации пытается угадать аутентификатор, проверяя различные его варианты.
4. Перехват сообщений протокола, при котором противник перехватывает сообщения протокола и обрабатывает их, надеясь получить информацию, которая позволит выдать себя за пользователя.
5. Противник посередине встраивается во взаимодействие между пользователем и системой во время выполнения протокола аутентификации;
6. Повторное использование данных аутентификации, которые уже ранее использовался законным пользователем;

Противник пытается использовать метод подмены ответов, при котором вмешивается в передачу данных между сторонами протокола и в ответ на аутентификатор одного пользователя возвращает данные другого.



a *b*

Рис. 1. Вид ПАП: *a* – Базовая аутентификация *a*; *b* – OAuth2 аутентификация
Fig. 1. Form SAP: *a* – Basic Authentication; *b* – OAuth2 with Authentication Code flow



a *b*

Рис. 2. Вид ПАП: *a* – Аутентификация с использованием PIN; *b* – Аутентификация с использованием OTP
Fig. 2. Form SAP: *a* – PIN authentication; *b* – OTP authentication

Рис. 3. ПАП, использующий аутентификацию, основанную на PIN и OTP
Fig. 3. SAP using PIN-code and OTP-based authentication

Заключение

Использование ПАП позволяет существенно повысить уровень контроля над данными, обеспечивая дополнительную аутентификацию и защиту от подмены подписываемого документа [3]. Тем не менее, даже с внедрением ПАП, остается возможность атаки со стороны злоумышленников.

Модификация ПАП направлена на минимизацию рисков при работе с технологией облачной ЭЦП. В дальнейшем исследования будут направлены на анализ уязвимости существующих систем, использующих облачную ЭЦП, чтобы обеспечить их безопасность и эффективность. Таким образом, сочетание

современных технологий и надежных протоколов аутентификации станет ключевым аспектом в поднятии уровня доверия граждан технологии облачной ЭЦП.

Список использованных источников

1. Сазонова, Д. В.Технологии использования облачной ЭЦП / Д. В. Сазонова, В. В. Козловский // Информационные технологии. Физика и математика : материалы 88-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 29 января – 16 февраля 2024 г. – Минск: БГТУ, 2024. – С. 30-35.

2. Теоретическая и прикладная криптография : материалы II Междунар. науч. конф., Минск, 19–20 окт. 2023 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2023. – С. 250-260.

3. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов // *Комплексная защита информации : материалы XXVIII научно-практической конференции*, г. Гомель, 23-25 мая 2023 г. / Белорусский государственный университет транспорта. – Гомель, 2023. – С. 257–261.

4. Josang A., Alfayyadh B. Robust WYSIWYS: A Method for Ensuring that What You See Is What You Sign // Sixth Australasian Information Security Conference (AISC 2008). т. 81. – Wollongong, NSW, Australia : ACS, 2008. – С. 53–58.

References

1. Sazonova, D. V. Technologies for using cloud EDS / D. V. Sazonova, V. V. Kozlovsky // Information technologies. Physics and Mathematics : materials of the 88th Scientific and Technical Conference of the teaching staff, researchers and aspirants (with international participation), Minsk, January 29 – February 16, 2024 – Minsk: BSTU, 2024. – pp. 30-35. (in Russian)

2. Theoretical and Applied cryptography : proceedings of the II International Scientific Conference, Minsk, October 19-20. 2023 / Belarusian State University ; editor: Yu. S. Kharin (chief editor) [and others]. – Minsk : BSU, 2023. – pp. 250-260. (in Russian)

3. Gerasimov, V. A. Information protection mechanisms in the development of cloud-based electronic digital signatures / V. A. Gerasimov // Integrated information protection : proceedings of the XXVIII scientific and practical conference, Gomel, May 23-25, 2023 / Belarusian State University of Transport. Gomel, 2023. pp. 257-261. (in Russian)

4. Josang A., Alfayad B. Reliable WYSIWYS: a method to ensure that what you see corresponds to what you sign // Sixth Australasian Conference on Information Security. (AISC, 2008). vol. 81. – Wollongong, New South Wales, Australia : ACS, 2008. – pp. 53-58.

Сведения об авторе

Герасимов В.А., магистр, сотрудник, Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», vger@niitzi.by.

Information about the author

Gerasimov V.A., Master's degree, employee, Scientific production republican unitary enterprise "Research institute for technical protection of information", vger@niitzi.by.

УДК 621.314.211 : 621.3.019.3

НОВЫЙ ПОДХОД К ОЦЕНКЕ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ТРАНСФОРМАТОРОВ ВТОРИЧНЫХ ИСТОЧНИКОВ ПИТАНИЯ

[1]Е.Д. Гришечкин, [2]А.В. Будник

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

[2] *Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается применение методов анализа данных для прогнозирования надежности трансформаторов вторичных источников питания радиоэлектронной аппаратуры. Описан подход, основанный на обработке эксплуатационных отчетов и статистическом анализе. Выявление

закономерностей отказов и использование математических моделей позволяют повысить точность прогнозирования, минимизировать риски отказов и оптимизировать техническое обслуживание. Предложенная модель учитывает реальные условия эксплуатации, что делает прогнозирование более достоверным и адаптивным.
Ключевые слова: прогнозирование надежности, эксплуатационные отчеты, статистический анализ, предиктивная аналитика, трансформаторы, вторичные источники питания.

A NEW APPROACH TO ASSESSING THE OPERATIONAL RELIABILITY OF SECONDARY POWER SUPPLY TRANSFORMERS

[1]E.D. Grieshechkin, [2]A.V. Budnik
[1] *Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus*
[2] *Educational Institution "Belarusian State Academy of Communications", Minsk, Belarus*

Abstract. The article discusses the application of data analysis methods for predicting the reliability of secondary power supply transformers of electronic equipment. An approach based on the processing of operational reports and statistical analysis is described. Identifying failure patterns and using mathematical models can improve forecasting accuracy, minimize failure risks and optimize maintenance. The proposed model takes into account real operating conditions, which makes forecasting more reliable and adaptive.
Keywords: reliability forecasting, operational reports, statistical analysis, predictive analytics, transformers, secondary power sources.

Введение

Трансформаторы играют ключевую роль в системах электропитания информационных и коммуникационных технологий, обеспечивая стабильность работы оборудования и минимизируя влияние электромагнитных помех (ЭМП). В условиях современных угроз кибербезопасности отказ силового оборудования может привести к серьезным сбоям в защите данных, особенно в критически важных системах. Надежность вторичных источников питания становится важным элементом защиты информации, предотвращая влияние нестабильного электропитания на безопасность вычислительных систем.

Широкое использование трансформаторов в электронной аппаратуре и их важность для стабильного функционирования оборудования требуют особого внимания к вопросам их надежности. Несмотря на тщательное проектирование и использование качественных материалов, любой трансформатор подвержен износу и постепенному старению из-за воздействия температурных, электрических и механических нагрузок. Прогнозирование эксплуатационной надежности позволяет не только определить ресурс трансформатора, но и оптимизировать графики его обслуживания, замен и модернизации. Анализ эксплуатационных данных играет ключевую роль в повышении точности оценки надежности трансформаторов.

Основная часть

Российский справочник «Надежность электрорадиоизделий». В отечественной практике для прогнозирования эксплуатационной надежности трансформаторов ($\lambda_Э$) используют модель, приводимую в Российском справочнике «Надежность электрорадиоизделий» (2006 год), разработанном Федеральным государственным учреждением «22-й Центральный научно-исследовательский испытательный институт Министерства обороны России». Модель имеет вид

$$\lambda_э = \lambda_б \cdot K_t \cdot K_Э \cdot K_{пр}, \quad (1)$$

где $\lambda_э$ – эксплуатационная интенсивность отказов трансформатора, соответствующая условиям его применения в составе электронной аппаратуры; $\lambda_б$ – базовая (обобщенная, усредненная) интенсивность отказов, характерная для данной группы трансформаторов в целом; K_t – коэффициент режима в зависимости от максимально допустимых температур по технической документации; $K_Э$ – коэффициент эксплуатации, учитывает другие условия эксплуатации, кроме температуры, температура как важнейший эксплуатационный фактор учитывается отдельно; $K_{пр}$ – коэффициент приемки, зависит от жесткости требований к контролю качества при изготовлении трансформаторов в условиях производства.

Отечественная методика отличается своей простотой и универсальностью. Она базируется на усредненных данных и нескольких коэффициентах, что позволяет легко применять ее в большинстве стандартных случаев. Однако из-за ограниченного числа параметров, учитываемых в расчете, она дает результаты ограниченной достоверности.

Стандарт Китая. В военном коммерческом стандарте Китая *GJB/z* 299*B* для прогнозирования эксплуатационной интенсивности отказов (λ_P) трансформаторов используют модель вида

$$\lambda_P = \lambda_b \cdot \pi_E \cdot \pi_Q \cdot \pi_K, \quad (2)$$

где λ_b – базовая (обобщенная, усредненная) интенсивность отказов, характерная для данной группы трансформаторов в целом; π_E – коэффициент, учитывающий влияние окружающей среды; π_Q – коэффициент качества изделия; π_K – коэффициент типа трансформатора (низкой мощности, импульсный, фильтрующий).

Для определения базовой интенсивности отказов λ_b в стандарте *GJB/z* 299*B* приводится формула, учитывающая влияние температуры и частоты работы трансформатора.

Справочник 217+ Модели прогнозирования надежности (MILHandbook of 217Plus Reliability Prediction Models), США, 2006 г. В этом справочнике приводится модель вида

$$\lambda_P = \pi_G (\lambda_{OB} \cdot \pi_{DCO} \cdot \pi_{TO} + \lambda_{EB} \cdot \pi_{DCN} \cdot \pi_{TE} + \lambda_{TCB} \cdot \pi_{CR} \cdot \pi_{DT}) + \lambda_{IND}, \quad (3)$$

где λ_P – прогнозируемая интенсивность отказов (в отказах на миллион календарных часов); λ_{OB} – базовая интенсивность отказов при работе; λ_{EB} – базовая интенсивность отказов, обусловленная условиями окружающей среды; λ_{TCB} – базовая интенсивность отказов, вызываемая тепловыми циклами; λ_{IND} – интенсивность отказов, обусловленная другими факторами, например такими как механическое повреждение, электрические помехи; π_G – коэффициент, учитывающий роста надежности от времени производства; π_{DCO}, π_{DCN} – коэффициенты рабочего (*DCO*) и нерабочего (*DCN*) циклов; π_{TO}, π_{TE} – температурные коэффициенты для рабочих (*TO*) и окружающих (*TE*) условий; π_{CR} – коэффициент, учитывающий частоту циклов; π_{DT} – коэффициент перепада температур.

Из рассмотренных в работе справочников и стандартов модель (3) отличается самым детализированным подходом, так как учитывает широкий спектр факторов, включая механические повреждения, электрические помехи, тепловые колебания, рабочие и нерабочие циклы. Такой подход позволяет моделировать эксплуатационную надежность трансформатора практически в любых условиях. Однако его реализация требует значительных усилий, а результаты будут сильно зависеть от точности используемых входных данных.

Предлагаемый подход к оценке эксплуатационной надежности трансформаторов. Для трансформаторов источников питания, как сложных изделий,

суммарный поток отказов которых складывается из независимых потоков отказов составных конструктивных частей, в частности магнитопровода, обмоток с учетом их числа и диаметра используемых проводов, внешних контактных выводов и др., предлагается использовать модель прогнозирования эксплуатационной интенсивности отказов $\lambda_Э$ (как показателя безотказности трансформатора в целом) в виде

$$\lambda_Э = \lambda_{Б1} \prod_{i=1}^{m_1} K_i^{(1)} + \ldots + \lambda_{Бn} \prod_{i=1}^{m_n} K_i^{(n)}, \quad (4)$$

где $\lambda_{Бj}$ – исходная (базовая, усредненная) интенсивность отказов j-й конструктивной части трансформатора, j = 1, …, n; n – количество выделенных составных конструктивных частей трансформатора, влияющих на его надежность; $K_i^{(j)}$ – поправочный коэффициент, учитывающий влияние i-го фактора для j-й конструктивной части трансформатора; i = 1, …, m; j =1, …, n; m_j – количество факторов, учитываемых для i-й части трансформатора.

Модель (4) принимает во внимание тот факт, что разные конструктивные части трансформатора могут иметь разные значения поправочных коэффициентов, учитывающих влияние одного и того же фактора, например, уровня качества изготовления частей трансформатора в условиях производства.

С начальным вариантом модели, основанной на использовании выражения (4), можно ознакомиться в сборнике научных статей XIV Международной научно-технической конференции «Средства медицинской электроники и новые медицинские технологии» (Минск, 5–6 декабря 2024 г.). Модель была включена в методику выполнения инженерных расчетов надежности комплектующих изделий и электронных устройств для *IT*-системы, предназначенной для автоматизированного расчета и обеспечения надежности электронных устройств, известной под названием система АРИОН [1]. Дальнейшие исследования авторов работы направлены на усовершенствование модели с учетом многообразия материалов, используемых в качестве магнитопровода трансформаторов электропитания, конструктивных их особенностей и физических свойств.

Заключение

Рассмотрены модели прогнозирования эксплуатационной надежности трансформаторов, используемых в радиоэлектронной аппаратуре. Анализ сделан по нормативно-техническим документам ведущих стран мира. Развитие методов анализа эксплуатационных характеристик позволяет повысить достоверность прогнозирования надежности трансформаторов. Учет множества факторов, влияющих на их работу, и систематизация данных об отказах помогают выявлять скрытые закономерности, влияющие на долговечность оборудования. Разработанная модель, основанная на анализе накопленных эксплуатационных данных, позволяет не только учитывать внешние и внутренние факторы, но и предоставлять более точные прогнозы отказов. Такой подход способствует повышению безопасности и эффективности электронных систем, а также оптимизации профилактического обслуживания, что в итоге снижает затраты на эксплуатацию и ремонт.

Список использованных источников

1. Боровиков С.М., Шнейдеров Е.Н., Матюшков В.Е., И.Н Цырельчук. (2011) Разработка методики прогнозирования надежности электронных устройств для системы АРИОН. *Доклады БГУИР.* 4 (58): 93–100.

References

1. Borovikov S.M., Shneiderov E.N., Matyushkov V.E., I.N. Tsyrelchuk. (2011) Development of a methodology for predicting the reliability of electronic devices for the ARION system. *BSUIR reports.* 4 (58): 93-100 (in Russian).

Сведения об авторах

Гришечкин Е.Д., магистрант кафедры проектирования информационно-компьютерных систем Белорусского государственного университета информатики и радиоэлектроники, egorgr2977@gmail.com.
Будник А.В., канд. техн. наук, доц., декан факультета инжиниринга и технологий Белорусской государственной академии связи, A.Budnik@bsac.by.

Information about the authors

Grieshechkin E., Master's student of the Department of Information and Computer Systems Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", egorgr2977@gmail.com.
Budnik A., Cand. of Sci. (Tech.), Dean of the Faculty of Engineering and Technology of the the Belarusian State Academy of Communications, A.Budnik@bsac.by.

УДК 004.45

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОБЛАСТИ ВИРТУАЛИЗАЦИИ

В.В. Гузнов
Государственное предприятие «НИИ ТЗИ»
(г. Минск, Республика Беларусь)

Аннотация. В современном мире виртуализация становится неотъемлемым элементом ИТ-инфраструктуры, обеспечивая эффективное использование вычислительных ресурсов, а также позволяя оптимизировать расходы на оборудование и улучшить управление вычислительными мощностями. Она способствует минимизации рисков, связанных с уязвимостями физической инфраструктуры, так как обеспечивает изоляцию виртуальных машин, что позволяет предотвратить распространение кибератак и сбоев между ними. Виртуализация также значительно повышает уровень отказоустойчивости систем, предоставляя возможность быстро восстанавливать данные из резервных копий и переносить рабочие нагрузки между серверами. В данной статье рассмотрены ключевые возможности, преимущества и недостатки использования виртуализации в корпоративных сетях. Также проведен сравнительный анализ популярных решений в области виртуализации. Оцениваются факторы, влияющие на выбор той или иной платформы для конкретных целей – от личных проектов до корпоративных решений.
Ключевые слова: виртуализация; платформа виртуализации; риск; отказоустойчивость; корпоративная сеть; уязвимость; сравнительный анализ; оптимизация; виртуальная машина; ИТ-инфраструктура.

ANALYSIS OF SOFTWARE IN THE FIELD OF VIRTUALIZATION

V.V. Guznov
State Enterprise "NII TZI" (Minsk, Republic of Belarus)

Abstract. In today`s world, virtualization has become an integral part of IT infrastructure, ensuring efficient use of computing resources, as well as optimizing hardware costs and improving the management of computing power. It helps minimize risks associated with vulnerabilities in physical infrastructure by providing isolation of virtual machines, which prevents the spread of attacks and failures between them. Virtualization also significantly increases the fault tolerance of systems, allowing for quick data recovery from backups and the ability to move workloads between servers. This article examines the key features, advantages, and disadvantages of using virtualization in corporate networks. It also provides a comparative analysis of popular virtualization solutions. Factors influencing the choice of a platform for specific purposes – from personal projects to corporate solutions.
Keywords: virtualization; virtualization platform; risk; fault tolerance; corporate network; vulnerability; analysis; optimization; virtual machine; IT infrastructure.

Введение

Виртуализация – технология, которая существенно изменила подход к управлению вычислительными ресурсами в современных информационных системах. Она позволяет эффективно использовать аппаратные ресурсы, упрощает администрирование и повышает гибкость инфраструктуры [1]. С каждым годом виртуализация становится неотъемлемой частью как в личных, так и в корпоративных проектах, благодаря своей возможности сократить затраты и повысить эффективность работы систем.

Целью данной работы является сравнительный анализ наиболее популярных систем виртуализации, в ходе которого выделение их ключевых особенностей и сферы использования. Статья будет полезна как для специалистов в области информационных технологий, так и для пользователей, желающих разобраться в особенностях виртуализации и выбрать оптимальное решение.

Основная часть

Основной принцип виртуализации заключается в абстракции, то есть в создании программного слоя, позволяющего изолировать виртуальные экземпляры (виртуальные машины) от физического оборудования. Виртуализация работает через гипервизор – специализированное программное обеспечение, управляющее виртуальными машинами [2]. По методу установки выделяют 2 типа гипервизоров:

1. Гипервизоры bare-metal (рис. 1) работают непосредственно на аппаратной части вычислительной машины.
2. Гипервизоры hosted (рис. 2) устанавливаются на машины с предварительно сконфигурированными операционными системами.

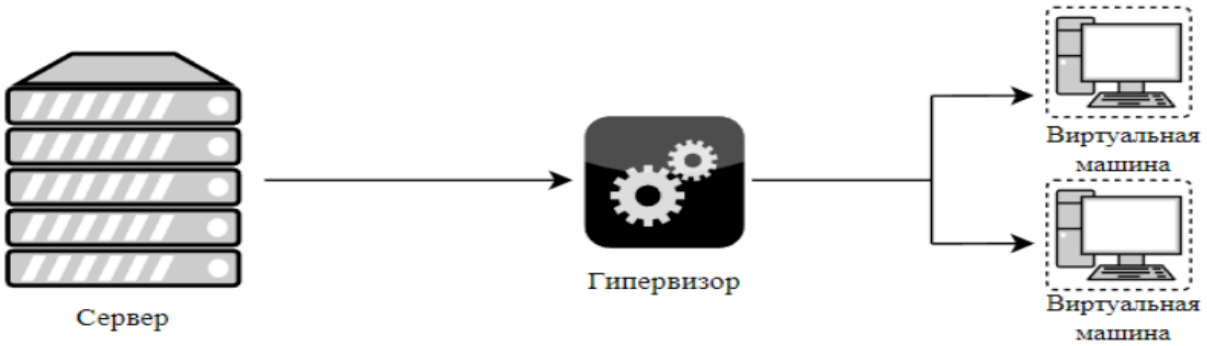


Рис. 1. Схема организации работы гипервизоров bare-metal
Fig. 1. Scheme of the operation bare-metal hypervisors

Рис. 2. Схема организации работы гипервизоров hosted
Fig. 2. Scheme of the operation of hosted hypervisors

После рассмотрения основ виртуализации и принципа работы гипервизоров различного типа, следует обратиться к практическим аспектам использования данной технологии. В последние годы на рынке платформы виртуализации представлены различными решениями, предлагаемые как международными, так и отечественными разработчиками. Эти системы могут существенно различаться по функциональным возможностям, области применения и поддерживаемым платформам. В таблице 1 приведен сравнительный анализ решений для корпоративных сетей от таких компаний, как VMware и Microsoft, а также отечественных разработчиков – РЕД СОФТ и ORIONsoft.

Таблица 1. Сравнительный анализ решений в области виртуализации
Table 1. Analysis of virtualization solutions

Компания / Критерий	VMware	Microsoft	РЕД СОФТ	ORIONsoft
Наименование продукта	ESXI	Hyper-V	РЕД Виртуализация	zVirt
Версия	7	Server 2019	7.3	4.2
Встроенные средства резервного копирования	–	–	+	+
Техническая поддержка от производителя	–	–	+	+
Максимальное количество ВМ на хосте	1024	1024	400	600
Максимальное количество CPU на хост	896	512	768	768
Максимальное количество RAM на хост	24 ТБ	24 ТБ	12 ТБ	12 ТБ
Максимальное количество CPU на ВМ	256	64	240	210
Максимальное количество RAM на ВМ	24 ТБ	12 ТБ	4 ТБ	16 ТБ
Проброс PCI устройств в ВМ	+	+	+	+
Живая миграция ВМ	+	+	+	+
Интеграция с LDAP	+	+	+	+
Наличие сертификата соответствия ТР 2013/027/BY	+	+	–	+

Заключение

Сравнительный анализ показал, что зарубежные решения, такие как VMware и Microsoft, обладают более высокой масштабируемостью. Однако, несмотря на их технологическое превосходство, эти платформы не предоставляют официальную техническую поддержку от производителя, что может затруднить оперативное решение проблем. Отечественные решения предлагают встроенные средства резервного копирования и восстановления, а также техническую поддержку. Также одним из важных факторов при выборе платформ виртуализации является наличие сертификата соответствия ТР 2013/027/BY, который позволяет использовать решение в информационных системах, обрабатывающих данные ограниченного распространения [3].

Таким образом, проведенный сравнительный анализ показал, что выбор платформы виртуализации должен основываться на балансе масштабируемости, уровня технической поддержки и соответствия требованиям информационной безопасности. Компании с приоритетом на производительность и гибкость могут ориентироваться на зарубежные решения, тогда как организации, работающие с конфиденциальными данными, могут выбрать отечественные продукты, обеспечивающие необходимый уровень поддержки и сертификации.

Список использованных источников

1. Питкевич П.И., Одинец Д.Н. (2021) Методика виртуализации вычислительных ресурсов масштаба предприятия. *Цифровая трансформация* 3 (16), 40–46.

2. Гаврилов Л.П. (2019) *Инновационные технологии в коммерции и бизнесе: учебник для бакалавров*. Москва, издательство «Юрайт».

3. Мартинкевич Д.Л., Насонова Н.В. (2024) Создание системы защиты информации коммерческого предприятия. *Технические средства защиты информации: тезисы докладов XXII Белорусско-российской научно-технической конференции*, 55–56.

References

1. Pitkevich P.I., Adzinets D.N. (2021) Enterprise-scale computing resource virtualization methodology. *Digital transformation* 3 (16), 40–46 (in Russian).

2. Gavrilov L.P. (2019) *Innovative technologies in commerce and business: textbook for bachelors*. Moscow, publishing house Yurati.

3. Martinkevich D.L., Nasonova N.V. (2024) Creating an information security system for a commercial enterprise. *Technical means of information protection: proceedings of the XXII Belarusian-Russian scientific and technical conference*, 55–56.

Сведения об авторе

Гузнов В.В., инженер испытательной лаборатории по требованиям безопасности информации, Государственное предприятие «НИИ ТЗИ», guznov1999@mail.ru.

Information about the author

Guznov V.V., Engineer of the Testing Laboratory for Information Security Requirements, State Enterprise "NII TZI", guznov1999@mail.ru.

УДК 004.056.53

МОНИТОРИНГ НАЛИЧИЯ ЭЛЕКТРОМАГНИТНЫХ СИГНАЛОВ В БЛИЖНЕЙ ЗОНЕ

Г.В. Давыдов, В.А. Попов, А.В. Потапович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Приведены исследования по выявлению каналов утечки информации за счет двойного использования отдельных элементов и устройств, в средствах вычислительной техники. С одной стороны, эти элементы и устройства выполняют основную функцию в изделии и дополнительно могут использоваться для выполнения функций, не оговоренных их основным назначением. Рассмотрены два метода мониторинга каналов утечки информации. Предложенный алгоритм и методика обнаружения синхронизированных с провоцирующим воздействием аномалий в тепловых полях проверяемого изделия является необходимым условием выявления аппаратных средств недекларированных возможностей образования канала утечки информации.
Ключевые слова: риск безопасности, защищенность информации, электромагнитный сигнал, радиоканал утечки информации.

MONITORING THE PRESENCE OF ELECTROMAGNETIC SIGNALS IN THE NEAR ZONE

H.V. Davydau, V.A. Papou, A.V. Patapovich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article presents studies on identifying information leakage channels due to dual use of individual elements and devices in computing equipment. On the one hand, these elements and devices perform the main function in the product and can additionally be used to perform functions not specified by their main purpose. Two methods of monitoring information leakage channels are considered. The proposed algorithm and method for detecting anomalies in thermal fields of the product being tested that are synchronized with the provoking effect are a necessary condition for identifying hardware with undeclared capabilities for forming an information leakage channel.
Keywords: security risk, information security, electromagnetic signal, radio channel of information leakage.

Защита информации, циркулирующей в средствах вычислительной техники, включает как организационные мероприятия, так и технические мероприятия защиты линий связи и питания от утечки информации. В месте, с тем существует опасность утечки информации по радиоканалу, организуемому на короткий промежуток времени от средств вычислительной техники. Такие каналы утечки информации могут образовываться как с использованием радиомодулей, интегрированных в центральный процессор, так и с использованием дополнительных функциональных возможностей элементов вычислительной техники (недекларированных возможностей) [1]. В работе в качестве примера образования канала утечки информации рассматривается использование радиомодуля RFID, внедренного в серверные центральные процессоры Xeon W-2255 компании Intel. Обнаружение встроенных в процессоры модулей или использование дополнительных функциональных возможностей элементов устройств вычислительной техники для образования недекларированных радиоканалов передачи информации рассматривается в работе. Обнаружение осуществляется по изменению теплового поля материнской платы вычислительного устройства при провоцирующем акустическом и электромагнитном воздействиях.

Структурная схема комплекса проверки вычислительной техники на наличие аппаратных средств недекларированных возможностей (НДВ) представлена на рис. 1.

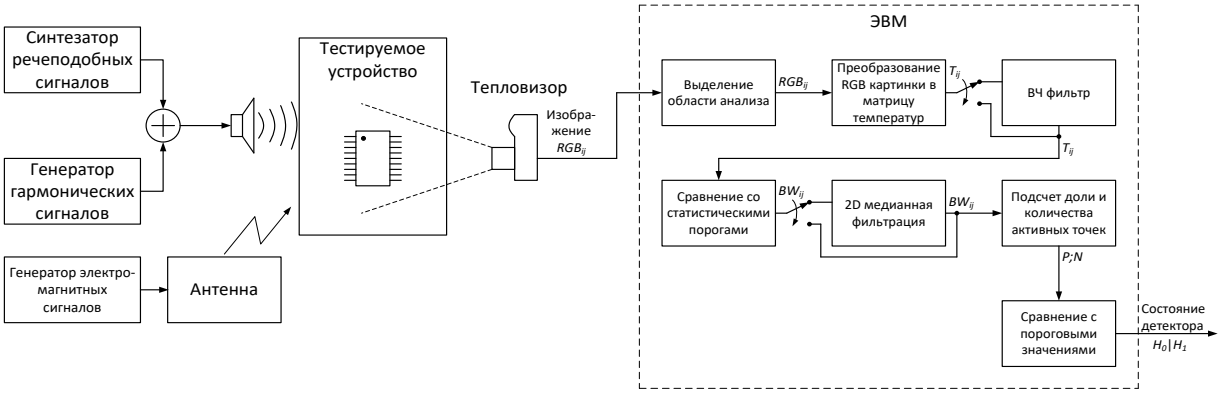


Рис. 1. Структурная схема комплекса проверки вычислительной техники на наличие аппаратных средств НДВ
Fig. 1. Structural diagram of the complex for checking computing equipment for the presence of NDV hardware

Для корректного проведения проверки вычислительной техники необходимы следующие ограничения и технические решения. Помещение для проведения проверки должно состоять из двух комнат. В одной комнате размещается испытуемый объект, тепловизор, акустические преобразователи для создания провоцирующих акустических полей и антенны, предназначенные для создания провоцирующих электромагнитных полей. В другой комнате, совмещенной с первой, располагаются операторы, управляющий компьютер, генератор провоцирующих акустических воздействий и генератор провоцирующих электромагнитных воздействий. Экспериментальные исследования показали, что на результаты проверки вычислительной техники на наличие аппаратных средств НДВ могут оказывать вибрации испытуемого объекта или тепловизора. Для исключения влияния этого фактора на результаты проверки была изменена конструкция крепления тепловизора к штативу, что позволило снизить вибрации тепловизора, вызываемые акустическим провоцирующим воздействием.

Для проведения проверки вычислительной техники на наличие аппаратных средств НДВ необходимо экранировать объект проверки и тепловизор от тепловых фоновых шумов. Тепловые фоновые шумы включают тепловое поле оператора, световое излучение, поступающее в помещение через окна, конвекционные тепловые потоки. Влияние теплового поля оператора на результаты проверки необходимо исключить путем организации его рабочего места в рядом расположенной комнате. На результаты проверки могут оказывать негативное влияние и конвекционные потоки и сквозняки. Поэтому при проведении проверки необходимо плотно закрывать двери и окна в комнате, где расположен проверяемый объект.

Для исключения влияния многократно переотраженного светового и инфракрасного излучения, попадающих в комнату через окна, окна в комнате, где проводятся проверки, должны быть зашторены.

Однако, изменения температуры в помещении из-за изменений погодных условий (температуры и освещения) могут приводить к изменениям температуры проверяемых объектов. Эксперименты показали, что температура проверяемых объектов в течении часа может изменяться на 0,3 °С. Кратковременные изменения температуры (в течении 10 минут) проверяемого объекта не превышают 0,1 °С. Чувствительность тепловизора составляет 0,04 ^{0}С, что является достаточным для проверки вычислительной техники на наличие аппаратных средств НДВ. Тепловые шумы из-за влияния рассмотренных выше факторов не превышают 0,1 °С.

В состав комплекса проверки входили следующие функциональные устройства. Генератор провоцирующих электромагнитных сигналов Agilent N5172B предназначен для создания электромагнитных провоцирующих полей в области расположения проверяемой вычислительной техники на наличие аппаратных средств НДВ. Параметры генератора провоцирующих электромагнитных сигналов следующие:

– диапазон сканирования по частоте от 10 до 3000 МГц с точность установки частоты не более 0,01%;

– мощность сигнала на выходе генератора не менее минус 10 dBm с точность не менее ± 1 dBm в диапазоне частот от 10 до 3000 МГц.

Рамочная антенна 6512 ETS LINDGREN предназначена для создания провоцирующего электромагнитного поля в диапазоне частот от 10 до 30 МГц, а биконическая антенна BicoLOG 20300 AARONIA для создания провоцирующего электромагнитного поля в диапазоне частот от 30 до 3000 МГц. Антенны подключены к генератору Agilent N5172B через согласующее устройство. Согласующее устройство разделяет диапазон частот от генератора на два диапазона с полосами частот от 10 до 30 МГц для антенны 6512 ETS LINDGREN и от 30 до 3000 МГц для антенны BicoLOG 20300 AARONIA

Генератор провоцирующих акустических сигналов предназначен для создания акустических полей в области расположения проверяемой вычислительной техники на наличие аппаратных средств НДВ. Генератор провоцирующих акустических сигналов выполнен программно на управляющем компьютере и позволяет формировать речеподобные или гармонические сигналы. Воспроизведение акустических сигналов выполняется с помощью акустических преобразователей на базе акустической системы SVEN SPS-611S. Интегральный уровень звукового давления провоцирующих акустических воздействий должен быть не менее 70 дБ в диапазоне частот от 100 до 8000 Гц.

Тепловизор Flir T640, входящий в состав комплекса, предназначен для съема распределения теплового поля по проверяемой вычислительной технике или ее отдельным функциональным узлам и передачи данных на управляющий компьютер. Разрешающая способность тепловизора должна быть не хуже 0,04 °С в диапазоне от 8 до 14 мкм. Более высокая разрешающая способность тепловизора не нужна, так как конвекционные потоки и колебания температуры проверяемой вычислительной техники из-за различного вида тепловых и световых помех составляют ± 0,1 °С. Меньшего значения колебаний температуры проверяемого объекта вычислительной техники достичь не удалось при использовании доступных методов защиты от тепловых и световых помех.

Управление комплексом осуществлялось переносным компьютером. Генератор провоцирующих акустических сигналов (речеподобных и гармонических сигналов) выполнен программно и установлен на персональный компьютер для управления комплексом. Для формирования речеподобных сигналов использовалась база аллофонов диктора. База аллофонов диктора создавалась по записям речи диктора. Аллофон был представлен в виде отдельного wav файла с присвоением файлу имени аллофона. Синтез речеподобных сигналов выполнялся с учетом вероятностей длины предложений и длины слов в русской речи, а также вероятностей появления определенных аллофонов в русской речи. Распределение вероятностей длины предложений (числа слов в предложении) для русской речи является не определяющим параметром при синтезе речеподобных сигналов. Лучше использовать при синтезе речеподобных сигналов длину синтагмы, на которые делится предложение (фраза)

и количество фраз в фоноабзаце. Среднее число слов в предложении для русской речи составляло 10,38. Эти характеристики для каждого диктора могут быть свои.

Генератором провоцирующих электромагнитных сигналов N5172B формировались сигналы с различными видами модуляции и протоколами связи.

Развертка гармонических сигналов в диапазоне частот от 10 до 3000 МГц выполнялась по логарифмическому закону. Это обусловлено тем, что относительная скорость перестройки должна оставаться постоянной. Время перестройки частоты генератора должно быть выбрано таким образом, чтобы прохождение частотной полосы приемника, настроенного на какую-то частоту, составляло не менее 0,5 с. Если на несущей частоте в 10 МГц ширина полосы принимаемых сигналов составляет 5 кГц, то развертка частоты от 10 до 10,005 МГц должна быть выполнена за время не менее 0,5 с. Исходя из этого время развертки гармонических сигналов в частотном диапазоне от 10 до 3000 МГц составит 96 мин.

Все виды провоцирующих электромагнитных сигналов были записаны в память генератора и управляющего компьютера и их воспроизведение выполнялось последовательно в автоматическом режиме.

Обнаружение радиоприемных устройств основано на приеме входным каскадом радиоприемного устройства провоцирующего гармонического сигнала на частоте работы радиоприемного устройства и усилении его до уровня необходимого для дальнейшей обработки. При усилении радиоприемным устройством провоцирующего гармонического сигнала температура его повышается, что будет зафиксировано с помощью тепловизора и передано на управляющий компьютер.

Обнаружение радиопередающих устройств основано на повышении температуры выходного каскада радиопередатчика при работе на передачу и фиксирование повышения температуры радиопередающего устройства с помощью тепловизора и управляющего компьютера. Встроенные передатчики НДВ могут работать на передачу лишь короткое время в течение суток или другого отрезка времени, накапливая информацию для передачи. Поэтому целесообразно проверку не прерывать при смене провоцирующих воздействий. При этом проверка при всех видах провоцирующих воздействий займет время не более 14 ч.

Обнаружение устройства съема акустической информации выполнялось путем контроля теплового режима аудиокодека при провоцирующих акустических воздействиях. Одним из вариантов построения НДВ для съема акустической информации может быть замена керамических конденсаторов, включенных на микрофонных или линейных входах аудиокодека на такие же керамические конденсаторы с такой же емкостью, но с высокими пьезоэлектрическими свойствами (пьезоэлектрический микрофон). При отсутствии микрофонного штекера в разъеме один конденсатор оказывается закороченным на "землю", а с другого может сниматься аудио информации и далее обрабатываться кодеком. В случае наличия в микрофонном разъеме штекера сигналы от микрофонов будут поступать в фазе на дифференциальный вход и разностный сигнал от керамических микрофонов будет равен нулю и не вызовет никаких подозрений и внешний микрофон буден выполнять свои функции. Если подключен не стереофонический микрофон, то сигнал от внешнего микрофона и от микрофона НДВ будут складываться и будет впечатление что это один сигнал акустической обстановки в помещении. Следует отметить, что некоторая разность фаз сигналов от двух микрофонов будет иметь место, но на слух это определить чрезвычайно сложно, так как сигнал от микрофона НДВ может быть по амплитуде значительно меньше, чем сигнал от внешнего микрофона.

Такие методы обнаружения возможных радиоканалов утечки информации являются весьма трудоемкими.

Более предпочтительным методом может быть мониторинг наличия электромагнитных сигналов (радиосигналов) в ближней зоне во время радиообмена с устройством приема информации. Так как время радиообмена его продолжительность, а также частота и протокол радиообмен неизвестны, то мониторинг электромагнитных сигналов в ближней зоне необходимо вести параллельно по каналам с шириной каждого канала в одну октаву. При наличии 10 каналов перекрывается диапазон частот от 7 до 7000 МГц. Такое разделение по каналом позволит обнаруживать как широкополосные сигналы, так и кратковременные с длительностями не менее 35 мс. Весь частотный диапазон разбит на каналы с октавными полосами частот. Среднегеометрические частоты полос равны: 10, 20, 40, 80, 160, 320, 1250, 2500, 5000 МГц. Для приема электромагнитных сигналов в ближней зоне используются разнесенные штыревые антенны. Непосредственно штыревые антенны устанавливаются на экранированные малошумящие усилители.

На входе малошумящих усилителей включены октавные полосовые фильтры 7-го порядка. Малошумящие усилители являются одновременно и октавными полосовыми фильтрами с затуханием в полосе задерживания (на двойной частоте от граничной) 54 дБ. Неравномерность частотной характеристики в полосе пропускания составила не более 7 дБ. В устройстве использовались логарифмические усилители с детекторами на выходе. Далее сигналы поступали на схемы сравнения и обработки и потом на индикаторную панель и в блок памяти.

На индикаторной панели устройства мониторинга отображается в цифровом виде величина градиента электромагнитного поля для каждого канала. При превышении градиента электромагнитного поля порогового значения в одном из каналов информация о таком событии записывается в протокол с указанием диапазона частот, величин градиента электромагнитного поля по всем каналам, времени произошедшего события.

Проведенные исследования показали, что для обеспечения защиты информации в вычислительной технике кроме ряда мероприятий по проверке ее на наличие недекларированных возможностей перед вводом в эксплуатацию, необходимо вести мониторинг наличия электромагнитных сигналов в ближней зоне от вычислительной техники во время ее эксплуатации, с целью выявления каналов утечки информации, которые не были обнаружены.

Список использованных источников

1. Хореев А.А., Чумаков А.А. (2025) Метод защиты средств вычислительной техники от НСД по шине I2S/SMBus с использованием радиомодулей RFID, интегрированных в центральный процессор. *Информационно-методический журнал INSIDE Защита информации*. (1), 6-19.

References

1. Khoryev A.A., Chumakov A.A. (2025) Method of protecting computing equipment from unauthorized access via the I2S/SMBus bus using RFID radio modules integrated into the central processor. *Information and methodological journal INSIDE Information Security*. (1), 6-19 (in Russian).

Сведения об авторах

Давыдов Г.В., к.т.н., в.н.с., НИЛ 5.3, учреждение образования « «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Попов В.А., с.н.с., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Потапович А.В., с.н.с., зав. НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Information about the authors

Davydau H.V., PhD, researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Papou V.A., researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Patapovich A.V., researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.

УДК 534.843.5

ОЦЕНКА РАЗБОРЧИВОСТИ РЕЧИ

Г.В. Давыдов, В.А. Попов, А.В. Потапович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Эта статья посвящена оценки разборчивости речи при ее защите от утечки по акустическим каналам путем ее маскирования комбинированными акустическими сигналами, включающими «белый» шум и речеподобные сигналы. Сложности в решении задач защиты речевой информации, как и задач защиты информации в целом, обусловлены неопределенностями, связанными с трудностями математической формулировкой задач защиты с одной стороны и большим множеством факторов, влияющих на показатели защищенности речевой информации с другой стороны. Для правильной оценки защищенности речевой информации по показателям ее разборчивости необходимо принять ряд допущений и ограничений, которые могут быть приняты на базе опыта практической реализации защиты речевой информации известными техническими средствами и комплексом организационных мероприятий.
Ключевые слова: риск безопасности, речевая информация, конфиденциальность, разборчивость речи, защищенность информации.

SPEECH INTELLIGIBILITY ASSESSMENT

H.V. Davydau, V.A. Papou, A.V. Patapovich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article is devoted to the evaluation of speech intelligibility when protecting it from leakage through acoustic channels by masking it with combined acoustic signals, including "white" noise and speech-like signals. The difficulties in solving speech information protection problems, as well as information protection problems in general, are due to uncertainties associated with the difficulties of mathematical formulation of protection problems, on the one hand, and a large number of factors affecting the indicators of speech information security, on the other hand. To correctly evaluate the security of speech information based on its intelligibility indicators, it is necessary to accept a number of assumptions and limitations that can be adopted based on the experience of practical implementation of speech information security using known technical means and a set of organizational measures.
Keywords: security risk, speech information, confidentiality, speech intelligibility, information security.

Сложности в решении задач защиты речевой информации, как и задач защиты информации в целом, обусловлены неопределенностями, связанными с трудностями математической формулировкой задач защиты с одной стороны и большим множеством факторов, влияющих на показатели защищенности речевой информации с другой стороны. Предлагается методику оценки разборчивости речи для оценки

защищенности речевой информации при ее использовании в системах защиты речевой информации вести по предельным состояниям. Для правильной оценки защищенности речевой информации по показателям ее разборчивости необходимо принять ряд допущений и ограничений, которые могут быть приняты на базе опыта практической реализации защиты речевой информации известными техническими средствами и комплексом организационных мероприятий.

Целью настоящей работы является разработка методики оценки разборчивости речи при маскировании ее комбинированными сигналами с учетом процедуры отбора дикторов и аудиторов с повышенной слуховой чувствительностью, что позволит с высокой степенью надежности определять разборчивость речи по индексу артикуляции и оценивать защищенность речевой информации [1].

Исторически разработки методик оценки разборчивости речи в условиях шумов были вызваны необходимостью контроля за обеспечением условий хорошей разборчивости при передаче информации по линиям связи и в первую очередь для использования в авиации. Развитие методик шло двумя направлениями. Первый подход был основан на формантной структуре речевого сигнала, т. е. концентрации энергии речевого сигнала для определенных формант в ряде областей частотного диапазона речи.

Второй подход также в некоторой степени является формантным методом оценки разборчивости речи с использованием индекса артикуляции и разрабатывался для английского языка.

Артикуляционный метод оценки разборчивости речи по индексу артикуляции разрабатывался в лаборатории Белла для обеспечения качества связи в авиационной технике и ориентирован был на английский язык. Как формантный, так и артикуляционный методы оценки разборчивости речи разрабатывались для областей разборчивости речи выше 50 % и лишь впоследствии с существенными доработками, они нашли применение для областей разборчивости речи в несколько процентов при решении задач защиты речевой информации.

Вместе с тем, следует отметить, что все методики оценки разборчивости речи в своей основе содержат экспериментально полученные зависимости разборчивости речи от индекса артикуляции или от другого какого-либо параметра. И этот другой параметр или индекс артикуляции, так или иначе, связан с отношением сигнал-шум в отдельных полосах частот (октавных, 1/3 октавных или 20 полосах равной разборчивости) или во всем диапазоне частот речевого сигнала. В публикациях обычно приводятся эти зависимости для интегрального уровня звукового давления, т. е. для всего диапазона частот. Известные методики оценки разборчивости речи маскированной шумами предполагают, что если в одной или нескольких октавных полосах отношение сигнал / шум больше чем среднее по всему диапазону частот, то в других полосах оно должно быть на столько же меньше, чем среднее по всему диапазону частот, т.е. применим принцип аддитивности.

Методики расчета оценки разборчивости речи при ее маскировании комбинированными сигналами отсутствовали. По структурному составу комбинированные маскирующие сигналы, предназначенные для защиты речевой информации от утечки по техническим каналам, обычно содержат шумовую компоненту в виде «белого» шума и речеподобные сигналы, сформированные по базе структурных единиц речи с учетом распределения вероятностей их появления в данном языке [1].

Экспериментальные исследования разборчивости речи проводить для комбинированных маскирующих сигналов и необходимых мероприятиях

по подготовке текстового материала, а также отбору и обучению дикторов и аудиторов. Методику оценки разборчивости речи для систем защиты информации следует выполнять по предельным состояниям.

Для экспериментальных исследований были сформированы комбинированные маскирующие сигналы, и они были наложены на фонограммы информационных речевых сигналов в виде связного текста длительностью около 2 – 3 минут и объемом 198–202 слов. Фонограммы озвучивались отобранными и подготовленными дикторами. При этом соотношения сигнал - комбинированный маскирующий шум были –14, –12, –10, –9 дБ.

Для оценки защищенности речевой информации комбинированными маскирующими сигналами были проведены испытания, для чего было отобрано 5 аудиторов в возрасте от 20 до 30 лет и с дифференциальную чувствительность слуха к изменению частоты звука не более 5 Гц на частоте 1000 Гц и высокой дифференциальной слуховой чувствительностью т. е. способностью воспринимать изменения интенсивности звука от 0,5 до 0,9 дБ по Люшеру. При этом измерения проводятся при средней интенсивности звука на 40 дБ выше порога слышимости и для каждой из частот 250, 500, 1000, 2000, 4000 Гц.

Результаты экспериментальных исследований словесной разборчивости подготовленными аудиторами путем многократного прослушивания фонограмм различными аудиторами представлены на рисунке 1. При этом речь маскировалась комбинированными сигналами и «белым» шумом.

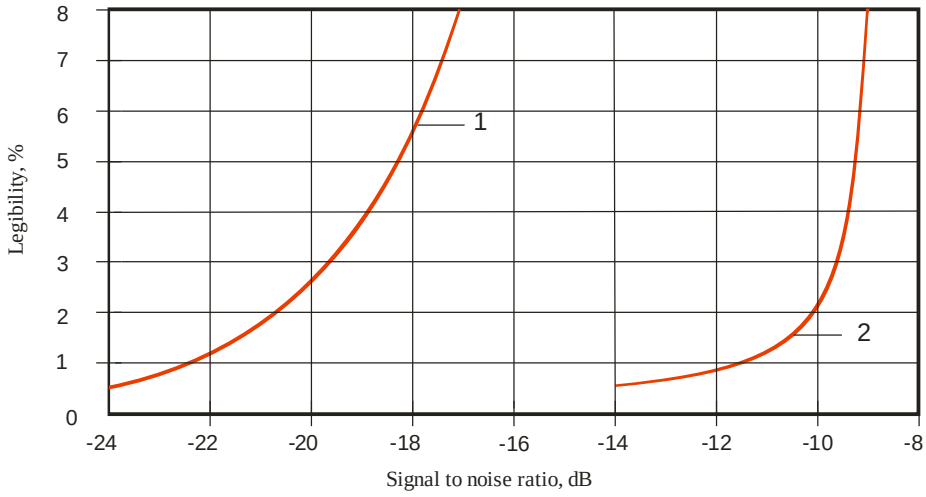


Рис. 1. Зависимость словесной разборчивости речи от отношения сигнал-шум для всего диапазона частот: Интегральное отношение сигнал-шум в относительных единицах (не в дБ) и справедливо для диапазона SN от 0 до 0,15 (для зависимости 1): 1 – для маскирующего сигнала в виде «белого» шума; 2 – для комбинированных маскирующих сигналов

Fig. 1. Dependence of speech intelligibility on the signal-to-noise ratio for the entire frequency range: Integral signal-to-noise ratio in relative units (not in dB) and is valid for the SN range from 0 to 0.15: 1 – for a masking signal in the form of "white" noise; 2 – for combined masking signals

Для комбинированных маскирующих сигналов словесная разборчивость речи может быть определена из выражения:

$$R = e^{-8{,}9+17{,}4 \cdot SN}, \quad (1)$$

где R – словесная разборчивость в относительных единицах (не в процентах); SN – интегральное отношение сигнал-шум в относительных единицах (не в дБ) и справедливо для диапазона SN от 0 до 0,35 (для зависимости 2).

Используемый параметр *SN* характеризует интегральное отношение сигнал-шум в относительных единицах, а не в дБ. Индекс артикуляции *SPI* – это логарифм среднегеометрического отношений сигнал-шум и в представленной методике не используется, хотя по своим значениям он близок к интегральному отношению сигнал-шум.

Для автоматизации вычислений словесной разборчивости речи от интегрального отношения сигнал-шум для маскирующего сигнала в виде «белого» шума была выполнена аппроксимация зависимости 1 (рис. 1.) выражением:

$$R = 6,9 \cdot SN^2 - 0,2 \cdot SN, \quad (2)$$

где R – словесная разборчивость в относительных единицах (не в процентах); SN – интегральное отношение сигнал-шум.

По результатам экспериментальных исследований получены выражения для вычисления словесной разборчивости речи для комбинированных маскирующих сигналов и для сигналов в виде «белого» шума.

Список использованных источников

1. Davydau H.V., Papou V.A., Patapovich A.V., Seitkulov Y.N., Li Ye, Fan Yanhong, et al. (2015) Method for protecting speech information. *Doklady BSUIR*, 8(94), 107–110.

References

1. Davydau H.V., Papou V.A., Patapovich A.V., Seitkulov Y.N., Li Ye, Fan Yanhong, et al. (2015) Method for protecting speech information. *Doklady BSUIR*, 8(94), 107–110.

Сведения об авторах

Давыдов Г.В., к.т.н., в.н.с., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Попов В.А., с.н.с., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Потапович А.В., с.н.с., зав. НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Information about the authors

Davydau H.V., PhD, researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Papou V.A., researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Patapovich A.V., researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.

УДК 004.934.2

МЕТОДИКА ВЫЯВЛЕНИЯ ГОЛОСОВЫХ ДИПФЕЙКОВ

И.С. Дейкало, В.Д. Вольфович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. С развитием информационных технологий и искусственного интеллекта появились инструменты создания голосовых дипфейков, представляющие серьезную угрозу для информационной безопасности и доверия к аудиоконтенту. Данная технология может быть использована для манипуляции общественным мнением и введения в заблуждение. Голосовые подделки активно применяются в мошеннических схемах, что создает значительные риски для финансовых организаций, корпоративных структур и персональных данных пользователей. В данной работе рассматриваются ключевые технологии синтеза речи, включая Text-to-Speech и Voice Conversion. Описан процесс создания

голосового дипфейка с использованием сервиса iMyFone VoxBox. Проведен анализ методов выявления подделок, включая онлайн-сервис Deepfake-o-Meter и спектральный анализ аудиозаписей. Работа направлена на демонстрацию процесса создания голосового дипфейка и использования доступных инструментов для его последующего анализа и возможного применения в контексте защиты данных.
Ключевые слова: голосовой дипфейк, обнаружение голосового дипфейка, Text-to-Speech, iMyFone VoxBox, анализ спектрограммы.

METHODOLOGY OF VOICE-DEEPFAKE DETECTION

I.S. Deikalo, V.D. Volfovich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. With the development of information technology and artificial intelligence, tools for creating voice deepfakes have emerged, posing a serious threat to information security and trust in audio content. This technology can be used to manipulate public opinion and mislead. Voice forgeries are actively used in fraudulent schemes, which creates significant risks for financial organizations, corporate structures and personal data of users. This paper discusses key speech synthesis technologies, including Text-to-Speech and Voice Conversion. The process of creating a voice deepfake using the iMyFone VoxBox service is described. The analysis of methods for detecting fakes, including the online Deepfake-o-Meter service and spectral analysis of audio recordings, was carried out. The work is aimed at demonstrating the process of creating a voice deepfake and using available tools for its subsequent analysis and possible application in the context of data protection.
Keywords: voice deepfake, voice deepfake detection, Text-to-Speech, iMyFone VoxBox, spectrogram analysis.

Введение

Стремительное развитие информационных технологий, в частности искусственного интеллекта, открыло обширный набор инструментов для создания дезинформации – дипфейк или же синтез подходящего для манипулятора материала в формате видео, аудио или изображения для распространения вымысла в пагубных целях. В последнее время данную технологию используют для введения людей в заблуждение, подрывая репутацию некого объекта. Результативность дипфейк-технологий и дальнейшие перспективы развития заставляют остерегаться и стимулируют выявление способов противодействия. В данной статье будет рассмотрен именно голосовой дипфейк, так как является наиболее распространенным в мошеннических махинациях.

Основная часть

Для лучшего и более глубокого понимания темы, стоит ознакомиться с основными методами реализации данной технологии.

Преобразование текста в речь (Text-to-Speech). Данный метод основан на технологиях искусственного интеллекта, где текстовая информация преобразуется в синтезированную речь, имитирующую голос реального человека. Нейронные сети и модели глубокого обучения позволяют создавать аудиозаписи с высокой степенью реалистичности, что затрудняет их различение от подлинных. На данный момент существуют такие модели Text-to-speech, как VoCo, MelGAN, AdaSpeech, Tacotron 2, DeepVoice 3, MelNet, GlowTTS [1].

Преобразование голоса (Voice Conversion), включая имитацию. Преобразование голоса предполагает изменение характеристик исходного голоса говорящего таким образом, чтобы он звучал как голос другого человека. Этот процесс также реализуется с помощью алгоритмов глубокого обучения и нейронных сетей, которые анализируют и воспроизводят уникальные особенности голоса, такие как тембр, интонация и

акценты. Существуют такие модели, как Voice Conversion: Cotatron, Assem, Mellotron VC, StarGAN VC, PPG-VC [1].

Для целей исследования авторами был создан экземпляр голосовой подделки с помощью сервиса iMyFone. Процесс включал несколько последовательных этапов, начиная с записи образцов реального голоса и заканчивая получением голосового дипфейка.

После записи образцов голоса было решено дополнительно улучшить качество записи путем шумоочистки. Этот процесс позволил снизить уровень фоновых помех и повысить четкость звука, что было критически важно для последующего использования записи в качестве исходных данных для синтеза голосового дипфейка.

Полученная аудиозапись была загружена в сервис iMyFone VoxBox, который использует методы машинного обучения для синтеза речи. Было введено текстовое сообщение «*Мне очень тяжело, попал в беду и нуждаюсь в помощи. Каждая ваша поддержка важна для меня. Перевести средства можно на карту или через кошельки*», необходимый для реализации эксперимента, а также аудиофайл с записью голоса. На основе предоставленных данных, сервис использовал алгоритмы, которые анализируют особенности произношения, тембр, интонации и другие параметры голоса.

Была проведена проверка существующих сервисов обнаружения подделок. Первым был рассмотрен онлайн сервис Deepfake-o-Meter, который предоставляет возможность проверки аудиофайла на составляющие дипфейка с помощью определенной модели. По результатам модели «RawNet3(2023)» была высчитана процентная вероятность в 83,3 %, что экземпляр представляет синтезированную подделку (рис. 1).

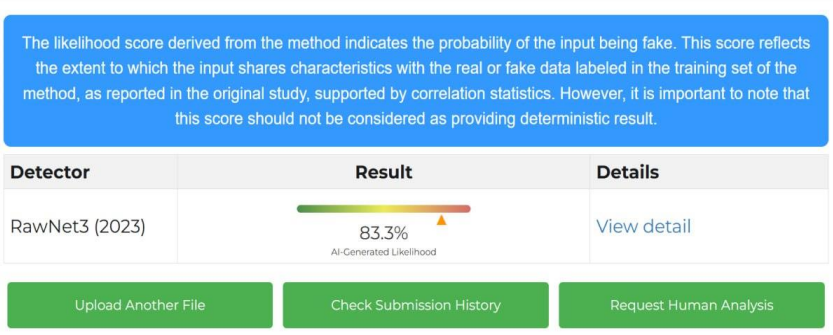


Рис. 1. Результаты проверки сервисом Deepfake-o-Meter
Fig. 1. Results of the Deepfake-o-Meter service check

Вторым методом является спектральный анализ. Для проверки была записана речь такого-же содержания настоящим человеком, голос которого был взят за основу при генерации с помощью сервиса iMyFone VoxBox. С помощью другого сервиса были извлечены спектрограммы человеческого и синтезированного происхождения.

На рис. 2 и рис. 3 представлены спектрограммы, на которых можно наблюдать некоторые схожести на начальных и конечных сегментах. Однако, стоит заметить, что в большинстве своем синтезированный экземпляр является обрезанной и неполной версией человеческой речи, хоть на выходе и звучит более чем правдоподобно. Самым главным наблюдением является аномалия в центральном сегменте, которая является главным доказательством работоспособности спектрального анализа для выявления подделок. Дело в том, что спектрограмма отображает изменение непрерывного аудио сигнала во времени [2]. А наличие аномальных пустот гласит о том, что присутствуют

незаметные для человеческого организма прерывания в сигнале, что противоречит природе человеческой речи.

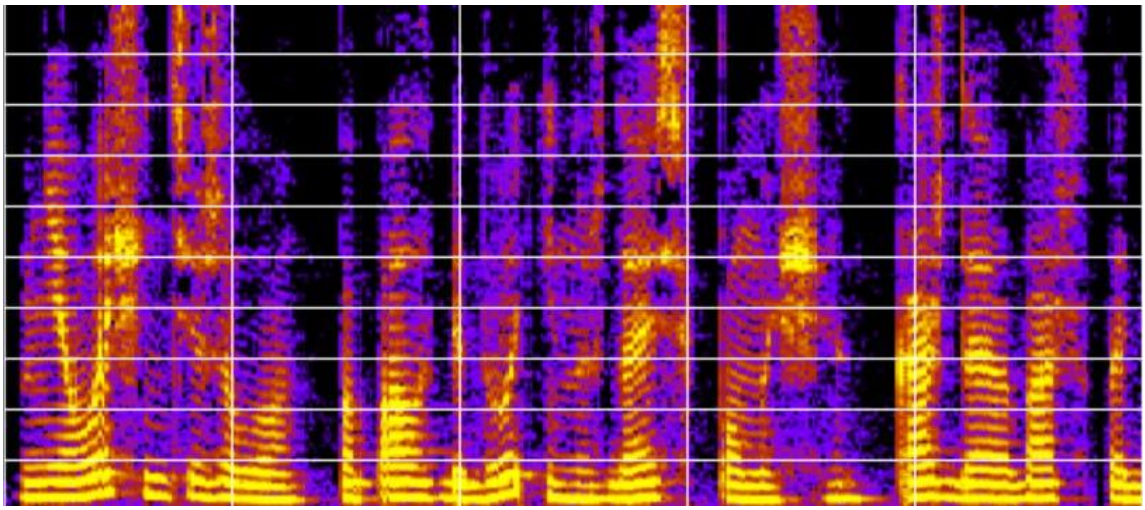


Рис. 2. Спектрограмма реального голосового сообщения
Fig. 2. Spectrogram of a real voice message

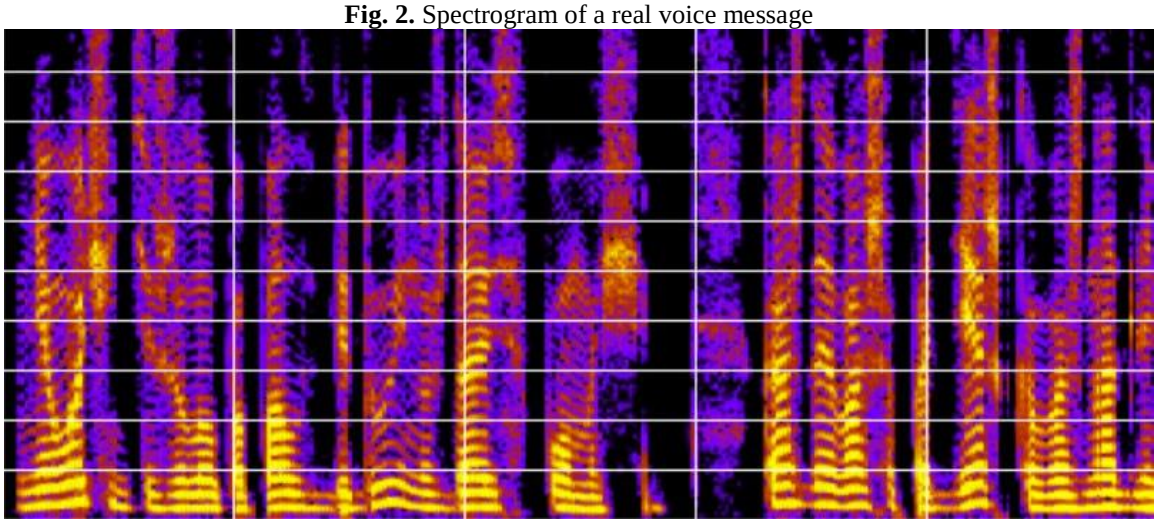


Рис. 3. Спектрограмма синтезированного голосового сообщения
Fig. 3. Spectrogram of a synthesized voice message

Заключение

В рамках исследования был синтезирован экземпляр голосового дипфейка и проведен его спектральный анализ. Анализ показал наличие выраженных различий в исходном и синтезированном речевом фрагменте, что можно использовать в дальнейших исследованиях методов выявления голосовых дипфейков.

Список использованных источников / References

1. Khanjani Z., Watson G., Janeja V.P., Audio deepfakes: A survey. Front. Big Data. 5:1001063. – 24 P. DOI: 10.3389/fdata.2022.1001063

2. Blue L., Warren K., Abdullah H., Gibson C., Vargas L., O'Dell J., Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. University of Florida. 978-1-939133-31-1.

Сведения об авторах

Дейкало И.С., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ila.dejkalo.rabota@gmail.com.
Вольфович В.Д., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», volfovich-v@inbox.ru.

Information about the authors

Deikalo I.S., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ila.dejkalo.rabota@gmail.com.
Volfovich V.D., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", volfovich-v@inbox.ru.

УДК 004.056.53

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ FORTIGATE

М.К. До[1], В.К. Фунг[2]
[1] Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь
[2]Университет ИТМО, Санкт-Петербург, Россия

Аннотация. В статье представлены результаты исследования функциональности Intrusion Prevention System (IPS) межсетевого экрана FortiGate. Описаны методы выявления угроз и предотвращения их проникновения в сеть. Составлена методика конфигурации IPS-систем и тестирования ее работы.
Ключевые слова: IPS, FortiGate, FortiNet, FortiGuard, NGFW, сигнатура, аномалия, угроза.

FORTIGATE INTRUSION PREVENTION SYSTEM

M.K. Do[1], V.Q. Phung[2]
[1]Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus
[2]ITMO University, Saint Petersburg, Russia

Abstract. The article presents the results of the study of the definition of Intrusion Prevention System (IPS) FortiGate firewall. The method of identifying threats and preventing their penetration into the network is shown. The configuration method of IPS systems and its operation testing is compiled.
Keywords: IPS, FortiGate, FortiNet, FortiGuard, NGFW, signature, anomaly, threat.

Введение

В современном мире, где информационные технологии играют ключевую роль в функционировании бизнеса и общества, защита данных и сетевой инфраструктуры становится одной из главных задач. Кибератаки на компьютерные системы становятся все более изощренными, что требует от организаций применения эффективных мер безопасности. Одним из таких решений является система предотвращения вторжений (Intrusion Prevention System, IPS), которая активно используется для защиты сетевых ресурсов. FortiGate – это межсетевой экран для обеспечения безопасности, предоставляемый компанией Fortinet. Он сочетает в себе функции межсетевого экрана, антивируса, системы предотвращения вторжений и др. FortiGate позволяет не только обнаруживать и блокировать угрозы в реальном времени, но и анализировать трафик, предоставляя администратору возможность оперативно реагировать на инциденты.

Основная часть

Система предотвращения вторжений (IPS) обнаруживает сетевые кибератаки и предотвращает угрозы, которые могут нанести ущерб сети, включая защищенные устройства. IPS может быть в виде отдельного устройства или части набора функций межсетевого экрана нового поколения (NGFW), такого как FortiGate [1]. IPS использует сигнатуры, декодеры протоколов, эвристику (или поведенческий мониторинг), аналитику угроз (например, FortiGuard Labs) и расширенное обнаружение угроз для предотвращения эксплуатации известных и неизвестных угроз нулевого дня. FortiGate IPS также выполняет глубокую проверку пакетов для сканирования зашифрованных полезных нагрузок для обнаружения и предотвращения угроз со стороны нарушителей.

Решение FortiNet объединяет ведущую в отрасли аналитику угроз от FortiGuard Labs с FortiGate NGFW для выявления новейших угроз и предотвращения их проникновения в сеть. Сигнатуры IPS являются одним из таких методов предоставления актуальной защиты. FortiGuard Labs использует искусственный интеллект (AI) и машинное обучение (ML) для анализа миллиардов событий каждый день. Исследовательская группа FortiGuard Labs также активно проводит исследования угроз для обнаружения новых уязвимостей и их эксплуатации и создает сигнатуры для выявления таких угроз. Сигнатуры IPS ежедневно обновляются на межсетевых экранах FortiGate.

Датчик FortiGate IPS представляет собой набор сигнатур и фильтров IPS, которые определяют область сканирования движка IPS при применении датчика IPS. Датчик IPS может иметь несколько наборов сигнатур и/или фильтров. Набор сигнатур IPS состоит из выбранных вручную сигнатур, в то время как набор фильтров IPS состоит из фильтров на основе атрибутов сигнатуры, таких как цель, серьезность, протокол, ОС и приложение. Каждая сигнатура имеет предопределенные атрибуты и действия (блокировать, разрешать, карантин и др.). Также можно создавать пользовательские сигнатуры IPS для применения к датчику IPS.

IPS-систем предоставляют следующие возможности:

– обнаружение вторжения или сетевой атаки и их предотвращение;

– выявление возможных кибератак и уязвимостей;

– документирование существующих угроз;

– обеспечение контроля качества безопасности администрирования;

– получение актуальной информации о кибератаках;

– определение расположение источника кибератаки по отношению к локальной сети (внешние или внутренние).

В результате конфигурации IPS-систем на межсетевом экране FortiGate была составлена следующая методика:

1. Подключение к веб-интерфейсу межсетевого экрана FortiGate.
2. Создание датчика IPS.
3. Конфигурация набора сигнатур и фильтров IPS.
4. Активация датчика IPS в политике безопастности межсетевого экрана.

Для тестирования правильности работы IPS-систем на межсетевом экране FortiGate было осуществлено моделирование кибератаки, имитирующей несанкционированное удаленное подключение по протоколу RDP. Для этого был разработан макет корпоративной сети на платформе GNS3 [2-4]. В GNS3 была смоделирована локальная сеть, состоящая из FortiGate, FortiAnalyzer, FortiManager, ПК с операционной системой (ОС) Windows 7. Также в смоделированную сети добавлено устройство нарушителя с операционной системой Kali Linux (рисунок 1).

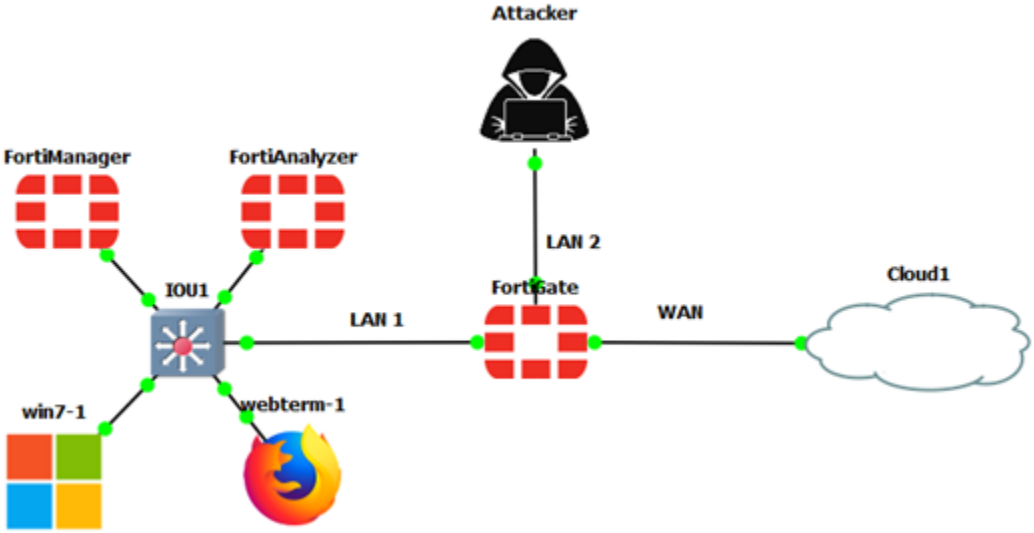
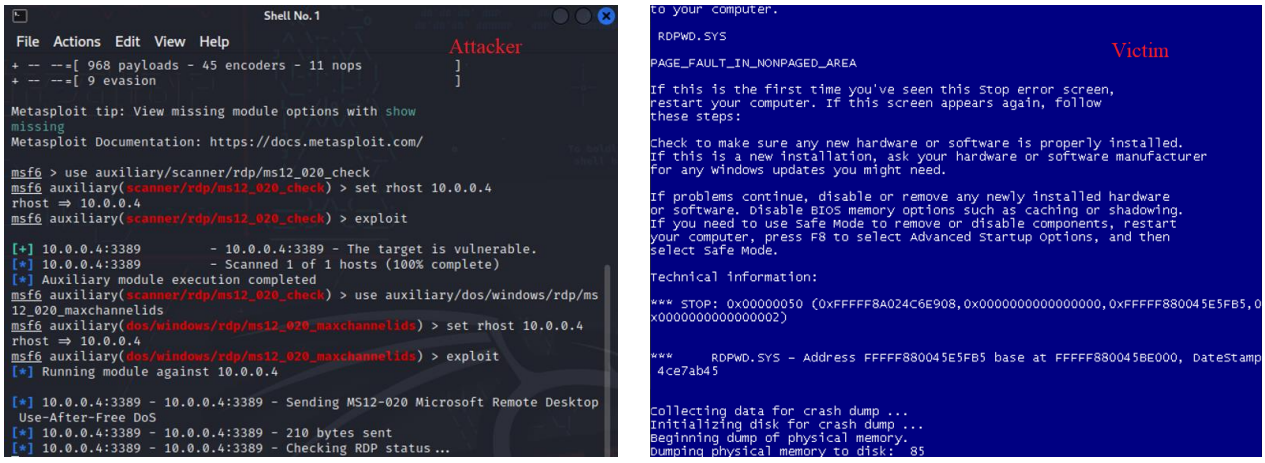


Рис. 1. Топология сети
Fig. 1. Network topology

С устройства с ОС Kali-Linux проведена кибератака на устройство с ОС Windows7 с помощью набора инструментов Metasploit (рисунок 2, а). В результате на компьютере с ОС Windows7 при выходе пользователя из системы появляется синий экран, как показано на рисунке 2, б.



a *b*

Рис. 2. Несанкционированное удаленное подключение по протоколу RDP (*a*) и его результат (*b*)
Fig. 2. Unauthorized remote connection via RDP protocol (*a*) and its result (*b*)

Для предотвращения вторжений нарушителя необходимо актировать IPS на FortiGate с профилем высокой безопасности, который фильтрует все предопределенные сигнатуры с определенными действиями и следующими типами: критический, высокий, средний (рисунок 3). Для сигнатур с низким типом устанавливается действие по умолчанию. В результате процесс несанкционированного удаленного подключения будет заблокирован, и попытка проникновения будет внесена в отчет событий на FortiAnalyzer, как показано на рисунке 4.

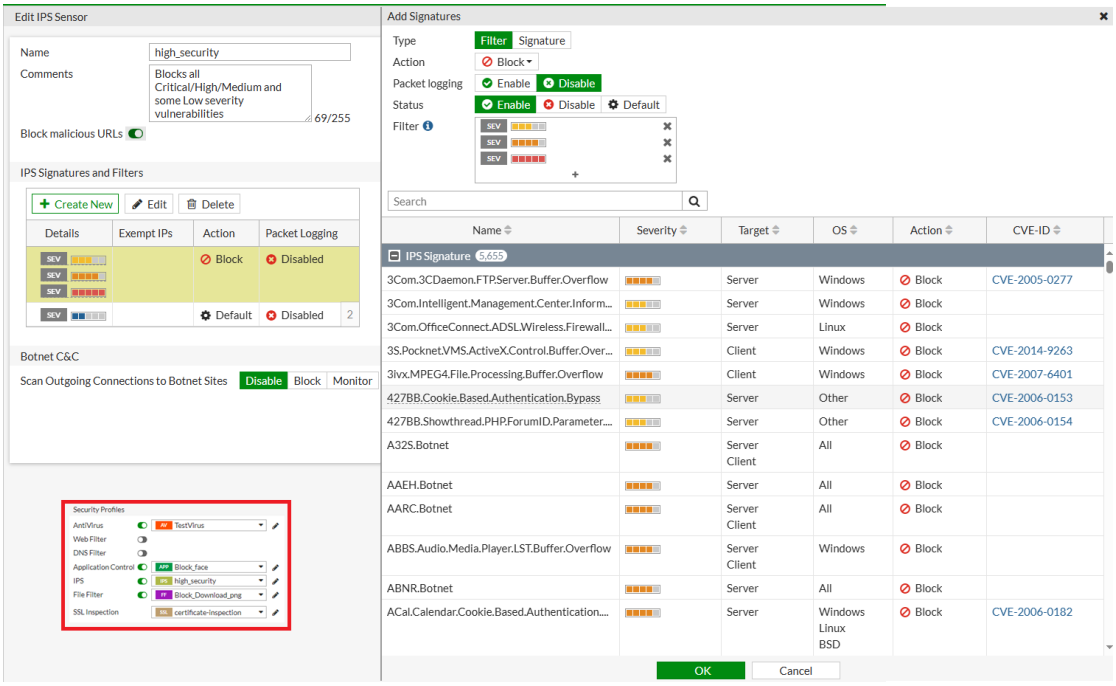


Рис. 3. Настройка IPS-систем с профилем высокой безопасности
Fig. 3. Configure IPS systems with a high security profile

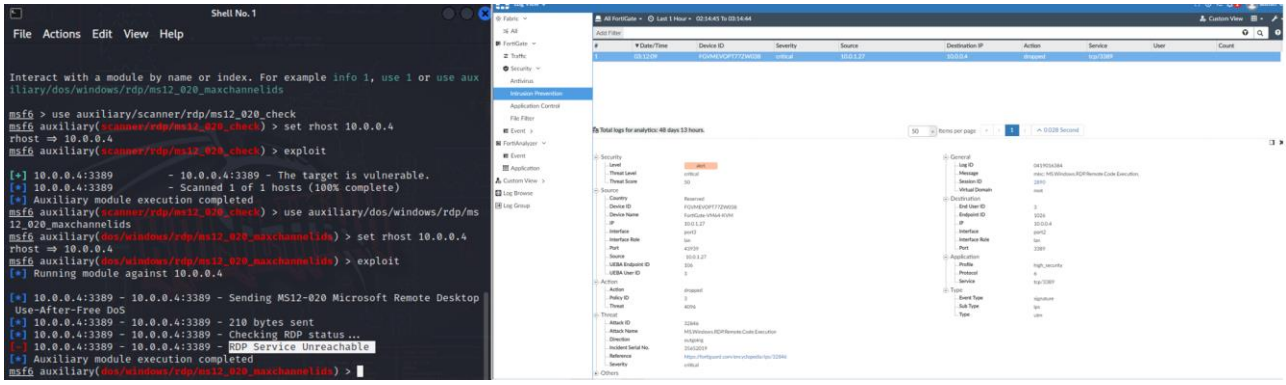


Рис. 4. Успешно блокировка несанкционированного удаленного подключения
Fig. 4. Successfully blocked unauthorized remote connection

Заключение

Таким образом, посредством реализации разработанной методики настройки IPS-систем и тестирования ее работы было установлено, что FortiGate использует сигнатуры, декодеры протоколов, эвристику, аналитику угроз и расширенное обнаружение угроз для предотвращения эксплуатации различных угроз. Благодаря такому раннему обнаружению угроз аномалии кибератак пакеты блокируются еще до проверки другими политиками (антивирус, веб-фильтр и др.). Также необходимо отметить, что составными элементами IPS-систем являются сенсоры IPS, которые проверяют сетевой трафик, поступающий на интерфейс, на наличие аномальных параметров, указывающих на кибератаку.

Список использованных источников

1. Руководства администратора FortiGate/FortiOS 6.4.12 // Fortinet [Электронный ресурс] – 2025. – Режим доступа: https://docs.fortinet.com/document/forti-gate/6.4.12/administration-guide/565562/intrusion-prevention. – Дата доступа: 06.02.2025.

2. До, М.К. Обоснование выбора эмулятора GNS3 для изучения принципов построения локальных сетей с межсетевым экранированием / М.К. До, Е.С. Белоусова // 59-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17–21 апреля 2023 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2023. – С. 41-43.

3. Богатырев В.А. Структурная надежность многопутевой маршрутной сети с реконфигурациями при переключении маршрутов / Богатырев В.А., Ле А., Абрамова Е.А. // Международная российская конференция по автоматике (RusAutoCon), 2022, стр. 414-418.

4. Богатырев В.А. Надежность реконфигурируемой сети с переключением сегментов / Богатырев В.А., Ле А., Абрамова Е.А. // Волновая электроника и инфокоммуникационные системы: материалы XXVI международной научной конференции (Санкт-Петербург, 29 мая-2 июня 2023г.) – 2023. – Т. 1. – С. 26-31.

References

1. Admin Guides FortiGate/FortiOS 6.4.12 // Fortinet [Electronic resource] – 2025. – Access mode: https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/565562/intrusion-prevention. – Date of access: 06.02.2025.

2. Do, M.K. Justification for the Choice of the GNS3 Emulator for Studying the Principles of Building Local Area Networks with Firewalling / M.K. Do, E.S. Belousova // 59th Scientific Conference of Postgraduate, Master's and Undergraduate Students of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", April 17-21, 2023, BSUIR, Minsk, Belarus: Collection of Materials. – Mn. – 2023. – P. 41-43.

3. Bogatyrev V.A. Structural reliability of a multipath routing network with reconfigurations when switching routes / Bogatyrev V.A., Le A., Abramova E.A // 2022 International Russian Automation Conference (RusAutoCon), 2022, pp. 414-418.

4. Bogatyrev V.A. Reliability of a reconfigurable network with segment switching / Bogatyrev V.A., Le A., Abramova E.A. // Wave electronics and infocommunication systems: materials of the XXVI international scientific conference (St. Petersburg, May 29 - June 2, 2023) –2023. – V. 1. – P. 26-31.

Сведения об авторах

До М.К., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», domanhkiemnd@gmail.com.
Фунг В.К., аспирант, университет ИТМО, phungvanquy97@gmail.com

Information about the authors

Do M.K., Master's student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", domanhkiemnd@gmail.com.
Phung V.Q., Post-Graduate Student, ITMO University, phungvanquy97@gmail.com.

УДК 53.096

ЭЛЕКТРИЧЕСКИЕ И ОПТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ФОТОДЕТЕКТОРА УЛЬТРАФИОЛЕТОВОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ГЕТЕРОПЕРЕХОДА ОСУНТ / КРЕМНИЙ В ШИРОКОМ ДИАПАЗОНЕ ТЕМПЕРАТУР

Е.А. Дронина, Н.Г. Ковальчук, А.Л. Данилюк, С.Л. Прищепа
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Исследованы электрические и оптические характеристики фотодетектора ультрафиолетового излучения на основе гетероперехода ОСУНТ/кремний в температурном диапазоне от 20К до 300К.Полученные результаты позволяют получить важное представление о количественной характеристике высоты барьера Шоттки между умеренно легированным кремнием и пленкой из ОСУНТ. Также подобное исследование необходимо для более глубокого понимания фундаментальных принципов работы разрабатываемых на их основе фотодетекторов и расширения их рабочих температур.

Ключевые слова: Тонкая пленка из одностенных углеродных нанотрубок; химическое парофазное осаждение; рамановская спектроскопия; барьер Шоттки; высота барьера Шоттки; фактор неидеальности; фотодетектор на основе ОСУНТ; фоточувствительность.

ELECTRICAL AND OPTICAL CHARACTERISTICS OF UV PHOTODETECTOR BASED ON SWCNT / SILICON HETEROJUNCTION IN A WIDE TEMPERATURE RANGE

L.A. Dronina, N.G. Kovalchuk, A.L. Danilyul, S.L. Prischepa
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The electrical and optical characteristics of the ultraviolet photodetector based on SWCNT/silicon heterojunction in the temperature range from 20K to 300K have been investigated. The results obtained provide important insights into the quantitative characterization of the Schottky barrier height between moderately doped silicon and SWCNT film. Also, such a study is necessary for a deeper understanding of the of the fundamental principles of operation of photodetectors developed on their basis and expansion of their operating temperatures.
Keywords: Single-walled carbon nanotube thin film; chemical vapor deposition; Raman spectroscopy; Schottky barrier; Schottky barrier height; ideality factor; SWCNT-based photodetector; responsivity.

Введение

Фотодетекторы являются критически важными компонентами в современных технологиях, с приложениями, варьирующимися от мониторинга окружающей среды до систем связи, визуализации и медицинской диагностики [1]. Способность обнаруживать свет и преобразовывать его в электрический сигнал является фундаментальным процессом, который привел к разработке различных устройств, включая видеокамеры, солнечные элементы и оптические датчики [2, 3]. За последние несколько десятилетий область фотодетектирования претерпела значительные изменения, вызванные достижениями в области материаловедения, приборостроения и появлением новых приложений, требующих более высокой производительности.

Большое внимание уделяется поиску и применению в фотодетекторах новых материалов, способных повысить чувствительность, скорость обработки информации и расширить диапазон длин волн оптоэлектронных устройств. С этой точки зрения большим потенциалом обладают углеродосодержащие материалы, в первую очередь графен и углеродные нанотрубки (УНТ). Они прозрачны в видимой части спектра, а также в ультрафиолетовом и ближнем красном диапазонах, обладают высокой проводимостью. Подвижность носителей заряда в них достигает рекордных значений. Все это делает их весьма привлекательными для использования в качестве верхнего электрода в барьерах Шоттки, которые хорошо пропускают свет и быстро доставляют фотогенерированные носители заряда к электрическим контактам [4]. В данной работе рассматриваются свойства фотодетектора, сформированного на основе гетероперехода кремний/ пленка одностенных углеродных нанотрубок (ОСУНТ) с металлическим типом проводимости.

Результаты

Образцы изготавливались путем осаждения пленки ОСУНТ толщиной 30 нм на подложку из слабо легированного кремния. Пленка выращивалась методом химического парофазного осаждения при атмосферном давлении [5]. Полученные пленки исследовались с помощью спектроскопии комбинационного рассеивания света и ИК-спектроскопии. Было установлено, что трубки являются одностенными,

со средним диаметром 1,08 нм. Гистограмма распределения диаметров ОСУНТ показана на рис. 1.

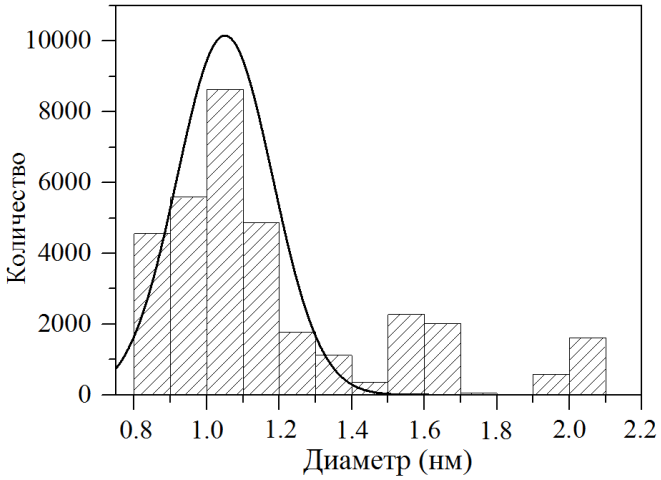


Рис. 1. Гистограмма распределения диаметров ОСУНТ (сплошная линия – распределение Гаусса)
Fig. 1. Histogram of SWCNTs diameter distribution (the solid line is for Gaussian fit)

Исследовались как темновые вольт-амперные характеристики (ВАХ) гетеропереходов ОСУНТ/Si, так и ВАХ при облучении длиной волны 375 нм. Измерения проводились в широком температурном диапазоне, от комнатной температуры до 10 К.

Из темновых ВАХ, в рамках модели термоэлектронной эмиссии, были получены значения высоты барьера Шоттки и коэффициента неидеальности, связанные с отклонением ВАХ от экспоненциального вида. Температурные зависимости этих параметров приведены на рис. 2.

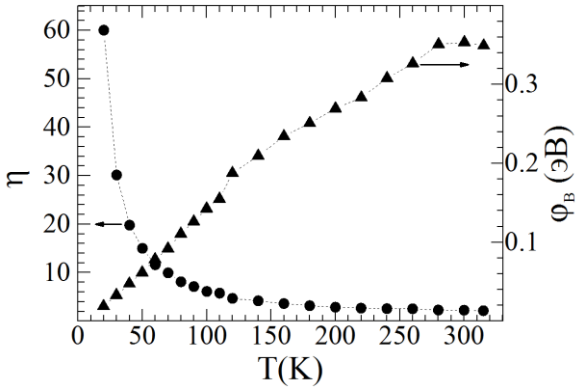
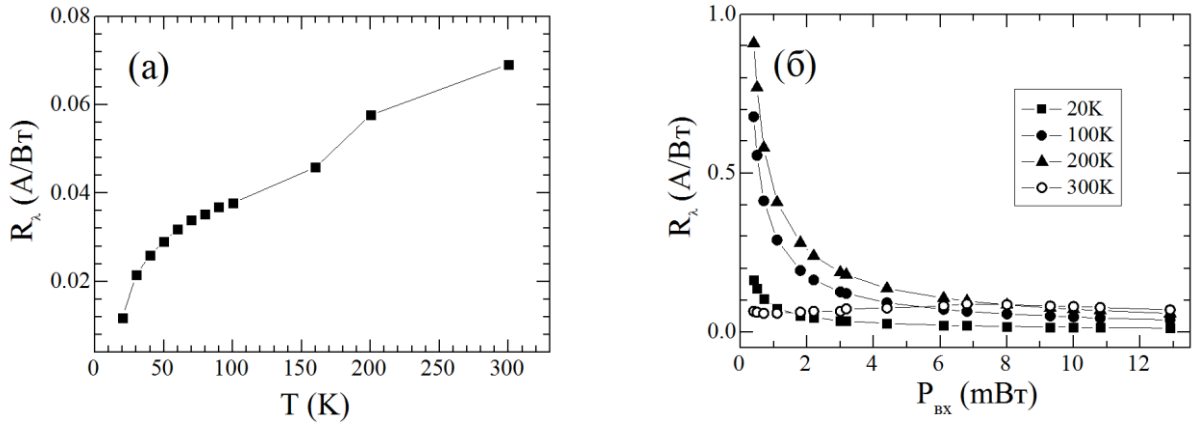


Рис. 2. Температурные зависимости коэффициента неидеальности и высоты барьера контактов Шоттки ОСУНТ/Si
Fig. 2. Temperature dependencies of the ideality coefficient and SWCNT/Si Schottky barrier height

Полученные зависимости свидетельствуют о наличии неоднородностей барьера с размерами меньше, чем ширина области пространственного заряда контакта (ОПЗ) [6, 7]. Действительно, наиболее вероятной физической причиной снижения барьера при низких температурах является наличие локальных барьеров малой высоты. С учетом того, что основным механизмом транспорта является термоэлектронная эмиссия, со снижением температуры малые барьеры начинают проявляться с большей вероятностью, чем высокие. В то же время рост коэфицциента неидеальности свидетельствует о том, что при низких температурах, помимо термоэлектронной

эмиссии, необходимо рассматривать и другие механизмы транспорта, такие как дрейф и диффузия носителей заряда, в области обедненного слоя, рассеяние на оптических фононах, квантово-механическое отражение, туннелирование через барьер [8,9].

Полученные зависимости параметров гетероперехода отражались на его фотодетектирующих свойствах. Анализируя обратные ветви ВАХ при облучении, были определены значения фоточувствительности при разных температурах. Эта зависимость приведена на рисунке 3а. Данные относятся к максимальной используемой плотности мощности облучения, 192 мВт/см^2. При этом было установлено, что со снижением плотности мощности облучения фоточувствительность растет, и для плотностей мощности 13 мВт/см^2 она достигает 0,9 А/Вт при 200 К, рис. 3, *б*.



a *b*

Рис. 3. Зависимость фоточувствительности гетероперехода ОСУНТ/Si от температуры (*a*) и мощности облучения (*b*)

Fig. 3. Responsivity of SWCNT/Si heterojunction as a function of temperature (*a*) and light power density (*b*)

Заключение

Выполнены исследования влияния температуры на параметры барьера Шоттки ОСУНТ/Si. Пленки ОСУНТ осаждались методом ХПО непосредственно на рабочее окно фотодетектора. Одностенность углеродных нанотрубок доказана методом спектроскопии комбинационного рассеяния света. Параметры барьера извлекались из анализа ВАХ, измеренных в диапазоне температур от 20 до 300 К. Полученные данные проанализированы в рамках теория термоэлектронной эмиссии. Установлено, что пространственные неоднородности барьера сильно влияют на параметры гетероперехода, оцененные в рамках термоэлектронной теории. На это указывает нелинейность температурных зависимостей как высоты барьера, так и фактора неидеальности. Последнее изменяется от 2,13 при комнатной температуре, что довольно типично для барьера Шоттки на основе SWCNT/Si SB, до 60 при T = 20 К. Такое поведение параметров при низких температурах объяснялось уменьшением роли термоэлектронной эмиссии и увеличением вклада других механизмов переноса тока в области низких температур. К таковым относятся дрейф, диффузия, туннелирование, рассеяние на оптических фононах и квантово-механическое надбарьерное отражение. Фоточувствительность сформированных фотодиодов зависела от температуры и мощности облучения. Она снижалась с понижением температуры и ростом мощности облучения. Полученное максимальное значение фоточувствительности в 0,9 А/Вт при малых мощностях облучения сравнимо с лучшими параметрами для фотодетекторов на основе ОСУНТ.

Список использованных источников / References

1. Fan P., Chettiar U.K., Cao L., Afshinmanesh F., Engheta N., Brongersma M.L. (2012) An Invisible Metal-Semiconductor Photodetector. *Nature Photonics*. 6, 380–385.

2. Fu X.W., Liao Z.M., Zhou Y.B., Wu H.C., Bie Y.Q., Xu J., et al. (2012) Graphene/ZnO Nanowire/Graphene Vertical Structure Based Fast-Response Ultraviolet Photodetector. *Applied Physics Letters*. 100 (22), 223114.

3. Wu S., Chen Y., Wang X., Jiao H., Zhao Q., Huang X. et al. (2022) Ultra-Sensitive Polarization-Resolved Black Phosphorus Homojunction Photodetector Defined by Ferroelectric Domains. *Nature Communications*. 13, 3198.

4. Scagliotti M., Salvato M., De Crescenzi M., Castrucci P., Kovalchuk N. G., Komissarov I. V, et al. (2019) 2D Carbon Material/Silicon Heterojunctions for Fast Response Self-Powered Photodetector. *International Journal of Nanoscience*. 18 (3&4), 1940088.

5. Dronina L A., Kovalchuk N. G., Komissarov I. V., Danilyuk A. L., Labunov V. A., Lutsenko E. V., et al. (2025) Properties of Single-Walled Carbon Nanotube Film/Si Heterojunctions Fabricated In-Situ. *Applied Nanoscience*. 15, 2.

6. Werner J. H., Güttler H. H. (1991) Barrier Inhomogeneities at Schottky Contacts. *Journal of Applied Physics* 69 (3)**,** 1522-1533.

7. Tung R. T. (1992) Electron Transport at Metal-Semiconductor Interfaces: General Theory. *Physical Review B* 45 (23), 13509-13523.

8. Sze S. M., Ng K. K. (2007) *Physics of Semiconductor Devices*. USA, John Wiley & Sons.

9. Kao K. C., Hwang W. (1981) *Electrical Transport in Solids*. England, Pergamon Press.

Сведения об авторах

Дронина Е.А., аспирант кафедры микро- и наноэлектроники (МНЭ), учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР), lizadronina@yandex.by.
Ковальчук Н.Г., науч. сотр. НИЛ «Интегрированные микро- и наносистемы», БГУИР, n.kovalchuk@bsuir.by.
Данилюк А.Л, канд. физ.-мат. наук, доц., доц. кафедры МНЭ БГУИР, danilyuk@bsuir.by.
Прищепа С.Л., д-р физ.-мат. наук, проф., проф. кафедры защита информации БГУИР, prischepa@bsuir.by

Information about the authors

Dronina L.A., Postgraduate Student at the Department of Micro and Nanoelectronics, Educational Institution "Belarusian State University of Informatics and Radioelectronics" (BSUIR), elizadronina@yandex.by.
Kovalchuk N. G. Researcher of the Research Laboratory at the Department of Micro- and Nanoelectronics. e-mail. n.kovalchuk@bsuir.by.
Danilyuk A. L. Cand. of Sci., Associate Professor at the Department of Micro- and Nanoelectronics, BSUIR, danilyuk@bsuir.by.
Prischepa S. L. Dr. Hab., Professor, Professor of the Information Protection Department, BSUIR, prischepa@bsuir.by.

УДК 004.056.53

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ KERBEROASTING

В.В. Дубовский, Е.С. Белоусова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Статья посвящена анализу угрозы безопасности Active Directory, известной как Kerberoasting, которая использует уязвимости протокола Kerberos для получения хешей паролей учетных записей сервисов. Авторы рассматривают основные этапы аутентификации Kerberos, методы проведения кибератаки, а также инструменты, используемые нарушителями. В работе предложены рекомендации по защите инфраструктуры Active Directory: использование стойких алгоритмов шифрования, мониторинг журналов безопасности и применение сложных паролей для учетных записей. Статья актуальна для специалистов в области кибербезопасности, занимающихся защитой корпоративных сетей.
Ключевые слова: Active Directory; Kerberos; Kerberoasting; аутентификация; хеши паролей; угрозы AD; мониторинг журналов.

KERBEROASTING INFORMATION SECURITY THREAT

V.V. Dubovsky, E.S. Belousova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article analyzes the Active Directory security threat known as Kerberoasting, which exploits vulnerabilities in the Kerberos protocol to obtain hashes of service account passwords. The authors review the main stages of Kerberos authentication, methods of cyberattack, and tools used by the attackers. The paper offers recommendations for protecting Active Directory infrastructure: using strong encryption algorithms, monitoring security logs and using complex passwords for accounts. The article is relevant for cybersecurity specialists involved in the protection of corporate networks.
Keywords: Active Directory; Kerberos; Kerberoasting; authentication; hash password; AD threats; log monitoring.

Введение

В условиях, когда кибербезопасность становится критически важной, защита Active Directory (AD) является приоритетной задачей для организаций. Специалисты отмечают, что AD в 90 % случаев выступает либо вектором кибератаки, либо средством закрепления или повышения привилегий в домене. При этом более 40% кибератак на AD оказываются успешными [1]. Около 90 % компаний в мире используют AD для управления учетными записями, что делает ее привлекательной целью для нарушителей. В последние годы наблюдается значительное увеличение числа кибератак на Active Directory. Это связано с тем, что данная система является важнейшим хранилищем информации, включая учетные записи и права доступа сотрудников. Распространенными угрозами для инфраструктуры AD являются Roasting-атаки (AS-REP Roasting, Kerberoasting). Техники таких атак представлены в MITRE ATT&CK: T1558 (Steal or Forge Kerberos Tickets) [2] и T1595 (Active Scanning) [3]. С уверенностью можно утверждать, что такие кибератаки являются одними из наиболее популярных в корпоративных сетях.

Roasting-атаки используют уязвимости в протоколе Kerberos для получения хешей паролей учетных записей. Kerberos – это протокол, который позволяет пользователям аутентифицироваться в сети и получать доступ к службам. По умолчанию Kerberos использует подключение TCP, порт 88 и является основным протоколом аутентификации для учетных записей домена, начиная с операционной системы Windows 2000. Благодаря Kerberos пользователю не нужно постоянно вводить свой пароль, а серверу не нужно знать пароль каждого пользователя. В 2023 году Microsoft объявила об отказе от использования аутентификации NTLM (NT LAN Manager), в пользу протокола Kerberos [4], что также подтверждает актуальность исследования уязвимостей данного протокола. Основное отличие Kerberos от NTLM заключается в процессе аутентификации. При использовании NTLM аутентификация осуществляется на сервере, к которому обращается клиент. Kerberos полагается на службу Центра распространения ключей KDC (Key Distribution Center), работающую на контроллере домена (DC). Целью работы является выявить уязвимости процесса аутентификации пользователя по протоколу Kerberos на основе его изучения, проанализировать механизмы кибератак и их влияние на безопасность Active Directory.

Основная часть

Процесс аутентификации по протоколу Kerberos осуществляется в соответствии со следующими этапами:

1. Пользователь авторизируется в системе. В результате успешной авторизации отправляется запрос AS-REQ (Authentication Service REQuest) на сервер аутентификации (AS) службы KDC. Запрос AS-REQ (Authentication Service REQuest) включает в себя: временную метку (timestamp), которая шифруется с использованием хэша пароля пользователя; идентификатор пользователя (Client Principal Name), который отправляется в незашифрованном виде (например, username@domain.name), чтобы KDC мог идентифицировать пользователя.

2. KDC проверяет имя пользователя и его хэш пароля в базе NTDS, расшифровывает временную метку. Если метка была расшифрована, то KDC отвечает клиенту сообщением AS-REP (Authentication Service REPly), содержащим сгенерированный ключ сеанса для KDC, метку времени, TGT (Ticket-Granting Ticket), срок действия билета TGT. Ключ сеанса для KDC, метка времени и срок действия TGT шифруются с использованием хэша пароля пользователя. Это позволяет гарантировать, что только легитимный клиент сможет расшифровать эти данные и получить доступ к TGT.

TGT содержит аналогичные данные (ключ сеанса, метку времени и срок действия), но также включает идентификатор клиента (Client Principal Name). Важно отметить, что TGT зашифрован с использованием хэша пароля специальной учетной записи KDC – krbtgt. Это гарантирует, что только KDC может создавать и проверять TGT, обеспечивая безопасность процесса аутентификации. По умолчанию срок действия TGT составляет 10 часов.

При попытке получения клиентом доступа к какому-либо сервису в домене отправляется запрос на получение билета для службы (TGS-REQ) на KDC, которое включает в себя аутентификатор (идентификатор клиента, временную метку), TGT и Principal сервиса. Аутентификатор зашифрован с использованием сеансового ключа, который был выдан KDC при получении TGT. Principal сервиса указывает, к какому конкретному сервису (например, файловому серверу или базе данных) клиент пытается получить доступ.

Сервер выдачи разрешений TGS (Ticket Granting Service) в KDC при обработке запроса TGS-REQ выполняет следующие шаги:

1. Проверяет, существует ли указанный в запросе сервис. Если сервис не найден, запрос отклоняется.

2. Сервер расшифровывает TGT и извлекает: сеансовый ключ для KDC, идентификатор клиента, временную метку.

3. Сервер расшифровывает аутентификатор и проверяет, совпадает ли идентификатор клиента из TGT с идентификатором, указанным в аутентификаторе, а также проверяет временную метку, которая не должна превышать 2 минут.

4. TGS выполняет подтверждения подлинности запроса, проверяя срок действия TGT, идентификатор клиента; временную метку аутентификатора.

5. Если все проверки пройдены, TGS отправляет клиенту сообщение TGS-REP, которое содержит зашифрованные на сеансовом ключе для KDC данные о принципале сервиса, к которому предоставлен доступ, временную метку, ключ сеанса для сервиса и срок действия билета для сервиса (TGS). Кроме того, в сообщении TGS-REP содержится сам билет TGS, зашифрованный с использованием секретного ключа

сервиса. Такой подход обеспечивает безопасность билета TGS, который может расшифровать только KDC и тот сервис, для которого он предназначен.

Основной уязвимостью рассмотренного процесса аутентификации по протоколу Kerberos является то, что любой аутентифицированный пользователь домена может запросить билет Kerberos для любой учетной записи сервиса (Service Account), если он знает Service Principal Name (SPN) этой учетной записи. Получив билет Kerberos для учетной записи сервиса, нарушитель может использовать его для брутфорс-атаки, так как этот билет зашифрован NTLM-хэшем пароля сервисной учетной записи. Если пароль слабый, нарушитель получает контроль над учетной записью сервиса.

Большинство сервисов выполняются машинными учетными записями (COMPUTERNAME$), которые имеют случайно сгенерированные пароли длиной 120 символов, что делает нецелесообразным применение брутфорса. Иногда сервисы выполняются учетными записями пользователей. Учетная запись пользователя имеет пароль, установленный человеком, который с гораздо большей вероятностью будет предсказуемым. Кибератака Kerberoasting ориентирована на подобные учетные записи.

Пример реализации кибератаки может быть рассмотрен на основе использования нарушителем модуля PowerView на захваченном устройстве, находящемся в домене с операционной системой Windows. Данный модуль осуществляет поиск учетных записей служб, зарегистрированных в домене. Это позволяет нарушителю получить список всех учетных записей, связанных с сервисами, такими как SQL Server, HTTP, Exchange и другими. Результат выполнения команды для перечисления всех SPN в домене можно увидеть на рис. 1.

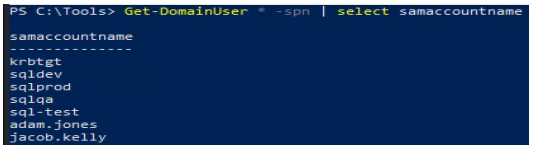


Рис. 1. Перечисление SPN с помощью модуля PowerView
Fig. 1. SPN enumeration using the PowerView module

В результате получения нарушителем списка SPN, возможно формирование запроса TGS для найденных учетных записей. Запросы отправляются с задержкой, маскируя их в общем потоке сетевого трафика. TGS зашифрован хэшем пароля учетной записи службы, что позволяет нарушителю, перехватив билет, попытаться подобрать пароль в автономном режиме. На рис. 2 представлен пример выполнение команды для запроса TGS.

Рис. 2. Запрос TGS для полученного SPN
Fig. 2. TGS request for a received SPN

После получения билета, нарушитель может в автономном режиме, без риска блокировки учетной записи, перебирать пароли, используя различные средства и методы для расшифровки, например Hashcat. Результат успешного перебора пароля можно увидеть на рис. 3.

Рис. 3. Результат получения учетных данных с помощью Hashcat
Fig 3. Result of obtaining credentials using Hashcat

Атакующий может провести аналогичные действия с устройства с ОС Linux, используя скрипт GetUserSPNs.py, который входит в набор инструментов Impacket. Нарушитель запускает скрипт, указав домен, контроллер домена и учетные данные. В результате нарушитель также может получить TGS билет, который использовать для брутфорса с использованием Hashcat.

Заключение

Несмотря на существование различных методов обнаружения и предотвращения Roasting-атак, они остаются актуальной проблемой для многих организаций. Это связано с рядом факторов, включая сложность настройки и мониторинга Active Directory, недостаточную осведомленность администраторов о существующих угрозах и использование устаревших версий программного обеспечения.

Для защиты от Roasting-атак рекомендуется убедиться, что предварительная аутентификация включена для всех учетных записей, кроме случаев, когда это необходимо для совместимости со старыми протоколами. Рекомендуется использовать стойкие алгоритмы шифрования Kerberos, такие как AES, и отказаться от устаревшего RC4. Регулярно следует проверять журналы на подозрительную активность, особенно для сервисных учетных записей. Обнаружение атак возможно путем мониторинга событий в журналах безопасности, таких как Event ID 4769 и 4768, связанных с изменениями учетных записей и запросами билетов Kerberos. Также необходимо использовать длинные и сложные пароли для учетных записей и ограничивать их права доступа.

Список использованных источников

1. Скоропупов И.О., Бубнова А.А., Карманов И.Н. Методы проведения атак для получения прав администратора домена в Active Directory // Интерэкспо Гео-Сибирь. 2019. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-provedeniya-atak-dlya-polucheniya-prav-administratora-domena-v-active-directory.

2. Еремеев М.А., Смирнов С.И., Прибылов И.А. ОБНАРУЖЕНИЕ ВРЕДОНОСНЫХ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА НА ОСНОВЕ ЖУРНАЛОВ СОБЫТИЙ ПРИ РАССЛЕДОВАНИИ ПРОДОЛЖАЮЩЕГОСЯ КИБЕРИНЦИДЕНТА // Инновационные аспекты развития науки и техники. 2021 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/detection-of-malicious-actions-of-an-attacker-based-on-event-logs-when-investigating-an-ongoing-cyber-incident.

References

1. Skoropupov I.O., Bubnova A.A., Karmanov I.N. Attack methods for obtaining domain administrator rights in active directory // Interexpo Geo-Siberia. 2019. [Electronic resourse]. – Mode of access: https://cyberleninka.ru/article/n/metody-provedeniya-atak-dlya-polucheniya-prav-administratora-domena-v-active-directory. – Date of access: 20.02.2025

2. Eremeev M.A., Smirnov S.I., Pribylov I.A. DETECTION OF MALICIOUS ACTIONS OF AN ATTACKER BASED ON EVENT LOGS WHEN INVESTIGATING AN ONGOING CYBER INCIDENT // Innovative aspects of science and technology development. 2021 [Electronic resourse]. – Mode of access: https://cyberleninka.ru/article/n/detection-of-malicious-actions-of-an-attacker-based-on-event-logs-when-investigating-an-ongoing-cyber-incident.

Сведения об авторах

Дубовский В.В., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.dubovski007@gmail.com.
Белоусова Е.С., кандидат технических наук, доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Dubovsky V.V., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", v.dubovski007@gmail.com.
Belousova E.S., PhD, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", belousova@bsuir.by.

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КЛАССИЧЕСКИХ И КВАНТОВЫХ МЕТОДОВ ШИФРОВАНИЯ

А.Ю. Ефремова, А.Н. Морозова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В представленной статье проведен сравнительный анализ классических и квантовых методов шифрования, с указанием их индивидуальных особенностей. Классические методы, такие как симметричное и ассиметричное шифрование, широко используются в современных системах безопасности, однако они подвержены угрозам взлома, связанным с развитием вычислительных технологий. В то же время квантовые методы шифрования, основанные на принципах квантовой механики, предлагают новые уровни безопасности благодаря использованию кубитов и явлению квантовой запутанности. Сравнительный анализ проводился по следующим показателям: скорости шифрования, сложности реализации, возможности применения, уязвимости к атакам, стоимости реализации.
Ключевые слова: безопасность данных; шифрование; классические методы шифрования; симметричное шифрование; ассиметричное шифрование; квантовая криптография; параметры; сравнительный анализ.

COMPARATIVE ANALYSIS OF CLASSICAL ENCRYPTION AND QUANTUM ENCRYPTION METHODS

A.Y. Yafremava, A.N. Morozova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In the presented article, a comparative analysis of classical and quantum encryption methods is conducted, highlighting their individual characteristics. Classical methods, such as AES and RSA, are widely used in modern security systems; however, they are susceptible to threats associated with the advancement of computational technologies. At the same time, quantum encryption methods, based on the principles of quantum mechanics, offer new levels of security through the use of qubits and the phenomenon of quantum entanglement. The comparative analysis is carried out based on the following criteria: encryption speed, implementation complexity, application possibilities, vulnerability to attacks, and implementation cost.
Keywords: encryption, data security; threat of hacking; comparative analysis, classical encryption methods, symmetric encryption; asymmetric encryption; quantum cryptography; quantum key distribution; quantum mechanics.

Введение

Вопрос безопасности в современном мире, где комфортную жизнь нельзя представить без обмена данными, занимает главенствующую роль. Большая часть этих данных содержит конфиденциальную информацию, распространение которой может нанести значительный ущерб. Для предотвращения распространения конфиденциальной информации используются специализированные системы

шифрования, гарантирующие, что доступ к этим данным смогут иметь только пользователям, обладающим ключами шифрования.

На протяжении многих лет использовались классические методы шифрования, так как они были в значительной степени эффективны, однако эти методы бессильны против квантовой угрозы. В таком случае наиболее верным решением станет использование квантовой криптографии.

В данной статье будут рассмотрены основные отличия классических методов шифрования от квантовых. В качестве сравниваемых параметров рассматриваются скорость шифрования, сложность реализации, возможности применения, уязвимость к атакам, а также стоимость реализации.

Основная часть

Под классическим шифрованием понимают совокупность методов шифрования, использующих простые алгоритмы и ключи для преобразования открытого текста в зашифрованный. В основе классического шифрования заложены методы, которые использовались еще до появления современных компьютерных алгоритмов. Среди таких шифров можно выделить шифр Цезаря (метод заключается в сдвиге алфавита на фиксированное число позиций), шифр Виженера (метод, в котором применяется ключевое слово для управления сдвигами), шифр *Playfair* (шифр, использующий квадрат символов 5×5 для шифрования биграмм), шифр транспозиции (шифр, использующий перестановку символов в тексте согласно определенной схеме, не изменяя сами символы), а также уже известное шифрование с использованием ключей.

Классические методы шифрования включают в том числе и симметричное и ассиметричное шифрование. Симметричное шифрование является фундаментальным методом, в котором для преобразования данных применяется один и тот же ключ. К наиболее известным алгоритмам симметричного шифрования обычно относят *DES* (относительно устаревший, использует ключ в 56 бит), *Triple DES* (улучшенная версия *DES*, использующая три итерации шифрования), *AES* (более безопасный по сравнению с *Triple DES*, поддерживающий ключи длинной в 128, 192 и 256 бит).

Симметричное шифрование позволяет быстро обрабатывать большие объемы данных, требуя при этом меньше вычислительных ресурсов. Несмотря на относительно невысокий уровень безопасности, симметричное шифрование широко используется для защиты файлов и данных на жестких дисках (*BitLocker*), передачи данных через защищенные каналы (*SSL/TLS*), а также для *VPN* соединений.

Асимметричное шифрование – это более сложный метод шифрования, который использует два ключа: открытый (публичный) и закрытый (приватный). Использование двух ключей обеспечивает высокий уровень безопасности, а также является основой многих современных систем. Открытый ключ используется для шифрования данных и находится в открытом доступе для пользователей, отправляющих зашифрованное сообщение. Закрытый ключ используется для расшифровки полученных данных и известен только владельцу.

Методы ассиметричного шифрования просты в реализации. Виду отсутствия необходимости передачи секретного ключа, риск его компрометации значительно снижен. В отличие от симметричного шифрования, асимметричное требует больше времени на обработку, что делает его менее подходящим для шифрования больших объемов данных. Высокий уровень безопасности позволяет применять ассиметричное шифрование во многих сферах, например, для создания и проверки цифровых подписей, подтверждающих подлинность сообщений, и в протоколах передачи, таких как SSL/TLS. Квантовое шифрование, также называемое квантовой криптографией, –

это метод шифрования, основанный на использовании квантовых битов для передачи и защиты информации с высоким уровнем безопасности [1].

Для квантового шифрования характерны следующие принципы: квантовая суперпозиция, принцип неопределенности и квантовая запутанность.

Целью квантовой криптографии является защита данных от квантовых угроз. Квантовая криптография, также называемая квантовым шифрованием, использует свойства квантовой механики для обеспечения безопасности данных. Квантовая криптография использует непредсказуемость природы материи на квантовом уровне для шифрования и дешифрования сообщений, что обеспечивает более высокий уровень безопасности. Информация в классических методах шифруется в битах, в то время как в квантовой криптографии используются кубиты.

Наиболее известным примером квантовой криптографии является квантовое распределение ключей (КРК), позволяющее двум сторонам обмениваться данными безопасно, значительно снижая риски взлома. В отличие от других методов, квантовое распределение ключей позволяет взаимодействующим сторонам обнаружить попытки перехвата сообщения за счет ввода ошибок в структуру кубитов при попытке взлома или измерения данных. Кроме того, квантовая криптография теоретически устойчива к увеличению мощности квантовых вычислений.

При этом, каналы связи квантового распределения ключей требуют тщательной настройки и надлежащего набора аппаратного обеспечения, такого как оптоволоконные соединения и фотонные излучатели для передачи и приема зашифрованных данных. В масштабах предприятия создание инфраструктуры для КРК может обойтись в несколько миллионов долларов, при этом для внедрения необходимы специализированные аппаратные каналы [2, 3].

Подробное сравнение методов шифрования представлено в таблице 1.

Таблица 1. Сравнительный анализ классических и квантовых методов шифрования
Table 1. Comparative Analysis of Classical and Quantum Encryption Methods

Характеристика	Классические методы шифрования	Квантовые методы шифрования
1	2	3
Скорость шифрования	150 Кбит –1 Гбит/с	1–10 Мбит/с
Сложность реализации	Необходимость в специализированном оборудовании присутствует только в случае повышения производительности. Необходимость в специализированной среде отсутствует. Достаточными являются общие знания о криптографии и управлении ключами.	Необходимость в специализированных устройствах (квантовые источники фотонов, детекторы и оптические волокна). Необходимость в специализированной инфраструктуре – надежной оптической сети. Необходимость в глубоких знаниях в области квантовой механики.
Возможности применения	Используется для шифрования различных объемов данных, таких как файлы, сетевые потоки, ключи шифрования и цифровые подписи.	Используется для защиты транзакций, обеспечения безопасности в чувствительных операциях, защиты данных в корпоративных сетях, обеспечения безопасности при подключении к сети и для защиты систем управления и мониторинга.

Продолжение таблицы 1
Continuation of table 1

1	2	3
Уязвимость к атакам	Методы уязвимы к следующим атакам: атака по шифротексту, атака по открытому тексту, атака на ключ, атака на алгоритм, атака на временные уязвимости, атака на подмену ключа. Менее безопасный вид шифрования.	Методы уязвимы к следующим атакам: атаки на источник квантовых битов, атаки на каналы передачи, атаки на протоколы, шум и потери в канале, атаки при помощи квантовых компьютеров. Более безопасный вид шифрования.
Стоимость реализации	Стоимость реализации варьируется в зависимости от метода, однако затраты сравнительно небольшие ввиду возможности реализации на стандартном оборудовании.	Для реализации требуются значительные инвестиции ввиду затрат на оборудование, развивающиеся технологии, а также обучение сотрудников.

Заключение

Исходя из данных в таблице видно, что классические методы шифрования остаются актуальными для защиты многих типов данных, но их уязвимость к атакам делает их менее перспективными для крупных систем с оборотом конфиденциальных данных. Квантовые методы шифрования обеспечивают высокий уровень безопасности благодаря уникальным свойствам квантовой механики, однако их реализация требует специализированного оборудования и знаний. Таким образом, выбор между этими методами зависит от конкретных требований безопасности и доступных ресурсов.

Список использованных источников

1. Алефиренко В.М., Ефремова А.Ю., Асиненко А.М. (2024) Анализ современных подходов к классификации методов шифрования. *SCIENCE TIME* (12), 45–50.
2. Stefano D.L., Tristan M., Samy C. (2024) Cryptographic security: Critical to Europe's digital sovereignty *European Parliamentary Research Service.* (11), 1–8.
3. Danda B.R., Kayhan Z.G. (2018) Smart Cities Cybersecurity and Privacy. USA, Washington.

References

1. Alefirenko V.M., Yafremava A.Y., Asinenko A.M. (2024) Analysis of Modern Approaches to the Classification of Encryption Methods. *SCIENCE TIME* (12), 45–50 (in Russian).
2. Stefano D.L., Tristan M., Samy C. (2024) Cryptographic security: Critical to Europe's digital sovereignty *European Parliamentary Research Service.* (11), 1–8.
3. Danda B.R., Kayhan Z.G. (2018) Smart Cities Cybersecurity and Privacy. USA, Washington.

Сведения об авторах

Ефремова А.Ю., ассистент кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.
Морозова А.Н., магистрант кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», annamorozova417@gmail.com.

Information about the authors

Yafremava A.Y., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", al617e13@gmail.com
Morozova A.N., Master's degree student of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", annamorozova417@gmail.com.

УДК 004.62

ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ И ВНЕДРЕНИЮ ФОРМАТА SDMX В РАМКАХ ИНФОРМАЦИОННОГО ОБМЕНА КОРПОРАТИВНЫМИ ДАННЫМИ

В.А. Завалей, И.Г. Скиба, С.А. Фурсанов
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются подходы к внедрению формата SDMX в корпоративных системах для стандартизации обмена данными. Анализируются его преимущества по сравнению с другими форматами, такими как XML, JSON и CSV, с акцентом на структурированность, поддержку метаданных и автоматизацию обработки. Обсуждаются основные этапы интеграции, возможные трудности и аспекты безопасности при передаче данных. Также рассматриваются перспективы применения SDMX с учетом современных требований к защите информации.
Ключевые слова: SDMX; корпоративный обмен данными; стандартизация данных; автоматизация обработки данных; безопасность данных; метаданные; интеграция информационных систем; сравнение форматов данных; XML; JSON.

APPROACHES TO THE USE AND IMPLEMENTATION OF THE SDMX FORMAT IN CORPORATE DATA EXCHANGE

V.A. Zavalei, I.G. Skiba, S.A. Fursanov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article examines approaches to the implementation of the SDMX format in corporate systems for data exchange standardization. Its advantages over other formats, such as XML, JSON, and CSV, are analyzed, with a focus on structuring, metadata support, and automation of data processing. The main stages of integration, possible challenges, and security aspects of data transmission are discussed. The paper also considers the prospects for using SDMX in the context of modern data protection requirements.
Keywords: SDMX; corporate data exchange; data standardization; data processing automation; data security; metadata; information systems integration; data format comparison; XML; JSON.

Введение

В современных корпоративных информационных системах эффективный обмен данными играет ключевую роль, однако рост объема информации и разнообразие форматов создают сложности при интеграции и обработке данных. Для упрощения этого процесса необходимы единые подходы к структуре и передаче данных, и в этой связи формат SDMX (Statistical Data and Metadata Exchange) был разработан как международный стандарт для унификации обмена статистическими и корпоративными данными. В отличие от XML и JSON, SDMX предлагает встроенную поддержку метаданных, улучшенную структуру и более высокую степень адаптации к автоматизированной обработке. Работа посвящена анализу подходов к внедрению SDMX в корпоративных системах, сравнению его с XML и JSON, а также вопросам безопасности при передаче данных, что позволит оценить перспективы его применения в условиях современных требований к информационному обмену.

Основная часть

1. Общие сведения о формате SDMX. Statistical Data and Metadata Exchange (SDMX) представляет собой международный стандарт для обмена статистическими и корпоративными данными. Он был разработан для обеспечения согласованности,

унифицированного подхода и структурированности информации между различными системами, что особенно важно в условиях увеличения объемов данных и требований к их обработке. SDMX активно используется такими организациями, как Международный валютный фонд (IMF), Всемирный банк (WB), Европейский центральный банк (ECB) и другими международными и национальными статистическими агентствами [1]. Основная цель SDMX – стандартизация процессов передачи, хранения и обработки данных, что снижает затраты на интеграцию различных систем и повышает эффективность работы с данными.

Ключевыми преимуществами SDMX являются строгая организация данных, поддержка метаданных и возможность автоматизированной обработки информации. Это делает формат особенно удобным для организаций, работающих с большими массивами информации, требующих не только передачи данных, но и их интерпретации, согласования с нормативными требованиями и обеспечения прозрачности процессов управления данными.

2. Сравнение SDMX с XML и JSON. Форматы XML и JSON широко применяются для обмена данными, однако они имеют ряд ограничений по сравнению с SDMX (таблица 1). XML отличается высокой формальностью, строгими требованиями к структуре данных и избыточностью, что увеличивает объем передаваемой информации. В то же время JSON является более легковесным и удобным для программной обработки, но не включает встроенные механизмы для работы с метаданными. SDMX, в свою очередь, объединяет структурированность XML и легкость автоматизации JSON, обеспечивая целостность данных и их стандартизированное описание [2].

Таблица 1. Сравнение SDMX, XML и JSON
Table 1. SDMX, XML and JSON comparison

Параметр	SDMX	XML	JSON
Структурированность данных	+	+	-
Поддержка метаданных	+	-	-
Автоматизация обработки	+	-	+
Объем передаваемых данных	-	-	+
Совместимость с системами	+	+	+
Гибкость использования	+	-	+

Как видно из таблицы, SDMX выигрывает по критически важным параметрам, таким как поддержка метаданных, структурированность данных и автоматизация обработки. Однако его применение требует более сложной настройки по сравнению с JSON и занимает больше места при передаче данных, чем облегченный JSON-формат.

3. Проблемы внедрения и аспекты безопасности. Несмотря на явные преимущества, внедрение SDMX сопряжено с рядом проблем. Основные сложности включают необходимость адаптации существующих корпоративных систем, обучение персонала и затраты на интеграцию. Кроме того, передача данных в SDMX требует соответствующих мер по обеспечению их безопасности, особенно если речь идет о конфиденциальных корпоративных или финансовых данных.

С точки зрения защиты информации SDMX предлагает механизмы шифрования, цифровой подписи и аутентификации, что позволяет снизить риски несанкционированного доступа и подделки данных [3]. Однако реализация этих механизмов требует дополнительных ресурсов и технических решений, что может стать барьером для внедрения в организациях с ограниченными IT-ресурсами.

4. Перспективы применения. В условиях цифровизации и роста объемов данных SDMX становится все более востребованным инструментом для унифицированного обмена информацией. Его использование особенно актуально в крупных компаниях и государственных структурах, работающих с большими массивами структурированных данных. Применение SDMX позволяет не только стандартизировать информационный обмен, но и облегчает процесс анализа данных, делая его более точным и надежным [4]. Внедрение SDMX в корпоративные системы будет способствовать повышению эффективности управления данными, снижению издержек на интеграцию и обеспечению соответствия нормативным требованиям.

Заключение

В условиях стремительного роста объемов данных и повышения требований к их обработке и обмену, использование формата SDMX становится важным шагом к стандартизации и оптимизации корпоративных информационных систем. В статье были рассмотрены ключевые преимущества SDMX по сравнению с форматами XML и JSON, такие как поддержка метаданных, улучшенная структурированность данных и возможность автоматизации обработки [5]. Несмотря на свою сложность в настройке и больший объем передаваемых данных, SDMX предлагает уникальные возможности для повышения эффективности информационного обмена и интеграции корпоративных систем. Внедрение SDMX требует комплексного подхода, включая адаптацию существующих систем, обучение сотрудников и решение вопросов безопасности. Однако его использование позволяет улучшить управление данными, сократить издержки на интеграцию и обеспечить соответствие нормативным требованиям, что способствует устойчивому развитию организаций в эпоху цифровизации.

Список использованных источников

1. OECD. (2021). Управление данными и стандартизация в цифровой экономике. OECD Publishing. Получено с сайта [OECD].
2. Ланге, Р., & Уддин, М. (2019). Управление данными и стандартизация в международных организациях: SDMX на практике. Springer.
3. Фицджеральд, С. (2018). Обмен данными и стандартизация: интеграция форматов данных в корпоративных системах. Wiley.
4. Перейра, С. (2020). Statistical Data and Metadata Exchange: Теория и приложения. Elsevier.
5. Лю, Дж., & Си, И. (2021). Роль SDMX в современном обмене данными и стандартизации. Springer.

References

1. OECD. (2021). Data Governance and Standardization in the Digital Economy. OECD Publishing. Retrieved from OECD.
2. Lange, R., & Uddin, M. (2019). Data Management and Standardization in International Organizations: SDMX in Practice. Springer.
3. Fitzgerald, S. (2018). Data Interchange and Standardization: Integrating Data Formats in Corporate Systems. Wiley.
4. Pereira, S. (2020). Statistical Data and Metadata Exchange: Theory and Applications. Elsevier.
5. Liu, J., & Xie, Y. (2021). The Role of SDMX in Modern Data Exchange and Standardization. Springer.

Сведения об авторах

Завалей В.А., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vladzavalej@gmail.com.
Скиба И.Г., магистр технических наук, ассистент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», i.skiba@bsuir.by.
Фурсанов С.А., инженер-программист, ОИТ ЦИИР, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.fursanov@bsuir.by.

Information about the authors

Zavalei V.A., Student of the Department of Electronic Computing Machines, Educational Institution "Belarusian State University of Informatics and Radioelectronics", vladzavalej@gmail.com.
Skiba I.G., Master of Science in Engineering, Senior Lecturer Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", i.skiba@bsuir.by.
Fursanou S.A., software engineer, Information Development Department, Center for Informatization and Innovative Developments, Educational Institution "Belarusian State University of Informatics and Radioelectronics" s.fursanov@bsuir.by.

УДК 004.001

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОЦЕССА АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ДОПОЛНИТЕЛЬНЫХ ФАКТОРОВ

С.А. Зайкова
Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Аннотация. Разработана новая многофакторная система аутентификации, где метод с использованием аудиопотоков используется в качестве второго фактора. Исследована область возможного применения, определены необходимые для поддержки клиентского приложения браузеры. Предложен алгоритм аутентификации, алгоритм сравнения двух тоновых наборов оцифрованных аудиопотоков. Спроектированы и реализованы программные средства для реализации взаимодействия между внутренними компонентами новой корпоративной системы, рассмотрены улучшенные методы защиты передаваемых данных. Основные идеи метода включают в себя: гарантию присутствия пользователя в точке входа; возможность автоматизации процесса ввода одноразового пароля для сотрудников компании. Предусмотрена интеграция с коммуникационной платформой Twilio. Тестирование успешного применения предложенного решения показало успешность и эффективность применяемого метода, как дополнительного фактора во внутреннюю систему ИТ-компании.
Ключевые слова: многофакторная аутентификация; обеспечение безопасности; программные средства; аудиопотоки; корпоративная система, точка входа, программный интерфейс.

ENSURING THE SECURITY OF THE AUTHENTICATION PROCESS USING ADDITIONAL FACTORS

S.A. Zaikova
Yanka Kupala State University of Grodno, Belarus

Abstract. A new multi-factor authentication system has been developed, where the method using audio streams is used as the second factor. The area of possible application has been investigated, the browsers required to support the client application have been identified. An authentication algorithm and an algorithm for comparing two sets of tones from digitized audio streams are proposed. Software tools have been designed and implemented to facilitate interaction between the internal components of the new corporate system, and improved methods for protecting transmitted data have been considered. The main ideas of the method include: guaranteeing the user's presence at the entry point; the ability to automate the process of entering a one-time password for company employees. Integration with the Twilio communication platform is provided. Testing the successful application of the proposed solution demonstrated the success and effectiveness of the applied method as an additional factor in the internal system of an IT company.
Keywords: multi-factor authentication; security assurance; software tools; audio streams; corporate system; entry point; software interface

Введение

В настоящее время существует множество различных систем аутентификации, включая корпоративные системы, но не каждая из них гарантирует наличие сотрудника в точке входа. Как один из способов решения данной проблемы, можно считать применение специализированных программных средств для ограничения ввода одноразового пароля, в рамках ограниченного промежутка времени [1, 2]. Следует отметить, что такие меры могут стать причиной неудачных попыток аутентификации и ситуации, когда сотрудники компании начинают игнорировать проблемный фактор, предпочитают быстрый альтернативный вариант. Наиболее пренебрежительные пользователи выбирают вход с помощью кодов восстановления. При рассмотрении других вариантов, возможно использование переносных аппаратных средств, например, для сканирования одноразового пароля в формате QR-кода. Однако, следует признать, что этот метод также не всегда удобен по нескольким причинам, и зачастую не оправдывает себя, потому что пользователь, знакомый с технологией QR-кодов, может потребовать дополнительного обучения. Поэтому современные системы аутентификации вынуждены предлагать альтернативные варианты входа для компаний и организаций.

Основная часть

Аутентификация на основе аудиопотоков решает указанную выше проблему и является удобной альтернативой, которая исключает человеческий фактор из цепочки проверки подлинности. В этом случае сотрудник компании не производит ввод одноразового пароля вручную. Этот метод аутентификации происходит быстро, достаточно лишь поднести источник звука к микрофону. Таким образом, данный метод не только обеспечивает безопасность аутентификации, но также и гарантирует присутствие сотрудника компании в точке входа, так как вероятность передачи токена пользователем посторонним либо злоумышленникам практически исключена.

Аутентификация на основе аудиопотоков может быть произведена на большом количестве устройств. Данный метод актуален в том числе, для корпоративных веб-приложений, которые используют второй фактор для аутентификации. Если руководители компаний, организаций сталкиваются с такой проблемой, как «усталость от безопасности», аутентификация на основе аудиопотоков позволит сотрудникам проходить процесс авторизации быстрее и проще. Кроме того, если программному сервису необходимо защититься от умышленной передачи пользователем реквизитов для входа, такой способ аутентификации заставит сотрудника компании находиться физически рядом с точкой логина к ресурсу, требовательному к процессам информационной безопасности. Например, в ситуации передачи доступа к критически важным данным и ресурсам посторонним лицам, находящимся удаленно физически.

Поддерживая постоянный сеанс связи, можно производить аутентификацию данным методом длительно. Например, если системе требуется гарантировать присутствие пользователя в течении продолжительного периода времени, то, изменив конфигурацию метода, аудиопоток можно не прекращать и производить аутентификацию постоянно. Это позволит осуществлять доступ только во время проигрывания аудиопотока. Целевая аудитория такого приложения должна понимать, как совершить данную аутентификацию. Если бизнес-требования ориентированы на поддержку широкого круга пользователей, данный метод может быть проблематичным, так как требует несколько активных сессий.

Спроектированная система удовлетворяет следующим требованиям: предложенное решение поддерживаться популярными браузерами. Корректно обрабатывает все этапы аутентификации. Отображает актуальный интерфейс приложения. Интегрируется с другими приложениями и системой управления компанией, предприятием. Поддерживаются GSM и WebRTC методы связи. Используемые библиотеки имеют открытый исходный код.

В процессе разработки учтено обстоятельство о том, что запись и воспроизведение аудио поддерживается большинством персональных устройств, и, таким образом, аутентификация на основе аудиопотоков должна поддерживаться большим количеством пользователей, сотрудников компании. Для передачи аудио необходимо создать аудиопоток между клиентским приложением и серверным. Если клиентское приложение запущено в системе, не поддерживающей аутентификацию на основе аудиопотоков, приложение должно корректно обрабатывать исключительные ситуации и оповещать пользователя, что аутентификация невозможна.

Клиентское приложение в системе выполняет две функции: отображает пользователю интерфейс и взаимодействует с сервером; взаимодействует с коммуникационной платформой. Коммуникационная платформа, в свою очередь, устанавливает связь с устройством пользователя для проигрывания аудиоряда в зависимости от выбранных настроек. Поведение и способ связи определяется через API платформы. Серверное приложение в предложенной схеме управляет процессом аутентификации: генерирует аудиофайл и инициализирует вызов через платформу, после чего взаимодействует через события с клиентским приложением. Ссылка на аудиофайл и идентификатор устройства пользователя используются в объекте конфигурации, передаваемом коммуникационной платформе. Во время вызова сервер обрабатывает асинхронные запросы от платформы.

На первом этапе парольного фактора логин и пароль пользователя отправляются POST запросом. Далее, сервер запрашивает из базы данных информацию о пользователе и сохраняет ее в хэш-хранилище. Взаимодействие между базой и сервером защищено SSL-шифрованием, срок действия аутентификационного токена устанавливается в зависимости от требований конкретной системы. Для всего процесса аутентификации требуется логин, пароль (парольный хэш) пользователя и его идентификаторы ранее зарегистрированных устройств. После валидации полученных реквизитов пользователя сервер отправляет ответ со статусом и списком доступных методов.

После того, как метод выбран, сервер генерирует аудиоряд с помощью набора сэмплов разных частот и функции, объединяющей их в один файл. Далее, сервер создает конфигурацию, которая состоит из: одноразовой ссылки для выгрузки аудиофайла, идентификатора устройства, инструкций, описывающих поведение платформы во время коммуникации и ссылки для обратных вызовов.

Объект с инструкциями будет передаваться коммуникационной платформе посредством POST запроса. После выгрузки аудиофайла, платформа инициирует коммуникацию со вторым устройством пользователя. Максимальную задержку после начала проигрывания аудиоряда и принятия аудиопотока и количество повторений были установлены с ограничением в двойном повторении.

В качестве коммуникационной платформы в разработанной системе выступает API-сервис Twilio, предоставляющий управление большим выбором различных методов связи. Предоставляя управление своим API через язык разметки TwiML, сервис позволяет создавать программируемые вызовы, определенные в требованиях к разработанному решению.

Заключение

Результаты проведенного исследования несут в себе практическую значимость, как один из эффективных способов, гарантирующих присутствие сотрудника в точке входа, и решают одну из проблем безопасности современных методов аутентификации. Предложенное программное решение учитывает то обстоятельство, что необходимые для аутентификации воспроизводящие и записывающие звук компоненты есть в большом количестве устройств, имеющих выход в сеть интернет. На следующем этапе проектирования и разработки модулей системы возможно использовать дополнительные программные инструменты на основе нейронных сетей, в том числе для отсеивания постороннего шума, так как набор используемых частот известен заранее.

Список использованных источников

1. Шнайдер Б. (2023) Взломать все. Москва, Издательство «Альпина паблишер».
2. Афанасьев А. А. и др. (2012) Теория и практика обеспечения безопасного доступа. Москва, Издательство «Горячая линия–Телеком».

References

1. Shnaider B (2023) Hack everything. Moscow, Alpina Publishing House (in Russian).
2. Afanasiev A. A. and oth., (2012) Theory and practice of ensuring secure access. Moscow, Hotline - Telecom Publishing House (in Russian).

Сведения об авторе

Зайкова С.А., канд. физ.-мат. наук, доц., доцент каф., УО «Гродненский государственный университет имени Янки Купалы», sunny@mf.grsu.by.

Information about the author

Zaikova S., Cand. Sci. (Phys. and Math.), Associate Professor of the Department, Yanka Kupala State University of Grodno, Republic of Belarus, sunny@mf.grsu.by.

УДК 004.056.5

ИНФОРМАЦИЯ, ПОДЛЕЖАЩАЯ ЗАЩИТЕ ОТ УТЕЧЕК СРЕДСТВАМИ DLP-СИСТЕМ

Е.С. Захарова
Институт информационных технологий БГУИР, г. Минск, Республика Беларусь

Аннотация. Информационная безопасность предприятия невозможна без построения надежной системы защиты информации. В настоящее время набирает популярность включение в систему защиты информации DLP-решений. Однако в Республике Беларусь отсутствуют научные исследования правового обеспечения внедрения и использования систем предотвращения утечки информации. Неизученным остается и вопрос о категории информации, которую целесообразно защищать от утечек с использованием DLP-систем. Динамика развития информационной сферы, законодательства о персональных данных, о коммерческой, банковской и иной тайне, появление новых вызовов и угроз информационной безопасности, включая угрозы утечки информации, позволяет сделать вывод, что эта работа должна продолжаться на высоком научном уровне.

Ключевые слова: информационная безопасность; риск; утечка информации; защита информации; общедоступная информация; информация, распространение и (или) предоставление которой ограничено; информационная система; проектирование системы защиты; система предотвращения утечки информации; DLP-система.

INFORMATION SUBJECT TO PROTECTION AGAINST LEAKS BY MEANS OF DLP SYSTEMS

H. Zakharova
Institute of Information Technologies BSUIR, Minsk city, Republic of Belarus

Abstract. Information security of an enterprise is impossible without building a reliable information security system. Currently, the inclusion of DLP solutions in the information security system is gaining popularity. However, in the Republic of Belarus there is no scientific research into the legal support for the implementation and use of information leakage prevention systems. The question of the category of information that is advisable to protect from leaks using DLP systems also remains unexplored. The dynamics of development of the information sphere, legislation on personal data, on commercial, banking and other secrets, the emergence of new challenges and threats to information security, including threats of information leakage, allows us to conclude that this work must continue at a high scientific level.
Keywords: information security; risk; information leak; information protection; public information; information, the distribution and (or) provision of which is limited; information system; design of a protection system; information leakage prevention system; DLP system.

Введение

Объемы информации, обрабатываемые и хранимые предприятиями и организациями в своих информационных ресурсах, зачастую не позволяют адекватным образом ее контролировать и защищать. При этом многие руководители оказываются не готовыми к внутренним угрозам, возникающим из-за утечки информации, вызванной действиями работников. Поэтому вопросы предотвращения утечек информации стоят сейчас особенно остро.

Одним из самых надежных способов защиты информации от внутренних угроз является установка систем предотвращения утечки информации (DLP – Data Leak Prevention – в дословном переводе «предотвращение утечки данных» [1, с. 37]).

Следует отметить, что в настоящее время отсутствуют нормативные правовые акты, закрепляющие требования к порядку и условиям внедрения и использования на предприятиях и в организациях Республики Беларусь систем предотвращения утечки информации. Законодательно не определена категория информации, для защиты которой могут быть использованы рассматриваемые системы. Не определены гарантии соблюдения прав работников предприятий, организаций, использующих в своей работе системы предотвращения утечки информации. Несмотря на это DLP-системы широко применяются на практике банками, предприятиями оборонного комплекса, предприятиями, имеющими коммерческие секреты [2, с. 57].

На основании изложенного представляется необходимым четко определить категорию информации, для защиты которой действующее законодательство предусматривает возможность применения систем предотвращения утечки информации.

Основная часть

В различных источниках авторы подчеркивают высокий уровень защиты DLP-системами от утечек «конфиденциальной информации» [1, с. 37; 3, с. 59, 61; 4, с. 4]. Отдельные авторы используют понятие «корпоративная информация» [5, с. 57].

Однако в Государственном стандарте Республики Беларусь «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования. СТБ 34.101.76-2017» используется термин «защищаемая информация», к которой

относится «информация, распространение и (или) предоставление которой ограничено Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» и иными законодательными актами Республики Беларусь, а также неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу» (п. 3.6).

Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (далее - Закон) в статье 15 в зависимости от категории доступа выделяет:

1. Общедоступную информацию;

2. Информацию, распространение и (или) предоставление которой ограничено.

Общедоступной является информация, доступ к которой, распространение и (или) предоставление которой не ограничены (ч. 1 ст. 16 Закона).

Распространение общедоступной информации не предполагает активных действий по доведению информации до как можно большего числа получателей. Достаточно обеспечить возможность любым лицам получить к ней доступ. Это можно сделать, например, разложив печатные материалы в общедоступном, публичном месте или предоставив информацию на интернет-сайте с возможностью для любого абонента найти ее в сети через поисковую систему [6, с. 177].

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней (ч. 2 ст. 28 Закона). Таким образом, действующее законодательство не предусматривает защиту общедоступной информации от утечек. Следовательно, применение систем предотвращения утечки информации при использовании в работе предприятий и организаций Республики Беларусь общедоступной информации, не требуется.

Ко второй категории – информации, распространение и (или) предоставление которой ограничено, Закон относит:

– информацию о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебную информацию ограниченного распространения;

– информацию, составляющую коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информацию, содержащуюся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иную информацию, доступ к которой ограничен законодательными актами (ч. 1 ст. 17 Закона).

Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством (ч. 3 ст. 28 Закона).

Положение о порядке государственной регистрации информационных ресурсов и ведения Государственного регистра информационных ресурсов, утвержденное Постановлением Совета Министров Республики Беларусь от 26.05.2009 № 673, предписывает при использовании государственных информационных систем реализовывать меры по защите информации в соответствии с законодательством о защите информации (абз. 8 п. 6).

Так, Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки

информации, распространение и (или) предоставление которой ограничено, утвержденным Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Положение), предусмотрено на этапе проектирования системы защиты информации составление технического задания, которое должно содержать требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем (п. 8, абз. 3 ч. 2 п. 10 Положения).

Информационные системы, в которых обрабатывается информация, распространение и (или) предоставление которой ограничено, могут быть отнесены к классам:

– 3-ин – если в них обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

– 3-спец – если в них обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

– 3-юл – если в них обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных (п.п. 6, 7, 9 Приложение 1 «Классы типовых информационных систем» к Положению).

Согласно п. 7.15. Приложения 3 к Положению, использование системы обнаружения утечек информации из информационных систем, отнесенных к классам 3-ин, 3-спец и 3-юл, является рекомендуемым, то есть не обязательным.

И только в отношении информационных систем, содержащих служебную информацию ограниченного распространения и которые подключены к открытым каналам передачи данных, отнесенных к классу 3-дсп (п. 10 Приложения 1 «Классы типовых информационных систем» к Положению) должны использоваться системы обнаружения утечек информации.

Заключение

В результате проведенного исследования действующего законодательства в сфере защиты информации можно сделать следующие выводы:

1. Многообразие дефиниций информации, защищаемой DLP-системами, слабая определенность используемого в различных научных и научно-популярных источниках понятийного аппарата, использование терминов «конфиденциальная информация», «корпоративная информация» для целей конкретной научной работы является актуальной проблемой на протяжении многих лет. Все это может привести к неправомерному использованию систем обнаружения утечек информации в отношении общедоступной информации.

2. Использование DLP-систем допускается в государственных информационных системах и информационных системах, в которых обрабатывается информация, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения).

3. Использование систем обнаружения утечек информации является обязательным для защиты служебной информации ограниченного распространения.

Список использованных источников

1. Станкевич, В. DLP: белорусский опыт / В. Станкевич // IT Бел : технологии автоматизации бизнеса : научно-практический журнал / учредитель частное производственное унитарное предприятие «Редакция журнала «IT Бел». – 2011. – № 1/2. – С. 37-39.
2. Никифоров, С.Н. Проблематика внедрения DLP систем в Республике Беларусь / С. Н. Никифоров // Технологии безопасности. – 2012. – № 3. – С. 57.
3. Барановский, А.В. Обзор систем противодействия утечкам информации. DLP системы в Беларуси / А.В. Барановский // Технологии безопасности. – 2012. – № 3. – С. 58-63.
4. Система противодействия утечке данных «Контур информационной безопасности Searchinform» : пособие / Т.В. Бороботько [и др.]. – Минск : БГУИР, 2021. – 284 с.
5. Акимов, А.И. DLP в Беларуси: пять вопросов, требующих ответов / А.И. Акимов // Технологии безопасности. – 2012. – № 3. – С. 56-57.
6. Саперов, С.А. Информация как объект правоотношений: монография / С.А. Саперов. – М.: Юстицинформ, 2023. – 704 с.

References

1. Stankevich, V. DLP: Belarusian experience / V. Stankevich // IT Bel: business automation technologies: scientific and practical journal / founder of the private production unitary enterprise "Editing Office of the magazine "IT Bel". – 2011. – № 1/2. – C. 37-39.
2. Nikiforov, S.N. Problems of implementing DLP systems in the Republic of Belarus / S.N. Nikiforov // Security technologies. – 2012. – № 3. – C. 57.
3. Baranovsky, A.V. Review of systems to combat information leaks. DLP systems in Belarus / A. V. Baranovsky // Security Technologies. – 2012. – № 3. – C. 58-63.
4. System for combating data leakage "Searchinform Information Security Circuit": manual / T. V. Borobotko [and others]. – Minsk: BSUIR, 2021. – 284 c.
5. Akimov, A.I. DLP in Belarus: five questions that require answers / A.I. Akimov // Security technologies. – 2012. – № 3. – C. 56-57
6. Saperov, S.A. Information as an object of legal relations: monograph / S.A. Saperov. – M.: Justitsinform, 2023. – 704 c.

Сведения об авторе

Захарова Е.С., слушатель Института информационных технологий БГУИР, zaharova@info-center.by.

Information about the author

Zakharova H., student of the Institute of Information Technologies BSUIR, zaharova@info-center.by.

УДК 616-71

К ВОПРОСУ ЗАЩИТЫ ДАННЫХ В БИОТЕХНИЧЕСКИХ СИСТЕМАХ МЕДИЦИНСКОГО НАЗНАЧЕНИЯ

О.Б. Зельманский, С.Н. Петров, Д.А. Фомин
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» Минск, Беларусь

Аннотация. Цифровизация системы здравоохранения в Республике Беларусь предусматривает интеграцию синтезируемых биотехнических систем медицинского назначения в медицинскую информационную сеть. Стандарт обмена, управления и интеграции электронной медицинской информации HL7 может применяться для организации процессов обработки, передачи и хранения медицинских данных. При этом актуальной задачей остается обеспечение безопасности медицинских данных, передаваемых биотехническими системами в медицинскую информационную сеть. Настоящая работа содержит описание разработанного веб-приложения, в котором реализована передача информации в формате HL7 сообщений. Для решения вопроса обеспечения защиты информации, передаваемой посредствам HL7 сообщений, проанализированы такие алгоритмы шифрования, как Mars, AES (Rijndel), Twofish, а также их RSA надстройки. С целью обеспечения защиты медицинской

информации обосновано применения в биотехнических системах медицинского назначения алгоритма шифрования Twofish.
Ключевые слова: синтез биотехнических систем; разработка медицинского оборудования; безопасность данных пациентов; защита медицинских данных; HL7 сообщение; цифровизация здравоохранения; eHealth.

TO THE ISSUE OF DATA PROTECTION IN MEDICAL PURPOSE BIOTECHNICAL SYSTEMS

O.B. Zelmanski, S.N. Petrov, D.A. Fomin
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Digitalization of the healthcare system in the Republic of Belarus involves the integration of synthesized biotechnical systems for medical purposes into the medical information network. The standard for the exchange, management and integration of electronic medical information HL7 can be used to organize the processes of processing, transfer and storage of medical data. At the same time, ensuring the security of medical data transmitted by biotechnical systems to the medical information network remains an urgent task. This work contains a description of the developed web application, which implements the transfer of information in the HL7 message format. To solve the issue of ensuring the protection of information transmitted via HL7 messages, such encryption algorithms as Mars, AES (Rijndel), Twofish, as well as their RSA add-ons are analyzed. In order to ensure the protection of medical information, the use of the Twofish encryption algorithm in biotechnical systems for medical purposes is justified.
Keywords: synthesis of biotechnical systems; development of medical equipment; patient data security; protection of medical data; HL7 message; digitalization of healthcare; eHealth.

Введение

В современном информационном обществе цифровизация становится ключевым элементом эффективного функционирования различных областей, включая систему здравоохранения [1]. Республика Беларусь, как одна из стран, активно внедряющих инновационные технологии в сферу здравоохранения, стремится обеспечить высокий уровень медицинского обслуживания и улучшить качество жизни своих граждан. Цифровизация системы здравоохранения в Республике Беларусь – это комплексный процесс, охватывающий внедрение современных информационных технологий для оптимизации медицинских процессов, повышения доступности медицинской помощи и обеспечения безопасности данных пациента. На фоне активных изменений в сфере здравоохранения Республики Беларуси, цифровые технологии становятся неотъемлемой частью системы обеспечения качественных и эффективных медицинских услуг. Таким образом, при разработке медицинских устройств и систем необходимо уделять особое внимание возможности их интеграции в медицинскую информационную сеть посредствам современных коммуникационных технологий, решая при этом задачу обеспечения защиты передаваемых медицинских данных, в том числе персональных.

Стандарт передачи медицинских данных HL7

Одной из актуальных задач в рамках цифровизации здравоохранения является стандартизация процессов обработки, передачи и хранения медицинских данных. Для ее решения международным сообществом по вопросам информатизации здравоохранения Health Level Seven International предложен стандарт HL7 (Health Level Seven), к которому в 2018 году присоединилась Республика Беларусь. Данные в стандарте HL7 организованы в логические блоки, называемые сегментами. Каждый сегмент представляет собой набор полей, которые содержат конкретные элементы информации,

такие как имя пациента, дата рождения и другие медицинские данные. Сегменты объединяются в группы, называемые сообщениями. Группы сегментов образуют структуру сообщений, представляющую собой логически связанный набор данных. Для обработки информации в формате HL7 предлагается протокол MLP (Medical Link Protocol), который предусматривает преобразование информации из HL7 в DICOM (Digital Imaging and Communications in Medicine), являющийся протоколом взаимодействия с медицинским оборудованием. Протокол MLP представляет собой стандарт, разработанный для обмена медицинскими данными между различными системами и приложениями в области здравоохранения. Он обеспечивает эффективный способ передачи информации о пациентах и клинических данных, способствуя интеграции и взаимодействию между различными участниками системы здравоохранения. Использование стандарта HL7 в здравоохранении предоставляет множество преимуществ, но в то же время имеет проблему обеспечения безопасности медицинских данных [2], поскольку он не предоставляет встроенных функций безопасности. Наиболее очевидные угрозы безопасности HL7 аналогичны Telnet и FTP. Это открытый текст, отсутствие аутентификации, отсутствие проверки и необязательность подтверждений [3]. Решение этой проблемы может быть основано на использовании алгоритмов шифрования [4, 5]. Одним из основных требований, которые должны предъявляться к алгоритмам шифрования информации, обрабатываемой в синтезируемых биотехнических системах, является высокая производительность.

Обоснование выбора алгоритма шифрования медицинских данных

С целью реализации обмена информацией по стандарту HL7 на языке программирования «Java Script» было разработано веб-приложение, использующее библиотеку SMART on FHIR JavaScript и реализующее взаимодействие с открытым тестовым медицинским сервером FHIR REST API server. В приложении реализована аутентификация пользователя и доступ к базе электронных медицинских карт пациентов. SMART on FHIR использует протокол OAuth 2.0 для аутентификации и авторизации. Библиотека предоставляет готовые методы для получения токенов доступа, что позволяет безопасно взаимодействовать с защищенными ресурсами. Библиотека предлагает удобные функции для выполнения запросов к API FHIR, включая создание, чтение, обновление и удаление ресурсов. Библиотека совместима с различными веб-платформами и может использоваться как в клиентских, так и в серверных приложениях. Это делает ее универсальным инструментом для разработчиков. С целью выбора алгоритма шифрования медицинских данных на основе результатов исследования, проведенных институтом NIST [4], в качестве объектов исследования были выбраны следующие алгоритмы шифрования данных: Mars, AES (Rijndel), Twofish, а также их RSA надстройки [6]. В процессе проведения исследований было выполнено более 11 000 экспериментов. Суть исследования состояла в оценке скорости шифрования данных различных форматов (*.doc, *.pdf, *.rar, *.ova, *.win, *.bak), различного размера (1 МБ, 5 МБ, 20 МБ, 100 МБ, 500 МБ, 2 ГБ, 5 ГБ, 20 ГБ), на различных аппаратных платформах. В результате установлено, что для защиты информации, передаваемой посредствам HL7 сообщений, целесообразно использовать алгоритм шифрования Twofish.

Заключение

На основе результатов проведенных исследований можно заключить, что в разрабатываемых биотехнических системах наиболее целесообразно использовать

алгоритм шифрования Twofish для защиты информации, передаваемой посредствам HL7 сообщений. Это обусловлено тем, что процесс шифрования как малых, так и больших массивов данных с использованием этого алгоритма характеризуется более высоким быстродействие по сравнению с процессами шифрования массивов данных с использованием других алгоритмов, рекомендуемых в настоящее время NIST.

Список использованных источников

1. Пономарев А.А. Использование Open XML для формирования клинических документов в формате HL7 CDA / А.А. Пономарев, Тап Ван Фам // Экономика, Статистика и Информатика. – 2010. – № 3. – С. 147–152.

2. Магомедов Ш.Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения / Ш. Г. Магомедов // Cloud of Science. – 2020. – № 7(3). – С. 685–704.

3. Даллас Хазелхорст, Взлом интерфейсов данных HL7 в медицинских средах: атака и защита – ахиллесова пята здравоохранения [Электронный ресурс]. – Режим доступа: https://linuxincluded.com/hl7-medical-attacking-defending/: 24.02.2025.

4. Рябко Б.Я., Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая Линия - Телеком, 2018. – 302 с.

5. Хан А.А. Специальный выпуск по информационной безопасности и криптографии: роль передовых цифровых технологий / А. А. Хан, Л. Й. Пор // Прикладные науки. – 2024. – № 14(5), 2045.

6. Баскаков И.В. Защита информации в информационных системах : учебное пособие / И.В. Баскаков, В.Л. Евсеев, А.В. Пролетарский, А.М. Суровов. – Москва : Рудомино, 2011. – 362 с.

References

1. Ponomarev, A. A. Using open xml in order to implement the electronic documents in the clinical format hl7 CDA / A. A. Ponomarev, Tap Van Pham // Economy, Statistics and informatics. – 2010. – № 3. – P. 147–152.

2. Magomedov, S. G. Security Analysis of Computer Networks and Applications of the Healthcare Organizations Information Processes / S. G. Magomedov // Cloud of Science. – 2020. – № 7(3). – P. 685–704.

3. Dallas Haselhorst, Hacking HL7 Data Interfaces in Medical Environments: Attacking and Defending the Achille's Heel of Healthcare [Electronic resource]. – Access mode: https://linuxincluded.com/hl7-medical-attacking-defending/: 24.02.2025.

4. Ryabko, B.Y. Cryptography in the information world / B.Y. Ryabko, A.N. Fionov. – M.: Hot Line - Telecom, 2018. – 302 p.

5. Khan, A. A. Special issue on information security and cryptography: the role of advanced digital technology / A. A. Khan, L. Y. Por // Applied Sciences. – 2024. – № 14 (5), 2045.

6. Baskakov, I.V. Information protection in information systems / I.V. Baskakov, V.L. Evseev, A.V. Proletarsky, A.M. Surovov. – Moscow : Rudomino, 2011. – 361 p.

Сведения об авторах

Зельманский О.Б., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», 7650772@rambler.ru.
Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.
Фомин Д.А., магистрант каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», d.fomin@bsuir.by.

Information about the authors

Zelmanski O.B., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", 7650772@rambler.ru
Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by
Fomin D.A., Master student of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", d.fomin@bsuir.by.

УДК 004.272, 004.31

РЕАЛИЗАЦИЯ НА FPGA КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С БОЛЬШИМ КОЛИЧЕСТВОМ ИТЕРАЦИЙ

М.В. Качинский, А.В.Станкевич, А.И.Шемаров
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются возможные архитектурные решения реализации на базе FPGA криптографических алгоритмов с большим количеством итераций однотипных вычислений, обеспечивающие высокую производительность при обработке блоков входных данных. Проведен анализ производительности. Обосновывается выбор для таких реализаций параллельно-итеративной или конвейерно-итеративной архитектуры разрабатываемых специализированных процессоров. Количество ступеней конвейера, количество параллельных подсистем предлагается выбирать, исходя из параметров криптографического алгоритма, ограничений аппаратных ресурсов конкретного кристалла FPGA, а также возможности размещения в кристалл и трассировки соединений итогового проекта полученного специализированного процессора используемыми инструментальными средствами проектирования. Даются рекомендации по выбору архитектуры.
Ключевые слова: реализация на FPGA; криптографический алгоритм; итерация; блок данных; итеративная, параллельная, конвейерная архитектура процессора; ступень конвейера; аппаратные ресурсы кристалла FPGA; производительность.

FPGA IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS WITH A LARGE NUMBER OF ITERATIONS

M.V. Kachinsky, A.V. Stankevich, A.I. Shemarov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article analyzes the usage of architectural solutions for FPGA implementations of cryptographic algorithms, with a significant number iterations of uniform calculations that provide high performance in processing of input data blocks. A performance analysis was performed. The choice of parallel-iterative or pipeline-iterative architecture for specialized processors is substantiated by the evidence. The number of pipeline stages and the number of parallel subsystems are to be chosen based on the parameters of the cryptographic algorithm and the limitations of hardware resources of a particular FPGA device, as well as the possibility of place and route of the final project of specialized processor. Recommendations are provided for the optimal selection of architectural design.
Keywords: FPGA implementation; cryptographic algorithm; iteration; data block; iterative, parallel and pipelined processor architecture; pipeline stage; FPGA hardware resources utilization; performance.

Введение

В настоящее время в задачах обеспечения конфиденциальности, целостности данных и аутентификации широко используются различные криптографические алгоритмы, с помощью которых обрабатывается некоторая последовательность блоков данных. При этом криптографический алгоритм может иметь большое количество итераций однотипных вычислений. В качестве примера можно рассмотреть задачу хэширования блока входных сообщений одинаковой длины алгоритмами SHA-1 (RFC3174) или семейства SHA-2 (RFC6234). В этом случае каждое входное сообщение разбивается на блоки, размер которых определяется алгоритмом, и далее эти блоки последовательно обрабатываются вычислительным ядром алгоритма SHA столько раз, сколько имеется этих входных блоков одного сообщения. При этом сам алгоритм SHA имеет некоторое фиксированное количество однотипных итераций (раундов). Другим примером является использование алгоритмов формирования ключа на основе пароля для блока паролей. В алгоритмах PBKDF2

(RFC2898) и Argon2 [1] имеется параметр, задающий количество итераций алгоритма верхнего уровня итерации. При этом алгоритмы, использующиеся на более низких уровнях иерархии, также имеют свое определенное количество итераций.

Если требуется высокопроизводительная реализация таких алгоритмов, то необходимо использовать аппаратную реализацию. Одним из таких возможных вариантов является реализация на базе FPGA (Field Programmable Gate Array). При реализации на конкретном кристалле FPGA разработчик имеет ограничение по имеющимся аппаратным ресурсам. Рассмотрим возможные варианты архитектурных решений таких реализаций с учетом этого ограничения и оценим возможную производительность таких решений.

Основная часть

В качестве базового блока архитектуры специализированного процессора будем рассматривать процессор одной итерации алгоритма. Этот процессор реализует одну базовую совокупность повторяющихся операций алгоритма и содержит комбинационную схему для реализации требуемых вычислений, а также выходной регистр для фиксации результата итерации. Например, для алгоритмов семейства SHA-2 в качестве такого процессора можно рассматривать устройство, реализующее один раунд алгоритма. Сравним возможные реализации.

На рис. 1 приведена параллельно-итеративная реализация криптографического алгоритма с итерациями.

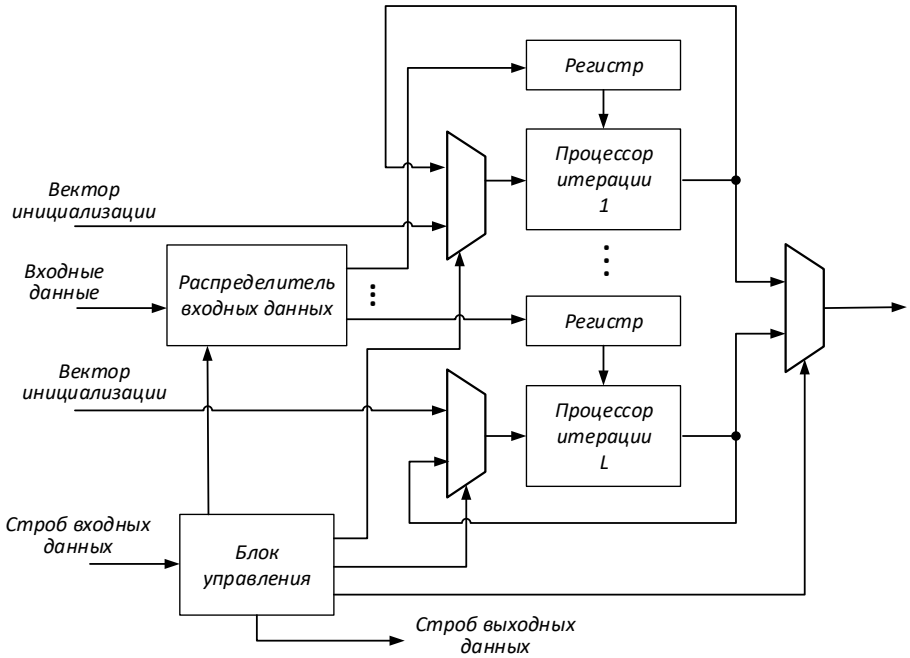


Рис. 1. Параллельно-итеративная архитектура
Fig. 1. Parallel-iterative architecture

Одно процессорное ядро такой архитектуры будет включать процессор одной итерации, регистр входных данных алгоритма и мультиплексор данных итерации. Этот мультиплексор обеспечивает передачу в процессор итерации вектора инициализации алгоритма (на первой итерации), либо промежуточного значения после текущей итерации. По завершении N итераций, определяемых соответствующим алгоритмом, на выходе процессора итераций будет получено требуемое значение алгоритма. При наличии в алгоритме каких-то однократных вычислений они могут быть

выполнены последовательно до или после рассмотренного процессорного ядра. Подсчет числа итераций организуется счетчиком блока управления.

Предположим, что вычисления одной итерации выполняются за один такт частоты синхронизации. В этом случае на каждое следующее процессорное ядро (рис. 1) входные данные должны подаваться со сдвигом на такт. Общий размер обрабатываемого блока данных равен L слов, что соответствует числу процессорных ядер. Порядок подачи входных данных на итеративные процессорные ядра обеспечивает распределитель входных данных. Данные вычислительных ядер объединяются в общий выходной поток с помощью выходного мультиплексора. Число процессорных ядер L зависит от имеющихся ресурсов кристалла FPGA. В простейшем случае при $L = 1$ распределитель данных и выходной мультиплексор не нужны. Время получения полного блока результата для параллельно-итеративной архитектуры равно $N + L - 1$ тактов (без учета такта на прием входных данных в регистр).

На рис. 2 приведена итеративно-конвейерная реализация криптографического алгоритма с итерациями.

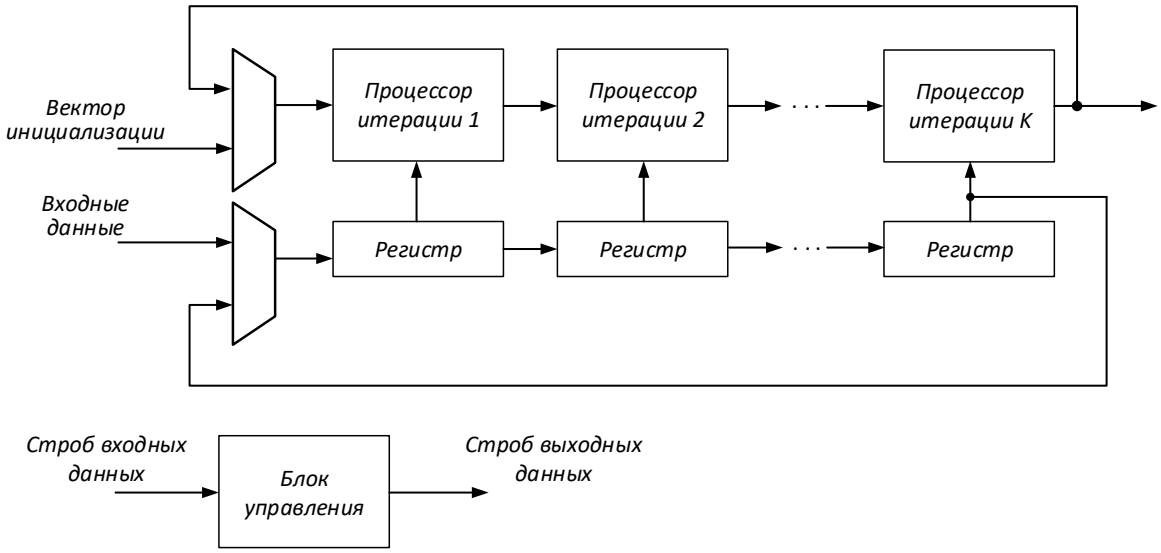


Рис. 2. Конвейерно-итеративная архитектура
Fig. 2. Pipeline-iterative architecture

Конвейерная архитектура реализует концепцию проектирования, заключающуюся в развертывании повторяющихся вычислений (unrolling the loop) [2]. В этом случае каждая из повторяющихся операций выполняется последовательно на своем процессоре, после чего полученный результат передается на процессор следующей итерации. В случае, если данные каждой итерации связаны с входными данными первой итерации (например, как в алгоритмах SHA), то параллельно с конвейером вычислительных итераций должен быть организован конвейер данных, который обеспечивает подачу правильных данных для соответствующей ступени конвейера вычислительных итераций (рис. 2).

В случае, если логической емкости кристалла FPGA достаточно для реализации всех N итераций алгоритма, то никакой обратной связи и входного мультиплексора, показанных на рис. 2 не требуется. Если логическая емкость кристалла позволяет разместить для повышения производительности несколько параллельно работающих конвейеров, то можно реализовать решение, подобное рис. 1, где вместо итеративных процессорных ядер будут использоваться параллельно работающие конвейеры.

В случае, если все итерации алгоритма для конвейерной архитектуры не могут быть размещены в кристалле FPGA, то можно реализовать только K из общего числа N

итераций ($K < N$) и полученные после K итераций результаты вычислений с помощью мультиплексора подать на вход первого процессора итераций для продолжения вычислений (рис. 2).

В конвейерно-итеративной архитектуре для удобства и упрощения аппаратной реализации N должно быть кратным числа K, то есть $N = i \times K$, где i – целое число. Размер блока входных данных, загружаемых в конвейер, состоит из K слов. По истечении K тактов (предполагается что одна итерация выполняется за такт) на выходе конвейера появится выходное значение для первого входного слова блока данных после выполнения K итераций. Для получения N итераций выходные данные надо мультиплексировать из K-ой ступени конвейера обратно на вход и пропустить через конвейер этот модифицированный блок промежуточных значений еще $i - 1$ раз.

Время получения полного блока результата для конвейерно-итеративной архитектуры равно $iK + K - 1 = N + K - 1$ тактов. Если L для параллельно-итеративной архитектуры выбрать равным K, то по производительности эти архитектуры будут соответствовать друг другу.

С точки зрения аппаратных затрат предпочтительнее итеративно-конвейерная архитектура, поскольку в ней будет отсутствовать выходной мультиплексор, схема распределения входных данных, вместо L мультиплексоров обратной связи будут только два, проще будет блок управления, поскольку будет необходимо только формирование выходного строба данных. Уменьшение аппаратных затрат создаст лучшие условия для размещения и трассировки проекта в кристалл FPGA, что потенциально может привести к более высокой тактовой частоте полученного проекта, и, следовательно, к более высокой производительности.

Заключение

При реализации на FPGA криптографических алгоритмов с большим количеством итераций могут использоваться различные варианты параллельно-итеративной и конвейерно-итеративной архитектур в зависимости от требуемой производительности и логической емкости используемого кристалла FPGA. Для получения высокой производительности целесообразнее использовать конвейерно-итеративную архитектуру, которая имеет меньшие аппаратные затраты по сравнению с параллельно-итеративной и позволяет создать лучшие условия для последующего размещения и трассировки проекта в кристалл FPGA.

Список использованных источников / References

1. Alex Biryukov, Daniel Dinu, Dmitry Khovratovich. (2016) Argon2: new generation of memory-hard functions for password hashing and other applications. *IEEE European Symposium on Security and Privacy (EuroS&P). IEEE.* 292-302.

2. Kilts S. (2007) Advanced FPGA design: Architecture, Implementation, and Optimization. USA, John Wiley & Sons, Inc.

Сведения об авторах

Качинский М.В., канд. техн. наук, доц., доцент кафедры электронных вычислительных средств, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kachinsky@bsuir.by.
Станкевич А.В., канд. техн. наук, доц., доцент кафедры электронных вычислительных средств, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stankevich@bsuir.by.
Шемаров А.И., канд. техн. наук, доц., доцент кафедры электронных вычислительных средств, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», shemarov@bsuir.by.

Information about the authors

Kachinsky M., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail: kachinsky@bsuir.by.
Stankevich A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail:stankevich@bsuir.by.
Shemarov A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail:shemarov@bsuir.by.

УДК 519.92

ДИСПЕРСИЯ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ОШИБКИ ПРИ НАБЛЮДЕНИИ ВЕКТОРОВ ПЕРЕХОДОВ

И.П. Кобяк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В работе исследован метод идентификации последовательностей случайных событий с помощью оценок наблюдения векторов переходов заданного вида. Рассмотрена дисперсия плотности распределения вероятностей ошибки, требуемая для задач сравнения статистических показателей предлагаемого и известных алгоритмов свертки. Основой для расчетов послужила производящая функция, позволяющая представить произведение комбинаторных моментов, характеризующих вероятности пропуска ошибки, в виде суммы произведений статистик на соответствующие моменты. Полученные в работе соотношения характеризуют метод наблюдения векторов переходов как наиболее эффективный алгоритм формирования оценок для идентификации сообщений со случайной или псевдослучайной природой.
Ключевые слова: сложные вероятностные события; дисперсия; идентификация последовательностей; вероятность пропуска ошибки; сигнатурный анализ; производящая функция.

THE VARIANCE OF THE ERROR PROBABILITY DISTRIBUTION WHEN OBSERVING TRANSITION VECTORS

I.P. Kobiak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Annotation. The paper investigates a method for identifying sequences of random events using estimates of the observation of transition vectors of a given type. The variance of the error probability distribution density required for the task of comparing statistical indicators of the proposed and known convolution algorithms is considered. The basis for the calculations was the generating function, which makes it possible to represent the product of combinatorial moments characterizing the probability of missing an error in the form of the sum of the products of statistics for the corresponding moments. The relations obtained in the work characterize the method of observing transition vectors as the most effective algorithm for generating estimates for identifying messages with a random or pseudorandom nature.
Keywords: complex probabilistic events; variance; sequence identification; probability of missing an error; signature analysis; generating function.

Введение

Шифрование сообщений с помощью шумоподобных последовательностей ставит под вопрос задачу обнаружения детерминизма в наблюдаемых каналах связи. При этом проблема обнаружения самих каналов оказывается весьма трудоемкой даже для самых современных компьютеров.

Классический поиск сообщений циркулирующих в криптосетях, как правило, осуществляется с помощью теоретических и эвристических алгоритмов анализа. Соответственно к теоретическим относят математические методы, основанные на решении задач, на основе теории вероятностей, а к эвристическим - методы свертки по модулю два и другие аппаратные или программно-аппаратные подходы. Недостатком всех известных теоретических алгоритмов является факт равенства единице нормированной интегральной суммы моментов под кривой функции распределения вероятностей пропуска ошибки.

На сегодняшний день одним из самых современных методов обнаружения детерминизма в *r*-разрядных случайных процессах следует считать методологию наблюдения событий на основе двух и более элементарных векторов [1]. При этом вероятность пропуска ошибки статистикой сложных событий оказывается существенно ниже, чем при регистрации элементарных событий.

В целом, вопросы, связанные с применением новых методов, таких, например, как наблюдение векторов переходов заданного вида (ВПЗВ), требуют детального анализа известных параметров, а именно: математического ожидания и дисперсии производящей функции (ПФ) или энумератора для заданного числа переменных. Соответственно в представляемой работе рассмотрена дисперсия распределения вероятностей пропуска ошибки при наблюдении ВПЗВ, используемая как база для определения свойств оценок данного параметра.

Дисперсия распределения вероятностей ошибки

Для определения дисперсии распределения вероятностей пропуска ошибки при наблюдении ВПЗВ используем классическое соотношение вида:

$$D_{ifc} = P''_{ifc} - \left(P'_{ifc}\right)^2, \tag{1}$$

где *ifc* – функция корреляции, P_{ifc} – перечисляющая ПФ [1] для вероятностей пропуска ошибки при наблюдении ВПЗВ, соответственно P'_{ifc}, P''_{ifc} две производные ПФ.

Первая производная вероятности в функции (1) равна:

$$P'_{ifc} = \sum_{g} \pi(g)(n-g)\left[\sum_{j=1}^{0,5(n-5)} \xi_j k_{j,1} p^j e^{jt} x_j^1 + \sum_{j=1}^{0,5(n-5)} \xi_j \sum_{i=2}^{n-2j-2} k_{j,i} p^j e^{jt} x_j^i \frac{1}{2^{i+1}} \beta_{j,i} + \right.$$

$$\left. + \sum_{j=1}^{0,5(n-3)} \xi_j k_{j,n-2j} p^j e^{jt} x_j^{n-2j} \frac{1}{2^{n-2j+1}} \beta_{j,n-2j} + \xi_{0,5(n-1)} k_{\frac{n-1}{2},1} p^{\frac{n-1}{2}} e^{\frac{n-1}{2}t} x_{\frac{n-1}{2}}^1 \right]^{n-g-1} \times \tag{2}$$

$$\times \left[\sum_{j=1}^{0,5(n-5)} \xi_j k_{j,1} p^j \left(\frac{\partial}{\partial t} e^{jt}\right) x_j^1 + \sum_{j=1}^{0,5(n-5)} \xi_j \sum_{i=2}^{n-2j-2} k_{j,i} p^j \left(\frac{\partial}{\partial t} e^{jt}\right) x_j^i \frac{1}{2^{i+1}} \beta_{j,i} + \right.$$

$$+\sum_{j=1}^{0,5(n-3)}\xi_j k_{j,n-2j}p^j\left(\frac{\partial}{\partial t}e^{jt}\right)x_j^{n-2j}\frac{1}{2^{n-2j+1}}\beta_{j,n-2j}+\xi_{0,5(n-1)}k_{\frac{n-1}{2},1}p^{\frac{n-1}{2}}\left(\frac{\partial}{\partial t}e^{\frac{n-1}{2}t}\right)x_{\frac{n-1}{2}}^1\Bigg]^{n-g-1}.$$

Практическое моделирование данной задачи показало, что ВПЗВ с параметром $j = 3$ встречаются достаточно редко, а параметр $j = 4$, например, при $r = 8$ отсутствует в течение весьма длительного времени наблюдения. Следовательно, для верхней границы вероятности p требуемые множители ξ_1, ξ_2, ξ_3 в (2) могут быть определены в соответствии с равенствами:

$$\xi_1 = \frac{1}{1{,}146}\left(1-\frac{3}{16}\right),\quad \xi_2 = \frac{1}{1{,}146}\cdot\frac{3}{16},\quad \xi_3 = \frac{0{,}146}{1{,}146}.$$

Подставляя данные значения в многочлен (2) получаем:

$$P'_{ifc} \approx n\left[\frac{33}{8}\left(\xi_1 p+\xi_2 p^2+\xi_3 p^3\right)\right]^{n-1}\left[\frac{33}{8}\left(\xi_1 p+2\xi_2 p^2+3\xi_3 p^3\right)\right] = 0{,}606n\left(0{,}576\right)^{n-1}. \quad (3)$$

Повторное дифференцирование равенства (2), с использованием вспомогательного параметра e^t ПФ, приводит к соотношению:

$$P''_{ifc} = \sum_g \pi(g)(n-g)(n-g-1)\left(k_{1,1}pe^t x_1^1+\sum_{i=2}^{n-4}k_{1,i}pe^t x_1^i\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n-2}pe^t x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right)^{n-g-2}\times$$

$$\times\left(k_{1,1}pe^t x_1^1+\sum_{i=2}^{n-4}k_{1,i}pe^t x_1^i\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n-2}pe^t x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right)^2+$$

$$+\sum_g \pi(g)(n-g)\left(k_{1,1}pe^t x_1^1+\sum_{i=2}^{n-4}k_{1,i}pe^t x_1^i\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n-2}pe^t x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right)^{n-g-1}.$$

При $t=0, x_1^i=1$ и $\pi(g)=1$ полученное равенство приводится к виду:

$$P''_{ifc} = n(n-1)\left(k_{1,1}p+\sum_{i=2}^{n_1-4}k_{1,i}p\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n_1-2}p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right)^{n-2}\times \quad (4)$$

$$\times\left[k_{1,1}p+\sum_{i=2}^{n_1-4}k_{1,i}p\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n_1-2}p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right]^2+n\left(k_{1,1}p+\sum_{i=2}^{n_1-4}k_{1,i}p\frac{1}{2^{i+1}}\beta_{1,i}+k_{1,n_1-2}p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right)^{n-1}.$$

Формирование суммы моментов в функции (4) выполним с учетом $k_{1,i}=1$ определив вспомогательную статистику $n_1 >> 1$ при $n \ge n_1$. Тогда:

$$P''_{ifc} = n(n-1)\left(p+\sum_{i=2}^{n_1-4}p\frac{1}{2^{i+1}}\beta_{1,i}+p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right)^{n-2}\times$$

$$\times\left(p+\sum_{i=2}^{n_1-4}p\frac{1}{2^{i+1}}\beta_{1,i}+p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right)^2+n\left(p+\sum_{i=2}^{n_1-4}p\frac{1}{2^{i+1}}\beta_{1,i}+p\frac{1}{2^{n_1-1}}\beta_{1,n_1-2}\right)^{n-1}.$$

С учетом результатов работы [2] то есть для максимального значения p можем записать:

$$P''_{ifc} = n(n-1)\left(p\frac{33}{8}\right)^{n-2}\left(p\frac{33}{8}\right)^{2} + n\left(p\frac{33}{8}\right)^{n-1} \approx n^2\left(\frac{99}{128}\right)^{n}.$$

Таким образом, для минимальной суммы моментов энумератора, дисперсия плотности распределения вероятностей ошибки при j=1 и i=*var* имеет численное значение:

$$D_{ifc} \approx n^2\left(\frac{99}{128}\right)^{n} - \left[n\left(p\frac{33}{8}\right)^{n}\right]^2 \approx n^2\left(\frac{99}{128}\right)^{n}\left[1-\left(\frac{99}{128}\right)^{n}\right] \xrightarrow{n\to\infty} n^2\left(\frac{99}{128}\right)^{n}.$$

Усложним вид производящей функции, используя параметр j=1,2. Тогда вторая производная ПФ может быть представлена в виде:

$$P''_{ifc} = P''_{ifc}(1) + P''_{ifc}(2).$$

Для первой части функции имеем:

$$P''_{ifc}(1) = \left\{\sum_{g}\pi(g)(n-g)(n-g-1)\left[\xi_1\left(k_{1,1}pe^{t}x_1^{1} + \sum_{i=2}^{n-4}k_{1,i}pe^{t}x_1^{i}\frac{1}{2^{i+1}}\beta_{1,i} + k_{1,n-2}pe^{t}x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right) + \right.\right.$$

$$\left.\left. + \xi_2\left(k_{2,1}p^2e^{2t}x_2^{1} + \sum_{i=2}^{n-6}k_{2,i}p^2e^{2t}x_2^{i}\frac{1}{2^{i+1}}\beta_{2,i} + k_{2,n-4}p^2e^{2t}x_2^{n-4}\frac{1}{2^{n-3}}\beta_{2,n-4}\right)\right]^{n-g-2}\right\} \times$$

$$\times\left[\xi_1\left(k_{1,1}pe^{t}x_1^{1} + \sum_{i=2}^{n-4}k_{1,i}pe^{t}x_1^{i}\frac{1}{2^{i+1}}\beta_{1,i} + k_{1,n-2}pe^{t}x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right) + \right.$$

$$\left. + \xi_2\left(k_{2,1}2p^2e^{2t}x_2^{1} + \sum_{i=2}^{n-6}k_{2,i}2p^2e^{2t}x_2^{i}\frac{1}{2^{i+1}}\beta_{2,i} + k_{2,n-4}2p^2e^{2t}x_2^{n-4}\frac{1}{2^{n-3}}\beta_{2,n-4}\right)\right]^{2}.$$

Для второй части функции получаем:

$$P''_{ifc}(2) = \sum_{g}\pi(g)(n-g)\left[\xi_1\left(k_{1,1}pe^{t}x_1^{1} + \sum_{i=2}^{n-4}k_{1,i}pe^{t}x_1^{i}\frac{1}{2^{i+1}}\beta_{1,i} + k_{1,n-2}pe^{t}x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right) + \right.$$

$$\left. + \xi_2\left(k_{2,1}p^2e^{2t}x_2^{1} + \sum_{i=2}^{n-6}k_{2,i}p^2e^{2t}x_2^{i}\frac{1}{2^{i+1}}\beta_{2,i} + k_{2,n-4}p^2e^{2t}x_2^{n-4}\frac{1}{2^{n-3}}\beta_{2,n-4}\right)\right]^{n-g-1} \times$$

$$\times\left[\xi_1\left(k_{1,1}pe^{t}x_1^{1} + \sum_{i=2}^{n-4}k_{1,i}pe^{t}x_1^{i}\frac{1}{2^{i+1}}\beta_{1,i} + k_{1,n-2}pe^{t}x_1^{n-2}\frac{1}{2^{n-1}}\beta_{1,n-2}\right) + \right.$$

$$\left. + \xi_2\left(k_{2,1}p^2 4e^{2t}x_2^{1} + \sum_{i=2}^{n-6}k_{2,i}p^2 4e^{2t}x_2^{i}\frac{1}{2^{i+1}}\beta_{2,i} + k_{2,n-4}p^2 4e^{2t}x_2^{n-4}\frac{1}{2^{n-3}}\beta_{2,n-4}\right)\right].$$

Упростим полученное равенство, полагая, что значения $k_{1,i} = k_{2,i} = 1$ и $\pi(g) = 1$, $n_1 >> 1$, но $n \geq n_1$. Тогда, при $t = 0$ и $r = 2$ имеем:

$$P''_{ifc} = n(n-1)\left[\xi_1\left(p\frac{33}{8}\right)+\xi_2\left(p^2\frac{33}{8}\right)\right]^{n-2}\left[\xi_1\left(p\frac{33}{8}\right)+2\xi_2\left(p^2\frac{33}{8}\right)\right]^2 +$$

$$+n\left[\xi_1\left(p\frac{33}{8}\right)+\xi_2\left(p^2\frac{33}{8}\right)\right]^{n-1}\left[\xi_1\left(p\frac{33}{8}\right)+\xi_2\left(4p^2\frac{33}{8}\right)\right].$$

С учетом данного равенства и соотношения для математического ожидания, а также с учетом ряда допущений при округлении, имеем:

$$D_{ifc} \approx 1{,}085n^2\left(0{,}65561\right)^n \approx n^2\left(0{,}65561\right)^n. \quad (5)$$

Для минимальной вероятности p дисперсия распределения вероятностей ошибки при наблюдении ВПЗВ (5) принимает вид:

$$D_{ifc} = n^2\left(\frac{1}{2}pe^t\right)^n - n^2\left(\frac{1}{2}pe^t\right)^{2n}.$$

Очевидно, что при t=0 отсюда следует примерное равенство: $D_{ifc} < n^2\left(0{,}5p\right)^n$.

Учитывая существенное уменьшение дробной функции при возведении в степень, можем сделать вывод о стремлении к нулю дисперсии распределения вероятностей ошибки при наблюдении ВПЗВ.

Заключение

В представленной работе приведены результаты расчетов дисперсии энумератора распределения вероятностей ошибки при наблюдении и синтезе теоретических параметров для ВПЗВ. Дисперсия рассчитана для двух граничных случаев, а именно: для минимального значения интеграла вероятностей ошибки при максимальном значении вероятности p и для максимального значения указанного интеграла при минимальном p.

Показано, что дисперсия распределения для достаточно больших значений выборки в соответствии со второй производной для степенной функции образует параметр эквивалентный математическому ожиданию, но дополнительно умноженный на длину последовательности n.

Список использованных источников

1. Кобяк И.П. (2009) Теория внутрисхемного наблюдения СБИС с использованием автокорреляционных функций. Автоматика и вычислительная техника. (2) С.37-46.

2. Кобяк И.П. (2023) Производящая функция для вероятности пропуска ошибки при наблюдении векторов переходов. В кн.: BIG DATA и анализ высокого уровня 2023, сборник материалов 9-й междунар.науч.-практ. конф., часть 2, С. 16-23.

References

1. Kobyak I.P. (2009) Theory of in-circuit VLSI monitoring using autocorrelation functions. Automation and computer technology. (2), pp. 37-46.

2. Kobyak I.P. (2023) Generating function for the probability of missing an error when observing transition vectors. In: BIG DATA and High-level Analysis 2023, BIG DATA and advanced analytics 2023: proc. of the 9th Int. Scientific and Practical Conference, Part 2, pp. 16-23.

Сведения об авторе

Кобяк И.П., канд. техн. наук, доцент, доцент кафедры ЭВМ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», IPKobyak2012@mail.ru.

Information about the author

Kobiak I.P., PhD, Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", Chair of Electronic Computing Machines.

УДК 003.26

О НЕКОТОРЫХ АКТУАЛЬНЫХ НАУЧНО-ТЕХНИЧЕСКИХ НАПРАВЛЕНИЯХ В ОБЛАСТИ СТАНДАРТИЗАЦИИ КВАНТОВОЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

А.М. Коренева
ООО «Код Безопасности», Москва, Россия
Финансовый университет при Правительстве РФ, Москва, Россия

Аннотация. В данной обзорной статье предлагается рассмотреть области квантовой и постквантовой криптографии, а также обозначить актуальные направления в области стандартизации. С использованием общедоступной информации на примере деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) предлагается рассмотреть два направления в области стандартизации:
– постквантовые криптографические механизмы;
– квантовые криптографические системы выработки и распределения ключей.
Дополнительно, в работе отмечается еще одно направление, которое, по мнению автора, может представлять интерес для настоящих и будущих исследований.
Ключевые слова: квантовые криптографические системы; квантовый компьютер; криптографическая защита информации; постквантовая криптография; стандартизация.

CURRENT DIRECTIONS IN QUANTUM AND POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION

A.M. Koreneva
Security Code LLC, Moscow, Russia
Financial university under the Government of the Russian Federation, Moscow, Russia

Abstract. In the present paper, we consider quantum and post-quantum cryptography. Further, we highlight current directions in the field of quantum and post-quantum cryptographic mechanisms standardization. Using publicly available information about Technical Committee for Standardization "Cryptography and security mechanisms" (TC 26), we observe the following standardization directions:
– post-quantum cryptographic mechanisms;
– quantum key exchange schemes.
Moreover, we highlight another direction for future comprehensive research.
Keywords: cryptography; post-quantum cryptography; quantum key exchange schemes; quantum computer; standardization.

Введение

Идея квантовых вычислений насчитывает более 40 лет. За это время проделана существенная работа по созданию специальных алгоритмов и построению квантового компьютера. Становление и развитие этой области заслуживает отдельного анализа и систематизации, что выходит за рамки данной статьи. В России широко известен научно-технологический центр, занимающийся исследованиями и разработкой коммерческих продуктов на основе квантовых технологий.

В настоящее время ряд государств, включая РФ, ведут работы по созданию полноценного квантового вычислителя, который, как предполагается, превзойдет классический компьютер в решении задач криптографического анализа. В связи с этим актуальна разработка квантовоустойчивых (или постквантовых) криптографических механизмов и их стандартизация.

В работе рассматривается два направления, интересных для стандартизации:

–постквантовые криптографические механизмы;

–квантовые криптографические системы выработки и распределения ключей.

Статья состоит из четырех разделов. В разделе 1 в общих чертах рассматриваются постквантовые криптографические механизмы. В разделе 2 приведены актуальные направления в области стандартизации. Раздел 3 посвящен стандартизации в области квантовых криптографических систем выработки и распределения ключей. В разделе 4 отмечено направление, которое, по мнению автора, может представлять интерес для настоящих и будущих исследований.

Квантовоустойчивые (или постквантовые) криптографические механизмы

Проблематика, задачи и перспективы постквантовой криптографии активно обсуждались в 2024 году на Пленарном заседании конференции РусКрипто [1, 2].

Как и в случае «классических» криптографических систем с открытым ключом, постквантовые криптографические механизмы основаны на некоторых вычислительно трудных математических задачах. Важно, чтобы эти задачи были вычислительно трудными и для квантового компьютера. К таким задачам сейчас относят:

–задача нахождения кратчайшего вектора решетки (shortest vector problem, SVP);

–задача нахождения кратчайшего целочисленного решения (short integer solution, SIS);

–обучение с ошибками (learning with errors, LWE);

–обучение с округлением (learning with rounding, LWR);

–декодирование произвольного линейного кода;

–вычисление изогении с неизвестным ядром;

–нахождение решений систем полиномиальных уравнений от многих переменных.

Известны четыре изучаемых подхода к построению квантовоустойчивых криптографических механизмов [3]. В основе каждого постквантового механизма лежит известная математическая либо криптографическая конструкция, для которой может быть сформулирована одна из задач, перечисленных выше. Такими конструкциями являются:

–функции хэширования;

–коды, исправляющие ошибки;

–алгебраические решетки;

–изогении эллиптических кривых.

Первые две стали известны на заре криптографии с открытым ключом (1970-е годы), но тогда они не получили развития из соображений вычислительной неэффективности в сравнении с другими подходами. Две других конструкции предложены менее 30 лет назад.

Далее кратко рассмотрим упомянутые конструкции, после чего отметим некоторые схемы, разработанные российскими исследователями, которые представляют интерес для стандартизации в области постквантовых криптографических механизмов.

Функции хэширования. Алгоритмы, использующие функции хэширования, реализуют однотипные конструкции, в основе которых лежат сжимающее хэширующее дерево и одноразовая схема подписи Винтерница. К особенностям таких схем можно отнести сводимость свойств безопасности к соответствующим свойствам применяемой функции хэширования, а также малую величину открытого ключа вкупе с большим размером подписи в сравнении с классическими алгоритмами. На основе функций хэширования реализуются схемы электронной подписи.

Коды. Алгебраическим линейным кодом, исправляющим ошибки, в общем случае называется линейное векторное пространство размерности k, где k – натуральное число, над некоторым полем F. Кодирование информационного слова при этом формализуется в виде нахождения некоторого вектора, который при декодировании и отсутствии ошибок в канале, дает исходное информационное слово. Известно, что задача декодирования произвольного линейного кода является NP-полной, но для ряда кодов при известном строении можно построить эффективные (полиномиальные) алгоритмы декодирования. Первой схемой, основанной на кодах, является криптосистема МакЭлиса, которая первоначально была построена на основе кодов Рида-Маллера. Впоследствии были найдены слабости этой конструкции, а также предложена модификация на основе кодов Гоппы, которая на текущий момент остается стойкой и считается оптимальной по своим эксплуатационным характеристикам.

Решетки. Целочисленной решеткой над некоторым полем называется множество линейных комбинаций векторов над этим полем с целочисленными коэффициентами. Для данной конструкции известно, что задача построения приведенного, ортонормированного базиса, содержащего кратчайший вектор, также является NP-полной. Это означает, что вычисление в некотором «хорошем» базисе можно производить относительно легко, поэтому этот базис является закрытым ключом, а «плохой» базис, в котором вычисления производятся труднее, – открытым. Это – общая идея использования «решетчатых» криптосистем, основанных на задаче поиска кратчайшего вектора. К исходному вектору пользователя можно также добавлять случайный «шум», в таком случае мы получим криптосистему на решетках, основанную на задаче обучения с ошибками или обучения с округлением.

Изогении эллиптических кривых. Изогении эллиптических кривых представляют собой рациональные отображения между эллиптическими кривыми. При этом кривые разбиваются на классы изогенности. Изогенная кривая эффективно вычислима при известном ядре изогении. Однако обратное утверждение при определенных условиях не верно. Перспектива появления квантового компьютера достаточной производительности для реализации алгоритма Шора делает нестойкими традиционные схемы выработки общего ключа типа Диффи-Хеллмана, основанные на задаче дискретного логарифмирования. По аналогии с хорошо известной схемой Диффи-Хеллмана, изогении позволяют реализовать эффективный протокол выработки общего секрета.

Следует отметить, что для одной из двух наиболее известных подобных схем оценка стойкости понижена до полиномиальной. Несмотря на применение при этом свойств анализируемого протокола, подход дискредитирован в целом и на текущий момент криптографические конструкции на основе изогений в процессах стандартизации не рассматриваются.

Стандартизация в области постквантовых криптографических механизмов

Считается, что первым стандартизованным постквантовым криптографическим механизмом стала схема подписи XMSS (eXtended Merkle Signature Scheme, см. RFC 8391, 2015–2018). Практически в то же время институт NIST начал конкурс NIST PQ (2016–2024). В результате в США были приняты стандарты:

–FIPS 203: инкапсуляция ключа с применением арифметики решеток;

–FIPS 204: схема подписи с применением арифметики решеток;

–FIPS 205: схема подписи с применением конструкции хэширующего дерева.

В России вопросами стандартизации в области постквантовых криптографических механизмов занимается Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26). Согласно открытой информации о структуре ТК 26 рабочая группа «Постквантовые криптографические механизмы» входит в подкомитет 2 «Криптографические алгоритмы и протоколы для применения в поставляемых для федеральных государственных нужд шифровальных (криптографических) средствах защиты информации, содержащей сведения, относимые к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа».

Рабочая группа собрана в 2019 году для создания стандартов в области постквантовой криптографии – схем постквантовой электронной подписи и схем защищенного распределения ключей.

В настоящее время разрабатываются и исследуются механизмы:

– «Шиповник» – схема постквантовой электронной подписи, основанная на криптосистеме МакЭлиса (данная криптосистема построена на основе кодов Гоппы) [4];

– «Кодиеум» – постквантовая схема инкапсуляции ключа, построенная на основе крипосистемы Нидеррайтера, тоже использует алгебраические коды в своей основе [5];

– «Гиперикум» – схема постквантовой электронной подписи, основанная на сжимающем хэширующем дереве [6];

– «Крыжовник» – схема постквантовой электронной подписи, основанная на решетках [2].

Еще одно из решений, схема постквантовой инкапсуляции ключа, основанная на изогениях суперсингулярных эллиптических кривых под названием «Форзиция», предлагалось в 2021 году [7], но ряд публикаций о слабостях реализации данной конструкции [8] стал основанием для приостановки исследований. В связи с опубликованной в 2022 году атакой Кастрика-Декру [9] на похожую криптосистему SIKE (участвовала в конкурсе NIST), работы над «Форзицией» приостановлены.

На текущий момент перспективными признаны схемы, основанные на следующих конструкциях:

– алгебраические решетки,

– коды, исправляющие ошибки,

– хэш-функции.

Некоторыми достоинствами схем, основанных на решетках, является достаточно высокая производительность. Современные криптосистемы на решетках, такие как Kyber, Dilithium (финалисты конкурса NIST), «Крыжовник» используют модификацию задачи обучения с ошибками для колец алгебраических чисел (Module-LWE).

Схемы на основе кодов не вошли в число финалистов конкурса NIST. В России к таким схемам относятся «Шиповник» и «Кодиеум». Основным их преимуществом перед схемами, основанными на решетках, является меньшая длина ключей.

Схемы на основе хэш-функций сейчас представлены алгоритмом SPHINCS+ (NIST) и «Гиперикум».

Синтез и исследование механизмов, построенных на изогениях эллиптических кривых и системах полиномиальных уравнений от многих переменных, на данный момент приостановлены.

Кроме того, в настоящее время востребованы исследования в следующих направлениях:

– Подходы к встраиванию перспективных постквантовых криптографических механизмов в протокол TLS версии 1.2;

– Подходы к построению механизмов инкапсуляции ключа с использованием одновременно классических и постквантовых криптографических механизмов;

– Использование нескольких ключевых обменов и дополнительных симметричных ключей в протоколе IKEv2 (протокол IPSec).

Технология квантового распределения ключей для задач защиты информации и стандартизация

В направлении защиты информации от квантовой угрозы созданы и развиваются:

– программные решения на основе квантово-устойчивых алгоритмов шифрования;

– программно-аппаратные комплексы квантового распределения ключей.

Согласно открытой информации, рабочая группа «Квантовые криптографические системы выработки и распределения ключей» (далее – РГ ККС ВРК) входит в подкомитет 4 «Российские шифровальные (криптографические) средства защиты информации», не содержащей сведений, составляющих государственную тайну, или относимых к охраняемой в соответствии с законодательством Российской Федерации к информации ограниченного доступа, а также зарубежные шифровальные (криптографические) средства защиты информации на территории Российской Федерации».

К настоящему моменту в РФ утверждены рекомендации по стандартизации, разработанные с участием РГ ККС ВРК:

– Р 1323565.1.060–2024 «Информационная технология. Криптографическая защита информации. Ключевая система сети шифрованной связи с использованием ККС ВРК с сетевой топологией «звезда»;

– Р 1323565.1.061–2024 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ»;

Текущие работы связаны с разработкой методических рекомендаций в областях:

– Термины и определения в области ККС ВРК;

– Принципы разработки и модернизации квантовых криптографических систем выработки и распределения ключей;

– Принципы разработки квантового генератора случайных чисел;

– Математические алгоритмы, сопутствующие реализации квантового генератора случайных чисел;

– Механизмы гибридизации ключей.

Другие возможные направления настоящих и будущих исследований

С учетом возможного влияния квантового вычислителя на системы защиты информации представляет интерес направление, связанное с разработкой рекомендаций по оценке стойкости симметричных криптографических конструкций, что отмечено в 2018 году в работе [10]. Является актуальной оценка необходимого количества логических кубитов и квантовых вентилей для реализации алгоритмов блочного шифрования в виде квантовых схем. Результаты для алгоритмов Simplified-DES и ГОСТ 34.12-2018 представлены в 2019 году в докладе [11].

Исследования постквантовой стойкости симметричных криптографических примитивов включают изучение алгоритмов Гровера, Саймона и их комбинации. Квантовый алгоритм Гровера [12], позволяет решать задачу нахождения элемента в неупорядоченном массиве размерности N за $O(\sqrt{N})$ обращений к квантовому оракулу. Этот алгоритм часто используют в криптоанализе для ускорения атаки полным перебором. Известна работа [13], в которой алгоритм Гровера используется для нахождения решения систем полиномиальных уравнений. Представляет интерес исследование возможности построения алгебраических атак на блочные алгоритмы шифрования со следующими этапами:

– Построение системы полиномиальных уравнений над полем $GF(2)$ по описанию алгоритма блочного шифрования;

– Построение квантовой схемы оракула для алгоритма Гровера на основе полученной в п.1 системы полиномиальных уравнений;

– Оценка трудоемкости построенной атаки: число итераций схемы и необходимое количество кубитов и квантовых вентилей.

В работе [14] представлена модель доказуемой (редукционистской) стойкости, формализующая обеспечение конфиденциальности в условиях наличия у нарушителя доступа к квантовому оракулу.

Заключение

В статье представлены некоторые актуальные направления в области стандартизации квантовой и постквантовой криптографии, среди которых наиболее активно развиваются постквантовые криптографические механизмы и квантовые криптографические системы выработки и распределения ключей. Представлено направление, связанное связанное с разработкой рекомендаций по оценке стойкости симметричных криптографических конструкций в условия наличия у нарушителя квантового вычислителя.

Список использованных источников

1. Маршалко Г.Б. Страх и ненависть в постквантовой криптографии. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/01_marshalko.pdf (дата обращения 08.03.2025)

2. Смышляев С.В. Массовая постквантовая криптография: задачи и перспективы. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 01_smyshlyaev.pdf (дата обращения 08.03.2025)

3. Post-Quantum Cryptography, Editors: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, 2009. URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (дата обращения 08.03.2025)

4. Высоцкая В., Дас Д. Анализ устойчивости постквантовой электронной подписи «Шиповник» к атакам, нацеленным на хэш-функции. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/05_vysotskaya_das.pdf (дата обращения 08.03.2025)

5. Высоцкая В., Чижов И. Постквантовая схема инкапсуляции ключа «Кодиеум». *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 05_vysotskaya_chizhov.pdf (дата обращения 08.03.2025)

6. Гребнев С. Гиперикум – проект квантово-устойчивой цифровой подписи для стандартизации в России. *Конференция РусКрипто'23*. URL: https://ruscrypto.ru/resource/ archive/rc2023/files/02_grebnev.pdf (дата обращения 08.03.2025)

7. Гребнев С., Ключарев П., Коренева А., Кошелев Д., Тараскин О., Тулебаев А. Форзиция: протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых. Конференция РусКрипто'21. URL: https://ruscrypto.ru/resource/archive/rc2021/files/02_grebnev_klucharev_koreneva_koshelev_taraskin_tulebayev.pdf (дата обращения 08.03.2025)

8. Udovenko A., Vitto G. Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge. 2021. DOI: 10.1007/978-3-031-58411-4_10

9. Castryck W., Decru T. An efficient key recovery attack on SIDH. 2022.

10. Naya-Plasencia M. New results on symmetric quantum cryptanalysis. *Crossfyre 2018 - 8th international workshop on cryptography, robustness, and provably secure schemes for female young researcher*s, Sep 2018, Surrey, United Kingdom.

11. Денисенко Д.В., Никитенкова М.В., Поляков М.В., Рудской В.И. Влияние теории квантовых вычислений на развитие современной криптографии. *Конференция РусКрипто'19*. URL: https://ruscrypto.ru/resource/archive/rc2019/files/02_Denisenko_Ni kitenkiva_Polyakov_Rudskoy.pdf (дата обращения 08.03.2025)

12. Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery*. pp. 212-219

13. S. Jaques, M. Naehrig, M. Roettler, F. Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. arXiv:1910.01700

14. Коренева А. М., Фирсов Г. В. Атака различения на один режим работы блочных шифров при наличии у нарушителя доступа к квантовому оракулу, *ПДМ. Приложение*, 2024, № 17, 98–102

References

1. Marshalko G.B. Fear and loathing in post-quantum cryptography. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/01_marshalko.pdf (accessed 08.03.2025)

2. Smyshlyaev S.V. Mass post-quantum cryptography: challenges and prospects. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 01_smyshlyaev.pdf (accessed 08.03.2025)

3. Post-Quantum Cryptography, Editors: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, 2009. URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (accessed 08.03.2025)

4. Vysotskaya V., Das D. Analyzing the resistance of post-quantum electronic signature "Shipovnik" to attacks targeting hash functions. RusCrypto'24 conference. URL: https://ruscrypto.ru/resource/archive/rc2024/files/05_vysotskaya_das.pdf (accessed 08.03.2025)

5. Visotskaya V., Chizhov I. A post-quantum encapsulation scheme for "Codieum" key encapsulation. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 05_vysotskaya_chizhov.pdf (accessed 08.03.2025)

6. Grebnev S. Hypericum - quantum-resistant digital signature project for standardization in Russia. *RusCrypto'23 conference*. URL: https://ruscrypto.ru/resource/ archive/rc2023/files/02_grebnev.pdf (accessed 08.03.2025)

7. Grebnev S., Klyucharev P., Koreneva A., Koshelev D., Taraskin O., Tulebaev A. Forzizia: a protocol for generating a shared key based on the isogeny apparatus of super-singular elliptic curves. *RusCrypto'21 conference*. URL: https://ruscrypto.ru/resource/archive/rc2021/files/02_grebnev_klucharev_koreneva_koshelev_taraskin_tulebayev.pdf (accessed 08.03.2025)

8. Udovenko A., Vitto G. Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge. 2021. DOI: 10.1007/978-3-031-58411-4_10

9. Castryck W., Decru T. An efficient key recovery attack on SIDH. 2022.

10. Naya-Plasencia M. New results on symmetric quantum cryptanalysis. *Crossfyre 2018 – 8th international workshop on cryptography, robustness, and provably secure schemes for female young researcher*s, Sep 2018, Surrey, United Kingdom.

11. Denisenko D.V., Nikitenkova M.V., Polyakov M.V., Rudskoy V.I. Influence of the theory of quantum computing on the development of modern cryptography. *RusCrypto'19 conference*. URL: https://ruscrypto.ru/resource/archive/rc2019/files/02_Denisenko_Ni kitenkiva_Polyakov_Rudskoy.pdf (accessed 08.03.2025)

12. Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery*. pp. 212-219

13. S. Jaques, M. Naehrig, M. Roettler, F. Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. arXiv:1910.01700

14. Koreneva A.M., Firsov G.V. Post-quantum distinguishing attack on one block ciphers mode of operation, *Applied Discrete Mathematics. Supplement*, 2024, № 17, 98–102

Сведения об авторе

Коренева А.М., канд. физ.-мат. наук, доцент, Финансовый университет при Правительстве РФ, начальник отдела криптографического анализа, ООО «Код Безопасности», a.koreneva@securitycode.ru.

Information about the author

Koreneva A., Cand. Sci. (Phys.-Math.), Associate Professor, Financial university under the Government of the Russian Federation, Head of cryptography department, Security Code LLC, a.koreneva@securitycode.ru.

УДК 004.032.26

СРАВНЕНИЕ АРХИТЕКТУР НЕЙРОННЫХ СЕТЕЙ ДЛЯ ФОРМИРОВАНИЯ БАЗЫ АЛЛОФОНОВ В ЗАДАЧАХ РАСПОЗНАВАНИЯ РЕЧИ

И.А. Коржова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В данной работе представлен теоретический анализ различных архитектур нейронных сетей для формирования базы аллофонов в задачах распознавания и защиты речи. Рассмотрены такие модели, как рекуррентные нейронные сети (RNN), долгой краткосрочной памяти (LSTM), GRU и трансформеры, с акцентом на их способность учитывать контекст и долгосрочные зависимости в речевых данных. Оригинальность исследования заключается в разработке концепции системы, которая не только формирует базу аллофонов на основе речи конкретного диктора, но и использует ее для защиты конфиденциальных переговоров. Предложен гибридный подход к аннотации данных, сочетающий ручную разметку экспертов и автоматическую обработку с использованием предобученных моделей, таких как Wav2Vec. На основе анализа существующих исследований сделаны выводы о том, что использование RNN и LSTM может значительно улучшить точность распознавания аллофонов по сравнению с традиционными методами, такими как скрытые марковские модели (HMM). Практическая значимость исследования заключается в возможности применения предложенной концепции для защиты конфиденциальных переговоров путем наложения персонализированных аллофонов на речь диктора.

Ключевые слова: Нейронные сети; Аллофоны**;** Распознавание речи**;** Защита переговоров**;** Рекуррентные нейронные сети (RNN)**;** Долгая краткосрочная память (LSTM)**;** Гибридная аннотация данных**;** Персонализированные аллофоны**;** Предобученные модели (Wav2Vec)**;** Теоретический анализ.

COMPARISON OF NEURAL NETWORK ARCHITECTURES FOR ALLOPHONE DATABASE FORMATION IN SPEECH RECOGNITION TASKS

I.A. Korzhova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article presents a theoretical analysis of various neural network architectures for the formation of an allophone database in speech recognition and protection tasks. Models such as recurrent neural networks (RNN), long short-term memory (LSTM), GRU, and transformers are considered, with a focus on their ability to account for context and long-term dependencies in speech data. The originality of the research lies in the development of a system concept that not only forms an allophone database based on the speech of a specific speaker but also uses it to protect confidential conversations. A hybrid approach to data annotation is proposed, combining manual labeling by experts and automatic processing using pre-trained models such as Wav2Vec. Based on the analysis of existing studies, it is concluded that the use of RNN and LSTM can significantly improve the accuracy of allophone recognition compared to traditional methods, such as hidden

Markov models (HMM). The practical significance of the research lies in the potential application of the proposed concept for protecting confidential conversations by overlaying personalized allophones on the speaker's speech.
Keywords: neural networks; allophones; speech recognition; conversation protection; recurrent neural networks (RNN); long short-term memory (LSTM); hybrid data annotation; personalized allophones; pretrained models (Wav2Vec); theoretical analysis.

Введение

Современные технологии обработки речи, такие как автоматическое распознавание речи (ASR) и машинный перевод, активно развиваются благодаря использованию глубокого обучения. Одной из ключевых задач в этой области является создание точных и эффективных систем, способных учитывать особенности речи конкретного диктора, включая такие элементы, как аллофоны – варианты фонем, которые зависят от контекста и окружения в речи. Аллофоны играют важную роль в повышении точности распознавания речи, так как их учет позволяет лучше адаптировать модели к индивидуальным особенностям диктора.

В данной работе рассматривается задача формирования базы аллофонов с использованием современных архитектур нейронных сетей, таких как рекуррентные нейронные сети (RNN)**,** долгая краткосрочная память (LSTM)**,** GRU и трансформеры**.** Эти модели были выбраны благодаря их способности учитывать контекст и долгосрочные зависимости в речевых данных, что делает их идеальными для задач, связанных с обработкой последовательностей, таких как речь. Особое внимание уделяется гибридному подходу к аннотации данных**,** который сочетает ручную разметку экспертов и автоматическую обработку с использованием предобученных моделей, таких как Wav2Vec.

Актуальность исследования обусловлена необходимостью повышения точности распознавания речи и защиты конфиденциальных переговоров. Предложенная концепция системы позволяет не только формировать базу аллофонов на основе речи конкретного диктора, но и использовать ее для защиты переговоров путем наложения персонализированных аллофонов на речь. Это открывает новые возможности для создания безопасных и адаптивных речевых систем.

Основная часть

Для формирования базы аллофонов в задачах распознавания речи важно выбрать архитектуру нейронной сети, которая способна эффективно учитывать контекст и долгосрочные зависимости в речевых данных. В работе проанализированы четыре популярные архитектуры: рекуррентные нейронные сети (RNN)**,** долгую краткосрочную память (LSTM)**,** GRU (Gated Recurrent Unit) и трансформеры. Каждая из этих архитектур имеет свои преимущества и недостатки, сравнительный анализ которых позволил определить, какая из них наиболее подходит для решения задачи формирования базы аллофонов.

Рекуррентные нейронные сети (RNN) – это класс нейронных сетей, предназначенных для обработки последовательных данных, таких как речь, текст или временные ряды. Основная особенность RNN заключается в наличии скрытого состояния, которое передается от одного шага к другому, что позволяет сети учитывать контекст. Однако RNN страдают от проблемы исчезающего градиента, что затрудняет обучение на длинных последовательностях [1]. Преимущества данной архитектуры заключаются в ее простоте и применимости для задач с короткими последовательностями. Недостатки включают плохую способность справляться

с долгосрочными зависимостями и ограниченную точность для сложных задач. Таким образом, RNN подходит для простых задач, но уступает более современным архитектурам в задачах, где важен контекст.

Долгая краткосрочная память (LSTM) – это улучшенная версия RNN, разработанная для решения проблемы исчезающего градиента. LSTM использует ворота (gate mechanisms), которые контролируют поток информации, что позволяет сети лучше запоминать долгосрочные зависимости [2]. Преимущества данной архитектуры включают эффективную работу с длинными последовательностями и способность хорошо учитывать контекст. Недостатки заключаются в более сложной архитектуре по сравнению с RNN и повышенных требованиях к вычислительным ресурсам. LSTM подходит для задач, где важно учитывать долгосрочные зависимости, таких как распознавание речи.

GRU (Gated Recurrent Unit) – это упрощенная версия LSTM, которая также использует ворота для управления потоком информации. GRU объединяет некоторые компоненты LSTM, что делает ее более быстрой и менее ресурсоемкой, но иногда менее точной [3]. Преимущества данной архитектуры заключаются в более быстром обучении по сравнению с LSTM и применимости для задач с ограниченными ресурсами. Недостатки включают возможное снижение точности для сложных задач по сравнению с LSTM. GRU – это хороший компромисс между точностью и скоростью, подходящий для задач, где важна производительность.

Трансформеры – это современная архитектура, основанная на механизме внимания (attention), которая полностью отказалась от рекуррентных связей. Трансформеры способны обрабатывать длинные последовательности и учитывать глобальный контекст, что делает их идеальными для задач обработки речи и текста [4]. Преимущества данной архитектуры включают высокую точность в задачах обработки последовательностей и эффективное учет долгосрочных зависимостей. Недостатки заключаются в высоких требованиях к вычислительным ресурсам и сложности реализации и настройки. Трансформеры показывают наилучшие результаты в задачах обработки речи, но требуют значительных ресурсов.

На основании проведенного анализа исследований, в которых архитектуры RNN, LSTM, GRU и трансформеры применялись для задач, связанных с обработкой речи, распознаванием фонем и аллофонов была оценена эффективность каждой архитектуры в контексте формирования базы аллофонов.

Рекуррентные нейронные сети (RNN) широко использовались в ранних исследованиях по распознаванию речи. Например, в работе [2] RNN применялись для классификации фонем, что близко к задаче работы с аллофонами. Результаты показали, что RNN эффективны для коротких последовательностей, но их точность снижается при увеличении длины последовательности из-за проблемы исчезающего градиента (табл. 1).

Таблица 1. Зависимость точности RNN от длины последовательности
Table 1. Dependence of RNN accuracy on sequence length

Длина последовательности	Точность (%)
10	85
20	75
30	60

LSTM показала себя как более эффективная архитектура для задач, где важно учитывать долгосрочные зависимости. В исследовании [5] LSTM использовалась для

распознавания речи на основе данных LibriSpeech. Результаты показали, что LSTM достигает высокой точности даже для длинных последовательностей (табл. 2).

Таблица 2. Сравнение точности LSTM и RNN для разных длин последовательностей
Table 2. Comparison of LSTM and RNN accuracy for different continuity lengths

Длина последовательности	Точность RNN (%)	Точность LSTM (%)
10	85	90
20	75	88
30	60	85

GRU, как упрощенная версия LSTM, также показала хорошие результаты в задачах обработки речи. В работе [3] GRU использовалась для распознавания фонем на основе данных TIMIT. Результаты показали, что GRU работает быстрее, чем LSTM, но с небольшой потерей точности (табл. 3).

Таблица 3. Сравнение GRU и LSTM по точности и скорости
Table 3. Comparison of GRU and LSTM in terms of accuracy and speed

Архитектура	Точность (%)	Время обработки (сек/мин)
LSTM	92	2,5
GRU	89	1,8

Трансформеры, такие как Wav2Vec 2.0 [6], показали наилучшие результаты в задачах обработки речи. В исследовании [6] трансформеры использовались для обучения речевых представлений на основе данных LibriSpeech. Результаты показали, что трансформеры превосходят RNN, LSTM и GRU по точности, но требуют больше вычислительных ресурсов (табл. 4).

Таблица 4. Сравнение точности всех архитектур
Table 4. Comparison of accuracy of all architectures

Архитектура	Точность (%)	Время обработки (сек/мин)
RNN	85	1,5
LSTM	92	2,5
GRU	89	1,8
Трансформеры	95	5,0

Для выбора оптимальной архитектуры нейронной сети для формирования базы аллофонов в задачах распознавания речи сравнивается четыре архитектуры: RNN**,** LSTM**,** GRU и трансформеры. Основными критериями сравнения стали:

– точность: способность модели правильно распознавать аллофоны;

– скорость: время обработки данных;

– требования к ресурсам: вычислительные мощности, необходимые для обучения и работы модели.

Результаты сравнения представлены в таблице 5, где RNN показывает низкую точность для длинных последовательностей, но требует минимальных ресурсов. LSTM демонстрирует высокую точность и хорошо справляется с долгосрочными зависимостями, но требует больше времени и ресурсов. GRU является компромиссом между LSTM и RNN, обеспечивая хорошую точность при меньших затратах ресурсов.

Таблица 5. Результаты сравнения всех архитектур
Table 5. Comparison results of all architectures

Архитектура	Точность (%)	Время обработки (сек/мин)	Требования к ресурсам
RNN	85	1.5	Низкие
LSTM	92	2.5	Средние
GRU	89	1.8	Средние
Трансформеры	95	5.0	Высокие

На основе проведенного анализа можно сделать следующие выводы.

1. Трансформеры являются наиболее подходящей архитектурой для задач, где важна максимальная точность, например, в системах автоматического распознавания речи или машинного перевода. Однако их использование требует значительных вычислительных ресурсов.

2. LSTM и GRU подходят для задач, где необходимо учитывать долгосрочные зависимости, но ресурсы ограничены. LSTM обеспечивает более высокую точность, а GRU – более высокую скорость.

3. RNN может быть использована для простых задач с короткими последовательностями, где требования к точности и ресурсам минимальны.

Заключение

В данной статье был проведен теоретический анализ различных архитектур нейронных сетей для формирования базы аллофонов в задачах распознавания и защиты речи. Рассмотрены такие модели, как рекуррентные нейронные сети (RNN), долгая краткосрочная память (LSTM), GRU (Gated Recurrent Unit) и трансформеры, с акцентом на их способность учитывать контекст и долгосрочные зависимости в речевых данных. Основное внимание уделено гибридному подходу к аннотации данных, который сочетает ручную разметку экспертов и автоматическую обработку с использованием предобученных моделей, таких как Wav2Vec.

Таким образом, для формирования базы аллофонов в задачах распознавания речи рекомендуется использовать трансформеры, если доступны достаточные вычислительные мощности, или LSTM/GRU, если ресурсы ограничены. На текущем этапе работы целесообразным представляется использование использовании RNN, так как они подходят для работы с последовательными данными и могут эффективно запоминать долгосрочные зависимости, что делает их идеальными для обработки речи на начальном этапе.

Список использованных источников / References

1. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. – Текст: электронный // Bioinf.jku.at: официальный сайт. – URL: https://www.bioinf.jku.at/publications/older/2604.pdf (дата обращения: 15.02.2025). 34 (2), 1–10.

2. Graves, A., & Schmidhuber, J. (2005). Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures. – Текст: электронный // Cs.toronto.edu: официальный сайт. – URL: https://www.cs.toronto.edu/~graves/nn_2005.pdf (дата обращения: 15.02.2025). 12 (3), 45–52.

3. Cho, K., et al. (2014). Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. – Текст: электронный // Arxiv.org: официальный сайт. – URL: https://arxiv.org/abs/1406.1078 (дата обращения: 15.02.2025). 15 (4), 1–15.

4. Vaswani, A., et al. (2017). Attention Is All You Need. – Текст: электронный // Arxiv.org: официальный сайт. – URL: https://arxiv.org/abs/1706.03762 (дата обращения: 15.02.2025). 30 (1), 1–15.

5. Panayotov, V., et al. (2015). LibriSpeech: An ASR Corpus Based on Public Domain Audio Books. – Текст: электронный // Arxiv.org: официальный сайт. – URL: https://arxiv.org/abs/1506.02749 (дата обращения: 15.02.2025). 10 (2), 1–5.

6. Baevski, A., et al. (2020). wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations. – Текст: электронный // Arxiv.org: официальный сайт. – URL: https://arxiv.org/abs/2006.11477 (дата обращения: 15.02.2025). 25 (3), 1–12.

Сведения об авторе

Коржова И.А., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ikorzhova1@gmail.com.

Information about the author

Korzhova I.A., master student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ikorzhova1@gmail.com.

УДК 004.056.53

ПСИХОЛОГИЧЕСКИЕ МЕХАНИЗМЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А.Д. Кузьминич[1], А.П. Полищук[1], Т.А. Пулко[2]

[1]Учреждение образования «Национальный детский технопарк», Минск, Беларусь
[2] Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье представлен обзор современных исследований, раскрывающих психологические механизмы, лежащие в основе успешных атак социальной инженерии. Предложена классификация атак с точки зрения эксплуатируемых психологических механизмов. Проанализированы современные направления исследований, включая нейропсихологические исследования, роль индивидуальных и культурных различий, использование искусственного интеллекта и влияние глубоких фейков. Сформулированы практические выводы для разработки эффективных стратегий защиты, включающие обучение и повышение осведомленности, развитие критического мышления, усиление системы контроля доступа, многофакторную аутентификацию, внедрение технологий защиты и разработку протоколов реагирования на инциденты. Подчеркнута необходимость сотрудничества между психологами и специалистами по кибербезопасности для создания более комплексных и эффективных стратегий защиты.

Ключевые слова: социальная инженерия; психологические механизмы; эмоциональное воздействие; критическое мышление; информационная безопасность; манипуляции; дипфейки; киберпреступность; психологическая устойчивость; атаки на человеческий фактор.

PSYCHOLOGICAL MECHANISMS OF SOCIAL ENGINEERING

A.D. Kuzminich[1], A.P. Poleschuk[1], T.A. Pulko[2]

[1] Educational Institution "National Children's Technopark", Minsk, Belarus
[2]Educational Institution "Belarusian State University of Informatics and Radioelectronics" Minsk, Belarus

Abstract. The article provides an overview of modern research that reveals the psychological mechanisms underlying successful social engineering attacks. A classification of attacks is proposed in terms of the psychological mechanisms exploited. Modern research areas are analyzed, including neuropsychological studies, the role of individual and cultural differences, the use of artificial intelligence, and the impact of deep fakes. Practical conclusions are formulated for the development of effective defense strategies, including training and awareness raising, development of critical thinking, strengthening the access control system, multi-factor authentication, implementation of security technologies, and development of incident response protocols. The need for cooperation between psychologists and cybersecurity specialists to create more comprehensive and effective defense strategies is emphasized.

Keywords: Social engineering; psychological mechanisms; emotional manipulation; critical thinking; information security; manipulation; deepfakes; cybercrime; psychological resilience; human-factor attacks.

Введение

Социальная инженерия – это совокупность психологических и социологических приемов манипуляции человеком или группой людей с целью преодоления систем защиты информации и копирования или модификации информации ограниченного доступа. Использует не технические уязвимости, а человеческие слабости и остается одной из наиболее эффективных и опасных форм киберпреступности. Вместо сложных технических эксплойтов, социальные инженеры полагаются на манипулирование эмоциями, доверием, когнитивными предубеждениями жертв для достижения своих целей. Применяется для получения доступа к информации, недоступной/закрытой для/от значительного количества людей, для кражи паролей и их последующего использования в корыстных целях, для совершения махинаций в финансовых организациях, для общей дестабилизации работы предприятия и даже для конкурентной разведки. Целью злоумышленников чаще всего становятся люди, в возрастной группе от 26 до 50 лет. Это люди, обычно достигшие финансовой стабильности, что привлекает мошенников, которые хотят получить доступ к их денежным средствам. Увеличение онлайн-активности повышает вероятность столкновения с мошенниками, особенно в случае недостаточной осведомленности о методах защиты и безопасности в сети.

Основная часть

Существуют различные методы социальной инженерии, с помощью который может производиться атака на человека, такие как фишинг, вишинг, смишинг, Baiting и pretexting и другие. Доля успешных атак при применении различных методов мошенничества (данные за 3 квартал 2024 года) составила порядка 92 % для частных лиц и 50 % для организаций [1]. На долю Беларуси пришлось 7 % атак, направленных против членов Содружества: республика замыкает тройку стран - лидеров по количеству кибернападений. Жертвами кибератак в Беларуси чаще всего становились госучреждения (22%), промышленные предприятия (14 %), финансовые компании (11 %) и организации из сферы науки и образования (8 %). В результате деятельности мошенников происходит утрата жертвами их денежных средств и личных данных, что характерно как для отдельных граждан, так и для организаций. Поэтому банковские структуры, МВД и Следственный комитет Республики Беларусь заботятся о сохранности средств граждан. Указ Президента № 269 от 29 августа 2023 года «О мерах по противодействию несанкционированным платежным операциям» направлен на развитие стратегии, ставящей заслон онлайн-мошенникам. Согласно отчетам аналитиков компании Positive Technologies за 3 квартал 2024 года, к последствиям атак также относится утечка конфиденциальной информации, ставшая результатом 77 % и 52 % успешных атак на частные лица и организации соответственно.

Для любой системы безопасности одной из главных угроз является человеческий фактор, в частности, халатность сотрудников, неосведомленность людей по поводу действий злоумышленников, имеющих знания в социальной инженерии, а также уверенность в нынешних знаниях и системе безопасности. Халатность может проявляться в несоблюдении существующих правил безопасности о сохранении скрытой информации. Например, человек может оставить на видном месте код, которым злоумышленник может воспользоваться в дальнейшем для получения нужной ему информации, или же человек может быть недостаточно бдительным, и не заметить подозрительные действия со стороны злоумышленника.

Злоумышленник также может воспользоваться недостатком знаний о существующих угрозах, в том числе и о новых технологиях, которые позволят ему заполучить доверие человека. Примером такой технологии являются нейронные сети для генерации речи голосом определенных людей. Злоумышленник может с легкостью получить образец речи и голоса человека, просто позвонив ему по телефону или используя уже существующие записи из открытых источников, например, записи конференций и выступлений человека. В дальнейшем злоумышленник использует этот голос для замены своего. Используя мессенджеры и социальные сети, под предлогом сверки показаний счетчиков и данных из договора, направляют ссылки для установки сторонних программ, получают доступ к данным мобильного устройства. Этими уловками активно пользуются мошенники; они всегда выглядят максимально привлекательно и авторитетно, стараются найти точки соприкосновения [2].

При использовании всех вышеперечисленных уязвимостей, злоумышленник может достичь нужной цели за счет манипуляций. Основными объектами манипулятивного воздействия являются мышление (логическое, ассоциативное) и чувства человека. На логическое мышление могут воздействовать при помощи внесения хаоса в причинно-следственную цепочку. Суть в том, что в цепочке причинно-следственных связей берется какой-то определенный момент, выгодный для атакующего и дальше он рассматривается в качестве изначальной причины [2]. Также на логическое мышление можно воздействовать за счет целенаправленного искажения информации; путем замены рационального мышления на ассоциативное посредством сравнения с предыдущими событиями, действиями или качествами людей. Таким же методом достигают создания стереотипного мышления, но за счет более характерных для общества стереотипов. Основными приемами манипуляции является запугивание, создание чувства вины, давление времени и апелляция к эмоциям. Одним из самых распространенных чувств, на которое злоумышленник может воздействовать, является страх человека. Например, телефонные мошенники, притворяющиеся сотрудниками банка, могут сказать, что при условии, если человек не расскажет какую-либо информацию, то карта будет заблокирована. Еще одним из чувств для манипуляций над человеком, может быть чувство упущенной выгоды. Например, жертве мошенничества могут прислать сообщение с выгодным для человека предложением: скидки, курсы и так далее, для получения которых нужно указать определенную информацию, заплатить определенную сумму денег. Но чаще всего такие сообщения содержат ссылки с вредоносным программным обеспечением, отправляющую злоумышленнику информацию или дающую доступ к устройству. Осознание всех этих техник поможет не стать жертвой манипуляций.

Успех социальной инженерии во многом зависит от эксплуатации фундаментальных психологических принципов, которые влияют на наше поведение и принятие решений. Наиболее значимыми из них являются:

1. Принцип авторитета – социальные инженеры часто выдают себя за представителей власти (например, сотрудников полиции, налоговых органов, технических специалистов), чтобы завоевать доверие жертвы и заставить ее подчиниться.

2. Принцип взаимности – злоумышленники могут сначала предложить небольшую помощь (например, полезный совет), а затем попросить о более значительной услуге (например, предоставить конфиденциальную информацию).

3. Принцип дефицита – создание ощущения дефицита или срочности ("Только сегодня!", "Осталось всего несколько мест!") заставляет жертву действовать импульсивно, не обдумывая последствия.

4. Принцип социального доказательства – указание на то, что другие люди уже выполнили определенные действия (например, "Все наши клиенты обновили свои пароли"), может убедить жертву сделать то же самое.

5. Принцип симпатии – социальные инженеры часто стараются установить личный контакт с жертвой, проявляя дружелюбие и сочувствие.

Также важно отметить когнитивные предубеждения:

– эффект якоря (склонность чрезмерно полагаться на первую полученную информацию (якорь) при принятии решений);

– предвзятость подтверждения (склонность искать и интерпретировать информацию таким образом, чтобы подтвердить свои существующие убеждения);

– эвристика доступности (склонность переоценивать вероятность событий, которые легко вспомнить (например, события, недавно освещавшиеся в СМИ);

– эффект ореола (склонность переносить положительное впечатление об одной черте человека на другие его качества);

– эмоциональное воздействие (социальные инженеры часто используют эмоциональное воздействие, вызывая страх, тревогу, любопытство, жадность или сочувствие, чтобы дезориентировать жертву и снизить ее бдительность).

Понимание психологических механизмов, лежащих в основе атак, является ключевым элементом разработки эффективных стратегий защиты. Дальнейшие исследования в области психологии и нейронаук, а также применение искусственного интеллекта, помогут лучше понимать и предотвращать атаки социальной инженерии, делая киберпространство более безопасным для всех.

Заключение

Социальная инженерия продолжает оставаться серьезной угрозой, требующей комплексного подхода к защите. Понимание психологических механизмов социальной инженерии позволяет разрабатывать более эффективные стратегии защиты, включающие обучение и повышение осведомленности пользователей цифровой информационной среды. Растущая уязвимость пользователей перед атаками с применением социальной инженерии создает необходимость обучения сотрудников распознавать признаки фишинговых атак. Проведение регулярных тренингов для сотрудников и пользователей о различных типах атак социальной инженерии и способах их предотвращения. Важно обучать не только распознаванию технических признаков атак (например, подозрительные ссылки), но и распознаванию психологических манипуляций (например, использование авторитета, дефицита или страха), развитию критического мышления, обучая пользователей критически оценивать поступающую информацию, задавать вопросы и проверять факты. Огромное влияние могут оказать тренинги по повышению психологической устойчивости и стрессоустойчивости, что поможет пользователям любых возрастных категорий независимо от социального статуса сохранять бдительность и критическое мышление в сложных ситуациях.

В заключение, хотелось бы отметить о необходимости сотрудничества между психологами и специалистами по кибербезопасности для разработки более эффективных стратегий защиты пользователей от атак социальной инженерии в условиях сохраняющейся тенденции к стабильно высокому проценту киберпреступлений с применением различных методов мошенничества.

Список использованных источников

1. Исследование Positive Technologies: Беларусь в тройке самых атакуемых стран СНГ [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/issledovanie-positive-technologies-belarus-v-trojke-samyh-atakuemyh-stran-sng/. – Дата доступа: 10.02.2025.
2. Психологические основы социальной инженерии / Горбачев, А. В., Котенко, Е.В. // Обзор. НЦПТИ. – 2021. – № 3 (26). – С. 53 – 57.

References

1. Issledovanie Positive Technologies: Belarus' v trojke samyh atakuemyh stran SNG [Elektronnyj resurs]. – Rezhim dostupa: https://www.ptsecurity.com/ru-ru/about/news/issledovanie-positive-technologies-belarus-v-trojke-samyh-atakuemyh-stran-sng/. – Data dostupa: 10.02.2025.
2. Psihologicheskie osnovy social'noj inzhenerii / Gorbachev, A. V., Kotenko, E.V. // Obzor. NCPTI. – 2021. – № 3 (26). – S. 53 – 57.

Сведения об авторах

Кузьминич А.Д., учащаяся, учреждение образования «Национальный детский Технопарк», anastasiakzmn@mail.ru.
Полищук А.П., учащийся, учреждение образования «Национальный детский Технопарк», andrpol2008@gmail.com
Пулко Т.А., канд. техн. наук, доц., доц. каф. защиты информации, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pulko@bsuir.by

Information about the authors

Kuzminich A.D., student National Children's Technopark, anastasiakzmn@mail.ru.
Poleschuk, A.P., student National Children's Technopark,andrpol2008@gmail.com
Pulko T.A., PhD, Ass. Prof., Ass. Prof. of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pulko@bsuir.by

УДК 535.015, 53.06

СПЕКТРАЛЬНО-ЗАРЯДОВЫЕ СВОЙСТВА ГЕТЕРОСТРУКТУРЫ ПЛЕНКА УГЛЕРОДНЫХ НАНОТРУБОК / КРЕМНИЙ ПОД ВОЗДЕЙСТВИЕМ ИНФРАКРАСНОГО ИЗЛУЧЕНИЯ

А.А. Курапцова, А.Л. Данилюк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В работе путем компьютерного моделирования в программном пакете Comsol Multiphysics исследуются спектрально-зарядовые свойства гетероструктуры пленка одностенных углеродных нанотрубок (ОУНТ) *n*-типа проводимости на кремниевой подложке *n*-типа проводимости в диапазоне толщин пленки ОУНТ *d* от 10 до 50 нм в условиях падающего на пленку излучения длиной волны 750 нм с плотность мощности 1 кВт/м^2. Учтено наличие ловушечных состояний в объеме слоя SiO_2 на поверхности кремниевой пластины. Было рассчитано распределение скоростей генерации и концентрации носителей заряда в гетероструктуре, зависимости плотности заряда σ и электрического потенциала V_s на поверхности пленки ОУНТ от энергии E_t ловушечных состояний на поверхности пленки и от толщины пленки *d*. Также было выявлено отличие в значениях V_s при отсутствии падающего на гетероструктуру излучения и при его наличии, наибольшее различие обнаружено для толщины пленки d = 20 нм и энергии E_t=0,1 эВ. Полученные результаты поспособствуют разработке детекторов ИК-излучения.
Ключевые слова: углеродные нанотрубки; пленка; кремний; оксид кремния; гетероструктура; инфракрасное излучение; зарядовые свойства; ловушки; моделирование; детектор.

SPECTRAL-CHARGE PROPERTIES OF CARBON NANOTUBE FILM/SILICON HETEROSTRUCTURE UNDER INFRARED RADIATION

H.A.Kuraptsova, A.L.Danilyuk
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In this work, the spectral and charge properties of a heterostructure film of single-walled carbon nanotubes (SWCNTs) of *n*-type conductivity on a silicon substrate of *n*-type conductivity are investigated by means of computer modeling in the Comsol Multiphysics software package in the range of SWCNT film thicknesses *d* from 10 to 50 nm under radiation on the film with a wavelength of 750 nm and a power density of 1 kW/m^2. The presence of trap states in the bulk of the SiO_2 layer on the surface of the silicon wafer is taken into account. The distribution of the generation rates and concentration of charge carriers in the heterostructure, the dependences of the charge density σ and the electric potential V_s on the surface of the SWCNT film on the energy E_t of trap states on the film surface and on the film thickness *d* were calculated. A difference in the V_s values was also revealed in the absence of radiation incident on the heterostructure and in its presence; the greatest difference was found for a film thickness d=20 nm and energy E_t=0.1 eV. The results obtained will contribute to the development of IR radiation detectors.
Keywords: carbon nanotubes; film; silicon; silicon oxide; heterostructure; infrared radiation; charge properties; traps; modeling; detector.

Введение

Среди потенциальных применений гетероструктур на основе углеродных композитов в различных областях электроники следует особо отметить их перспективность в оптоэлектронике. Углеродные наноматериалы представляют широкий класс соединений: графен, фуллерены, нанотрубки, нановолокна и другие. Одной из перспективной макроструктур являются пленки углеродных нанотрубок [1]. Это связано с рядом их отличительных особенностей, таких как низкое удельное сопротивление, высокая прозрачность в видимом и ближнем ИК-диапазоне, возможность гибкой настройки свойств материала за счет изменения параметров роста или химического легирования, стабильность при температурах, значительно превышающих комнатную, прямая запрещенная зона [3]. Пленка одностенных углеродных нанотрубок (ОУНТ) состоит из переплетенных нанотрубок, каждая из которых характеризуются своими свойствами, такими как диаметр, длина, хиральность и т.д. Однако пленку ОУНТ можно рассматривать, как целостный объект, что упрощает интерпретацию данных [1]. Перспективной для оптоэлектроники является гетероструктура пленка ОУНТ/кремний, зарядовые свойства которой рассматриваются в данной работе. В работах последнего десятилетия продемонстрирована перспективность использования гетеропереходов ОУНТ/кремний в качестве солнечных элементов для преобразования энергии, а также эффективных сверхбыстрых широкополосных фотодетекторов [2].

На поверхности пленки ОУНТ в процессе формирования возникают различные ловушки носителей заряда. В основном они вызваны адсорбцией ионов кислорода O^-, что обеспечивает *n*-тип проводимости ОУНТ [1,3].

Основная часть

Моделирование проводилось в программном пакете Comsol Multyphysics на основании модели Андерсона для полупроводниковых гетеропереходов, решения уравнения Пуассона, уравнений непрерывности для электронов и дырок и уравнений Максвелла для электромагнитных волн. В данной работе рассматривается

гетероструктура пленка ОУНТ на кремнии. Целью данной работы является моделирование зарядовых свойств гетероструктуры пленка ОУНТ толщиной d от 10 нм до 50 нм на кремниевой подложке толщиной 2 мкм. В процессе формирования пленки ОУНТ на кремнии образуется тонкий слой оксида кремния SiO_2, в исследуемой модели толщина слоя SiO_2 составляла 2 нм.

Для ОУНТ, кремния и оксида кремния задавался комплексный показатель преломления, его действительная n и мнимая k части [4,5,6]. Для кремния n = 3,717 и k=0,008, для пленки ОУНТ n=1,59697 и k=0,49209, для оксида кремния n = 1,46 и k=0,0019.

На поверхности ОУНТ также были заданы ловушечные состояния донорного типа плотностью 10^{12} см$^{-2}$ и с энергией E_t от 0 до 0,1 эВ считая от дна зоны проводимости [1], в объеме SiO_2 были заданы ловушечные состояния донорного типа плотностью 10^{12} см$^{-3}$ и энергией 0,34 эВ считая от дна зоны проводимости [7]. Вероятность захвата носителей заряда ловушками на поверхности пленки ОУНТ и в объеме SiO_2 задавалась через среднее эффективное значение сечения захвата, $1{,}913\cdot10^{-12}$ см^2 и $2{,}838\cdot10^{-12}$ см^2 соответственно [8].

Плотность мощности излучения равна 1 кВт/м^2, длина волны падающего на гетероструктуру излучения 750 нм, температура 300 К. Использованные при моделировании параметры материалов представлены в таблице.

Таблица 1. Свойства материалов
Table 1. Materials properties

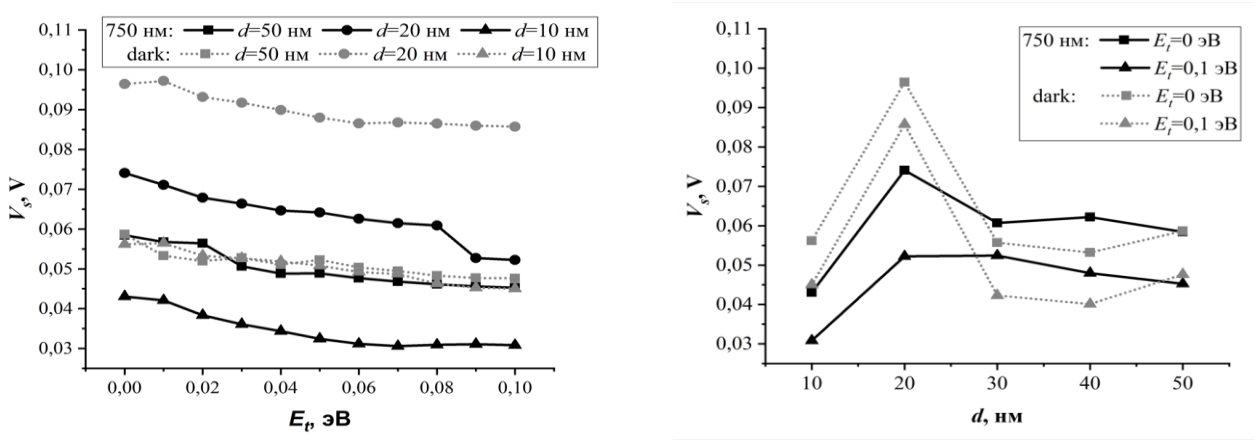
	n-Si	SiO_2	n-ОУНТ
Ширина запрещенной зоны, эВ	1,124	9	0,6
Сродство к электрону, эВ	4,05	0,75	4,2
Относительная диэлектрическая проницаемость	11,7	3,9	4,75
Время жизни электронов, мкс	10	0,012	0,0004
Время жизни дырок, мкс	10	0,012	0,0004
Концентрация примеси, см$^{-3}$	10^{16}	-	10^{18}
Подвижность электронов, см^2/(В·с)	1450	21	56
Подвижность дырок, см^2/(В·с)	500	0,0001	56

Под воздействием излучения наблюдалась генерация носителей заряда в гетероструктуре. При толщине пленки ОУНТ d = 50 нм на поверхности пленки скорость генерации носителей заряда на поверхности пленки составила $4{,}42\cdot10^{15}$см$^{-3}$с$^{-1}$, в кремниевой подложке на границе разделения с пленкой ОУНТ составляла $7{,}9\cdot10^{15}$см$^{-3}$с$^{-1}$. С уменьшением толщины пленки d до 10 нм скорость генерации носителей заряда на поверхности пленки монотонно уменьшалась до $2{,}21\cdot10^{15}$см$^{-3}$с$^{-1}$ и увеличивалась до $1{,}16\cdot10^{16}$см$^{-3}$с$^{-1}$, соответственно.

Поверхностная плотность электрического заряда σ на пленке ОУНТ не зависит от наличия падающего излучения или его отсутствия, но монотонно убывает от значения $\sigma=2{,}05\cdot10^{-2}$мкКл/см^2 до $1{,}09\cdot10^{-3}$мкКл/см^2 при росте энергии E_t от 0 В до 0,1 В.

Зависимости электрического потенциала V_s на поверхности пленки от энергии ловушечных состояний и от толщины d пленки в условиях наличия падающего излучения и при его отсутствии представлены на рис. 1, *a* и *b*, соответственно.

Из рис. 1, *a* видно, что потенциал V_s монотонно убывает с ростом энергии ловушек E_t при всех толщинах d пленки ОУНТ. Из рис. 1, *b* видно, что максимум электрического потенциала V_s приходится на толщину пленки d = 20 нм. Максимальное различие электрического потенциала V_s при отсутствии падающего излучения и при его наличии равное 33,5 мВ выявлено для толщины пленки d = 20 нм и для энергии E_t = 0,1 эВ. При наличии излучения V_s = 52,2 мВ, а при его отсутствии V_s=85,7 мВ.



a *b*

Рис. 1. Электрический потенциал V_s на поверхности пленки ОУНТ при наличии излучения и при его отсутствии (dark): *a* – от энергии E_t для различных толщин пленки *d*; *b* – от толщины пленки *d* для различных значений энергии E_t

Fig. 1. Electric potential V_s on the surface of the SWCNT film in the presence and absence of radiation (dark): *a* – from energy E_t for different film thicknesses *d*; *b* – from film thickness *d* for different values of energy E_t

Для объяснения полученных результатов были построены энергетические диаграммы гетероструктур по оси перпендикулярной поверхности пленки ОУНТ. При энергии ловушек E_t=0,1 эВ максимальное значение разрыва дна зоны проводимости в кремнии и пленке ОУНТ приходится на толщину пленки d = 20 нм и равняется 0,16047 эВ в условиях наличия излучения и 0,169 эВ в условиях его отсутствия. При других толщинах пленки *d* данный разрыв составил 0,15578–0,16042 эВ и 0,158–0,167 эВ при наличии и отсутствии излучения. Плотность пространственного заряда в пленке ОУНТ вблизи границы раздела Si/ОУНТ также оказалась максимальной при d = 20 нм и составляла 47 и 26,2 мКл/см$^{-3}$, соответственно.

Заключение

Результаты проведенного моделирования гетероструктуры продемонстрировали, что уменьшение толщины пленки *d* до 20 нм и использование пленки ОУНТ с высокой энергией ловушечных состояний на поверхности дает возможность выявить наличие падающего на гетероструктуру пленка ОУНТ/кремний излучения длиной волны 750 нм за счет различия в значении электрического потенциала на поверхности пленки ОУНТ, что может быть использовано при разработке детекторов ИК излучения с контролируемой концентрацией ловушек.

Список использованных источников

1. Kumar R., Khan M.A., Anupama A.V., Krupanidhi S.B., Sahoo B. (2021) Infrared photodetectors based on multiwalled carbon nanotubes: Insights into the effect of nitrogen doping. *Applied Surface Science*. 538, 148187-148197.

2. Hu X, Hou P., Liu C., Cheng H. (2019) Carbon nanotube/silicon heterojunctions for photovoltaic applications. *Nano Materials Science*. 1(3), 156–172.

3. Algharagholy L.A. (2019) Defects in carbon nanotubes and their impact on the electronic transport properties. *Journal of Electronic Materials*. 48(4), 2301–2306.

4. Green M. A. Self-consistent optical parameters of intrinsic silicon at 300K including temperature coefficients. (2008) *Solar Energy Materials & Solar Cells.* 92, 1305-1310.

5. Ermolaev G.A., Tsapenko A.P., Volkov V.S., Anisimov A.S., Gladush Y.G., Nasibulin A.G. (2020) Express determination of thickness and dielectric function of single-walled carbon nanotube films. *Applied Physics Letters.* 116, 231103-231107.

6. Rodríguez-de Marcos L. V., Larruquert J. I., Méndez J. A., Aznárez J. A. (2016) Self-consistent optical constants of SiO_2 and Ta_{15} films. *Optical Materials Express*. 6(11), 3622-3637.

7. Дементьев П.А., Иванова Е. В., Заморянская М. В. (2019) Ловушки в нанокомпозитном слое кремний-диоксид кремния и их влияние на люминесцентные свойства. *Физика твердого тела*. 61(8), 1448-1454.

8. Поклонский Н. А., Горбачук Н. И., Сягло А. И., Шпаковский С. В. (2009) *Исследование переходных процессов в полупроводниковых структурах : пособие*. Минск, БГУ.

References

1. Kumar R., Khan M.A., Anupama A.V., Krupanidhi S.B., Sahoo B. (2021) Infrared photodetectors based on multiwalled carbon nanotubes: Insights into the effect of nitrogen doping. *Applied Surface Science*. 538, 148187-148197.

2. Hu X, Hou P., Liu C., Cheng H. (2019) Carbon nanotube/silicon heterojunctions for photovoltaic applications. *Nano Materials Science*. 1(3), 156–172.

3. Algharagholy L.A. (2019) Defects in carbon nanotubes and their impact on the electronic transport properties. *Journal of Electronic Materials*. 48(4), 2301–2306.

4. Green M. A. Self-consistent optical parameters of intrinsic silicon at 300K including temperature coefficients. (2008) *Solar Energy Materials & Solar Cells.* 92, 1305-1310.

5. Ermolaev G.A., Tsapenko A.P., Volkov V.S., Anisimov A.S., Gladush Y.G., Nasibulin A.G. (2020) Express determination of thickness and dielectric function of single-walled carbon nanotube films. *Applied Physics Letters.* 116, 231103-231107.

6. Rodríguez-de Marcos L. V., Larruquert J. I., Méndez J. A., Aznárez J. A. (2008) Self-consistent optical constants of SiO2 and Ta15 films. *Optical Materials Express*. 6(11), 3622-3637.

7. Dement'ev, P. A.; Ivanova, E. V., Zamoryanskaya, M. V. (2019) Traps in the Nanocomposite Layer of Silicon–Silicon Dioxide and Their Effect on the Luminescent Properties. Physics of the Solid State, 61(8), 1394–1400.

8. Poklonskij N. A., Gorbachuk N. I., Sjaglo A. I., Shpakovskij S. V. (2009) *Study of transient processes in semiconductor structures: manual*. Minsk, BSU (in Russian).

Сведения об авторах

Курапцова А.А., младший научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», anku21qwerty@gmail.com.
Данилюк А.Л., кандидат физико-математических наук, доцент, ведущий научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danilyuk@bsuir.by.

Information about the authors

Kuraptsova A.A., junior researcher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", anku21qwerty@gmail.com.
Danilyuk A.L., PhD in Physics and Mathematics, Associate Professor, Leading Researcher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", danilyuk@bsuir.by.

УДК 004.056.5

СТАТИСТИЧЕСКИЙ АНАЛИЗ КОНЕЧНЫХ ГРУПП И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

В.Н. Кутин, В.А. Молчанов
Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, Саратов, Россия

Аннотация. В современной криптографии при построении криптографических примитивов, криптосистем и протоколов особое внимание уделяется использованию алгебраических структур, в частности, конечных групп. Группы играют ключевую роль в разработке эффективных и устойчивых к атакам криптосистем, обеспечивая математическую основу для широко применяемых криптографических схем.

Ключевые слова: конечная группа; треугольные матрицы; порядок элементов.

STATISTICAL ANALYSIS OF FINITE GROUPS AND THEIR APPLICATION IN CRYPTOGRAPHY

V.N. Kutin, V.A. Molchanov
Saratov National Research State University named after N. G. Chernyshevsky, Saratov, Russia

Abstract. In modern cryptography, when building cryptographic primitives, cryptosystems and protocols, special attention is paid to the use of algebraic structures, in particular, finite groups. The groups play a key role in the development of effective and attack-resistant cryptosystems, providing the mathematical basis for widely used cryptographic schemes.
Keywords: finite group; triangular matrices; order of elements.

Введение

Настоящая работа посвящена исследованию возможностей применения конечных групп в криптографии, включая их использование в построении криптосистем, основанных на сложных алгоритмических проблемах. Особый интерес представляют задачи, связанные с вычислительной сложностью поиска порядков элементов и проблемой дискретного логарифма в конечных группах, которые находят применение как в классической, так и в пост-квантовой криптографии.

Основная часть

Данная работа является продолжением исследований [1]. В рамках текущего исследования был проведен статистический анализ сгенерированных конечных групп верхне-треугольных матриц с элементами над полем $\mathbb{Z}_p$ (p-простое число) [2]. Также исследовалась структура этих групп, распределение порядков их элементов, а также их подгруппы. Полученные статистические характеристики позволили провести сравнительное исследование алгебраических свойств таких групп и оценить их возможное применение в криптографических и вычислительных задачах.

Выбор верхне-треугольных матриц с элементами над полем $\mathbb{Z}_p$ и ненулевым определителем, в качестве элементов множества, позволяет построить конечную группу с гарантированно обратимыми элементами. Таким образом используя свойство обратимости элементов полученной группы, был применен эффективный алгоритм Гельфонда – Шенкса для вычисления порядков элементов сгенерированной группы [3].

Были рассмотрены следующие конечные группы верхне-треугольных матриц:

1. Группа верхне-треугольных матриц размерностью 3 на 3, с элементами над полем $\mathbb{Z}_{11}$.

2. Группа верхне-треугольных матриц размерностью 3 на 3, с элементами над полем $\mathbb{Z}_{13}$.

3. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{19}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 6 \\ 0 & 3 & 9 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 7 & 12 \\ 0 & 3 & 9 \\ 0 & 0 & 9 \end{pmatrix}.$$

4. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{19}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 14 \\ 0 & 12 & 9 \\ 0 & 0 & 14 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 7 & 12 \\ 0 & 3 & 9 \\ 0 & 0 & 9 \end{pmatrix}.$$

5. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{23}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 6 \\ 0 & 3 & 1 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 12 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 17 \end{pmatrix}.$$

Для каждой пронумерованной выше группы и подгруппы были получены списки частот порядков элементов (в скобках указаны частоты):

1. 1(1), 2(727), 5(87124), 10(903148), 11(1330), 22(8590), 55(77920), 110(252160).

2. 1(1), 2(1015), 3(16226), 4(57800), 6(261614), 12(2630320), 13(2196), 26(14364), 39(40896), 52(65232), 78(138240), 156(568512).

3. 1(1), 2(361), 3(15884), 6(41876), 9(376884), 18(454860), 19(6858), 38(6498), 57(38988), 114(12996), 171(116964), 342(38988).

4. 1(1), 2(723), 3(15884), 6(99636), 9(376884), 18(1286604), 19(6858), 38(19854), 57(38988), 114(64980), 171(116964), 342(194940).

5. 1(1), 2(529), 11(1110900), 22(1343660), 23(12166), 253(349140), 506(116380).

В частности, были получены статистические характеристики: математическое ожидание, дисперсия, среднее квадратическое отклонение, сгенерированных групп и подгрупп, приведенные в Таблице 1, также распределения частот порядков преобразований, изображенных на Рисунке 1. Полученные распределения прошли тест Д'Агостино-Пирсона на нормальность, результаты тестов также приведены также в Таблице 1 [4]. Также согласно Рисунку 1, очевидно, что ядерные оценки плотности частот порядков элементов для групп близки нормальной кривой Гаусса.

Таблица 1. Статистические характеристики частот порядков элементов сгенерированных групп верхне-треугольных матриц, тестирование распределений полученных частот на нормальность тестом Пирсона (уровень значимости $a = 0.05$)

Table 1. Statistical characteristics of the frequencies of the orders of elements of the generated groups of upper triangular matrices, testing the distributions of the obtained frequencies for normality using the Pearson test (significance level $a = 0.05$)

№	Макс. порядок	Матем. ожидание	Дисперсия	Ср. кв. отклонение	Кол-во эл-тов	p-значние	Норм. Распр. p > 0.05
1	110	221833	99644311023	315664.87	1331000	0,0675	Да
2	156	474552	693883385533	832996.63	3796416	0,0738	Да
3	342	136458	27981412518	167276.46	1111158	0,1476	Да
4	342	259920	151540536440	389282.08	2222316	0,0677	Да
5	506	735353	1011289260182	1005628.79	2944414	0,1122	Да

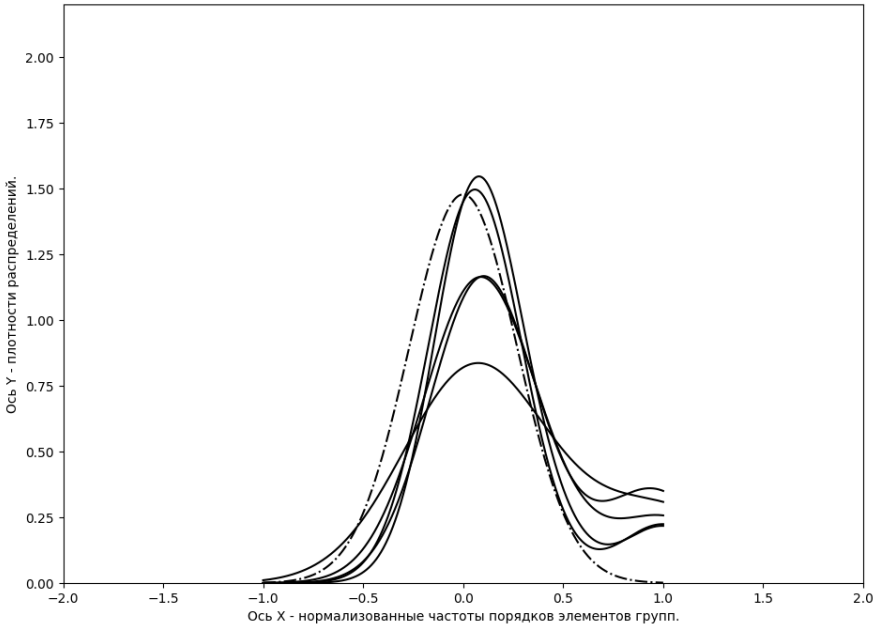


Рис. 1. Ядерные оценки плотности частот порядков элементов групп верхне-треугольных матриц (штрихпунктирный график – стандартная кривая Гаусса, черные графики – распределения частот)
Fig. 1. Nuclear estimates of the frequency density of the orders of elements of groups of upper triangular matrices (dotted line graph is the standard Gauss curve, black graphs are frequency distributions)

Заключение

В данной работе был проведен статистический анализ конечных групп верхне-треугольных матриц 3×3 с элементами над полями $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{19}$, $\mathbb{Z}_{23}$. Полученные результаты позволили изучить структуру этих групп, распределение порядков их элементов и выявить свойства их подгрупп. Анализ показал, что распределения порядков элементов таких групп обладают характеристиками, близкими к нормальному распределению Гаусса, что подтверждено тестом Д'Агостино-Пирсона.

Список использованных источников

1. Кутин В.Н., Молчанов В.А. Статистический анализ конечных полугрупп и их применение в криптографии / В.Н. Кутин, В.А. Молчанов // Технические средства защиты информации : тез. докл. XXI Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 6 июня 2023 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2023. – 104 с.

2. Гантмахер Ф.Р. . Теория матриц. 4-е изд. – М.: Наука, 1988. – 552 с. – ISBN 5-02-013722-7.

3. Панкратова И. А. Теоретико-числовые методы в криптографии: Учебное пособие. – Томск: ТГУ, 2009. – С. 90-98. – 120 с.

4. Кобзарь А. И. Прикладная математическая статистика. – М.: Физматлит, 2006. – с. 258.

References

1. Kutin V.N., Molchanov V.A. Statistical analysis of finite semigroups and their application in cryptography / V.N. Kutin, V.A. Molchanov // Technical means of information protection : thesis of the XXI Belarusian-Russian Scientific and Technical conference (Republic of Belarus, Minsk, June 6, 2023) / editor : T. V. Borbotko [et al.]. – Minsk : BGUIR, 2023. – 104 p.

2. Gantmacher F.R. Theory of matrices. 4th ed.– Moscow: Nauka, 1988– 552 p. ISBN 5-02-013722-7.

3. Pankratova I. A. Theoretical and numerical methods in cryptography: A textbook. Tomsk: TSU, 2009. pp. 90-98. 120 p.

4. Kobzar A. I. Applied Mathematical statistics, Moscow: Fizmatlit, 2006, p. 258.

Сведения об авторах

Кутин В.Н., аспирант кафедры теоретических основ компьютерной безопасности и криптографии, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, qooteen@mail.ru.
Молчанов В.А., доктор физ.-мат.наук, профессор, профессор кафедры теоретических основ компьютерной безопасности и криптографии, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, v.molchanov@inbox.ru.

Information about the authors

Kutin V.N., Postgraduate student of the Department of Theoretical Foundations of Computer Security and Cryptography, Saratov National Research State University named after N. G. Chernyshevsky, qooteen@mail.ru.
Molchanov V.A., Doctor of Physical and Mathematical Sciences, Professor, Professor of the Department of Theoretical Foundations of Computer Security and Cryptography, Saratov National Research State University named after N. G. Chernyshevsky, v.molchanov@inbox.ru.

УДК 538.945

ФОНОНЫ 3D КРИСТАЛЛА, ИНДУЦИРОВАННЫЕ 2D КРИСТАЛЛОМ

В.Н. Кушнир
Белорусский государственный университет, Минск, Беларусь

Аннотация. В данной работе представлена концепция "сгущения" фононных мод сверхпроводящего материала с покрытием из графена. Двуслойный и твистированный заданным образом графен может обладать спектром акустических фононов, поляризованных ортогонально поверхности, почти полностью перекрывающимся с фононным спектром сверхпроводящего материала. В результате взаимодействия сверхпроводника (ниобия) с акустической ортогонально-поляризованной ветвью графена частотный спектр всей структуры модифицируется, но при этом сохраняется полное число фононных мод, распространяющихся как в ниобии, так и в графене. Ввиду слабого взаимодействия 3D и 2D кристаллов полагаем, что частотный диапазон нормальных колебаний кристаллической решетки ниобия изменяется достаточно слабо. Это приводит к увеличению числа нормальных колебаний в ниобии за счет привнесенных мод. В итоге имеем увеличение эффективной константы электрон-фононного взаимодействия, что означает увеличение критической температуры.
Ключевые слова: сверхпроводимость; ниобий; графен; динамическая матрица; секулярное уравнение; собственные частоты; нормальные колебания; поляризация; критическая температура; электрон-фононное взаимодействие.

PHONONS IN 3D CRYSTAL INDUCED BY 2D CRYSTAL

V.N. Kushnir
Belarusian State University, Minsk, Republic of Belarus

Abstract. In this paper, we present a concept of "thickening" the phonon modes of a graphene-coated superconducting material. Bilayer graphene twisted in a given manner can have a spectrum of acoustic phonons polarized orthogonally to the surface, which almost completely overlaps with the phonon spectrum of the superconducting material. As a result of the interaction of the superconductor (niobium) with the acoustic orthogonally polarized branch of graphene, the frequency spectrum of the entire structure is modified, but the total number of phonon modes propagating in both niobium and graphene is preserved. Due to the weak interaction of 3D and 2D crystals, we believe that the frequency range of normal vibrations of the niobium crystal lattice changes quite weakly. This leads to an increase in the number of normal vibrations in niobium due to the introduced modes. As a result, we have an increase in the effective constant of the electron-phonon interaction, which means an increase in the critical temperature.
Keywords: superconductivity; niobium; graphene; dynamic matrix; secular equation; eigen frequencies; normal vibrations; polarization; critical temperature; electron-phonon interaction.

Введение

Очевидно, элементы устройств сверхпроводниковой наноэлектроники и спинтроники должны обладать стабильными характеристиками. Между тем, как раз

для рабочих (нанометровых) толщин сверхпроводящих пленок наблюдаются наибольшие вариации критической температуры [1]. В связи с этим трудно переоценить значение обнаруженного эффекта стабилизации критической температуры тонкой пленки Nb при нанесении на нее графенового (G) покрытия [2]. Природа этого эффекта, казалось бы, очевидна: акустические фононные моды графена распространяются в ниобии; в результате плотность числа фононных состояний увеличивается; это приводит к увеличению эффективной константы электрон-фононного взаимодействия в сверхпроводнике (S), что, в свою очередь, влечет рост критической температуры. Между тем последовательное объяснение эффекта с позиции динамической теории кристаллической решетки оказывается крайне сложным. Здесь мы систематизируем основные положения нашей трактовки эффекта.

Основная часть

Пленку Nb с графеновым покрытием можно рассматривать как структуру S/I/G, где I – разупорядоченный диэлектрик, образованный различными окислами Nb. I-прослойка играет как пассивную роль, увеличивая расстояние между атомами углерода и ниобия, так и создает хаотические воздействия на них. В итоге рассматриваем структуру как слабо взаимодействующие 3D и 2D кристаллы. Полагаем, что воздействие 2D кристалла реализуется посредством распространения фононов, поляризованных в ортогональном поверхности направлении [2,3] (см. также ссылки в [2,3]). В результате такой редукции динамика кристалла Nb с графеновым покрытием будет определяться задачей на собственные векторы и собственные значения

$$\begin{pmatrix} D_{Nb} & D_{Nb,G} \\ D_{G,Nb} & D_G \end{pmatrix}\begin{pmatrix} X_{Nb} \\ X_G \end{pmatrix} = \lambda \begin{pmatrix} X_{Nb} \\ X_G \end{pmatrix}, \quad (1)$$

где D_{Nb} – динамическая матрица Nb, и D_G – *редуцированная* матрица 2-мерного кристалла, $D_{Nb,G}$ – матрица взаимодействия, X_{Nb} и X_G – соответствующие вектор-столбцы отклонений от положений равновесия, λ – собственные значения, определяемые из секулярного уравнения.

Далее выполним «частичную» диагонализацию матрицы в левой части уравнения (1). А именно, представим матрицы слоев в виде

$$D_{Nb} = S_{Nb}\Lambda_{Nb}S_{Nb}^{+}, \quad (2)$$

$$D_G = S_G\Lambda_G S_G^{+}, \quad (3)$$

где $\Lambda_{Nb(G)}$ – диагональные матрицы из собственных значений для слоя Nb(G), а $S_{Nb(G)}$ – соответствующие унитарные матрицы из собственных векторов.
После этого система (1) преобразуется к виду

$$\begin{pmatrix} \Lambda_{Nb} - \lambda & V_{Nb,G} \\ V_{G,Nb} & \Lambda_G - \lambda \end{pmatrix}\begin{pmatrix} Y_{Nb} \\ Y_G \end{pmatrix} = 0, \quad (4)$$

где вектор-столбцы Y_{Nb} и Y_G получены из вектор-столбцов X_{Nb} и X_G соответствующими унитарными преобразованиями, преобразованные матрицы взаимодействия заданы формулами

$$V_{Nb,G} = S_{Nb}^{+}D_{Nb,G}S_G, \quad (5)$$

$$V_{G,Nb} = S_G^{+} D_{G,Nb} S_{Nb}\,. \qquad (6)$$

Легко видеть, что уравнения (4) сводятся к уравнениям Дайсона, однако здесь мы акцентируем внимание на следующих элементарных фактах. Из структуры (4) следует: во-первых, число мод в 3D-кристалле увеличивается на число колебательных степеней свободы в ортогональном направлении 2D-кристалла плюс трансляционные моды (их количество равно числу слоев графена); во-вторых, следует полагать, что процесс генерации дополнительных мод оказывается не затухающим, поскольку амплитуда колебаний атомов углерода в графене содержит фактор $(M_{Nb}/M_C)^{1/2}$, где M_{Nb} и M_C – массы соответствующих атомов. Совсем не очевидным, между тем, является факт увеличения плотности числа фононных состояний. Здесь играют роль два обстоятельства: во-первых, спектр акустических мод графена, поляризованных в ортогональном поверхности направлении почти полностью перекрывается с фононным спектром ниобия; во-вторых, существенна (что, на первый взгляд, достаточно странно) слабость взаимодействия 3D и 2D кристаллов – следует полагать, что максимальные возмущенная и невозмущенная частоты в 3D кристалле мало отличаются друг от друга [3]. Этим как раз и следует объяснить эффект, полученный численно в [2] для одномерной цепочки, дополненной легкими атомами.

Заключение

Таким образом, в рамках представленной концепции «сгущения фононных мод» сверхпроводника вполне приемлемо объясняются экспериментальные данные, приведенные в [2].

Список использованных источников

1. Кушнир В.Н. (2010) *Сверхпроводимость слоистых структур*. Минск, Издательство БНТУ.
2. Prischepa S.L., Kushnir V.N., Cirillo C., Granata V., Komissarov I.V., Kovalchuk N.G., et al. (2021) Superconducting Critical Temperature and Softening of the Phonon Spectrum in Ultrathin Nb and NbN/Graphene Hybrids. *Superconductor Science and Technology*. *IOP*. 34, 115021-1–15.
3. Prischepa S.L., Kushnir V.N. (2023) Phonon softening in nanostructured phonon–mediated superconductors (review). *Journal of Physics*: *Condensed matter*. *IOP*. 35, 313003-1–54.

References

1. Kushnir V.N. (2010) *Superconductivity of Layered Structures*. Minsk, BNTU Publishing (in Russian).
2. Prischepa S.L., Kushnir V.N., Cirillo C., Granata V., Komissarov I.V., Kovalchuk N.G., et al. (2021) Superconducting Critical Temperature and Softening of the Phonon Spectrum in Ultrathin Nb and NbN/Graphene Hybrids. *Superconductor Science and Technology*. *IOP*, 34, 115021-1–15.
3. Prischepa S.L., Kushnir V.N. (2023) Phonon softening in nanostructured phonon–mediated superconductors (review). *Journal of Physics*: *Condensed matter*. *IOP*. 35, 313003-1–54.

Сведения об авторе

Кушнир В.Н., д-р физ.-мат наук, доц., проф., Белорусский государственный университет, vnkushnir@gmail.com.

Information about the author

Kushnir V.N., Dr. Sci. (Phys. Mat.), Associate Professor, Professor, Belarusian State University, vnkushnir@gmail.com.

УДК 004.056

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ АТАКАМ ТИПА BADUSB

А.А. Лебедев
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В последнее время число подключаемых в компьютер устройств возросло. Вместе с ними возрос риск, что в одном из USB устройств будет вшит вредоносный код. Атака BadUSB представляет собой серьезную угрозу для информационной безопасности. Данный тип атаки может быть использован как для кражи, так и для уничтожения информации и получения неавторизованного доступа к системе. BadUSB часто используется теми, кто уже имеет физический доступ к системе, однако нередко это происходит и по неосторожности самих сотрудников компании. В этой статье приведены угрозы что может представлять атака BadUSB, концепция данной атаки, а также возможные защитные решения.
Ключевые слова: BadUSB; уязвимость; манипуляция, микроконтроллер, Arduino.

METHODS TO COUNTER BADUSB ATTACKS

A.A. Lebedev
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Recently, the number of devices connected to a computer has increased. Along with them, the risk has increased that malicious code will be embedded in one of the USB devices. The BadUSB attack poses a serious threat to information security. This type of attack can be used to steal or destroy information and gain unauthorized access to the system. BadUSB is often used by those who already have physical access to the system, but this often happens due to the negligence of the company's employees themselves. This article describes the threats that a BadUSB attack can pose, the concept of this attack, as well as possible defensive solutions.
Keywords: BadUSB; vulnerability; data theft; manipulation, microcontroller, Arduino.

Введение

BadUSB – это обобщенное название класса атак, основанных на эксплуатации уязвимостей USB-протоколов и архитектуры USB-устройств [1]. Атака связана с изменением прошивки устройства таким образом, чтобы оно имитировало другое устройство (например, клавиатуру), выполняло вредоносные команды или вмешивалось в работу компьютера (рис. 1). Успех атаки достигается путем скрытного проникновения на объект, атаки на внимательность жертвы либо ее отвлечения. С развитием технологий и увеличением числа подключаемых периферийных устройств эта угроза становится все более актуальной.

Основная часть

Основная проблема BadUSB заключается в том, что большинство современных операционных систем доверяют устройствам, подключаемым через USB-порт, предоставляя им высокий уровень привилегий. Отсюда следуют риски:

1. Потеря контроля над системой. После подключения BadUSB злоумышленник может удаленно управлять компьютером, запускать произвольные программы, изменять настройки системы или устанавливать вредоносное ПО.

2. Кража данных. Устройство может перехватывать нажатия клавиш, пароли, файлы или другие конфиденциальные данные, передавая их на сервер атакующего.

3. Распространение инфекции. При наличии NAND памяти, зараженное BadUSB-устройство способно распространять вредоносное ПО на другие компьютеры и сети, превращаясь в вектор распространения угроз.

4. Скрытность. Традиционные антивирусы не способны выявить такие устройства, поскольку они действуют на уровне аппаратного взаимодействия между устройством и операционной системой.

На практике, подготовить USB устройство для реализации атаки такого типа (рис. 1) довольно легко.

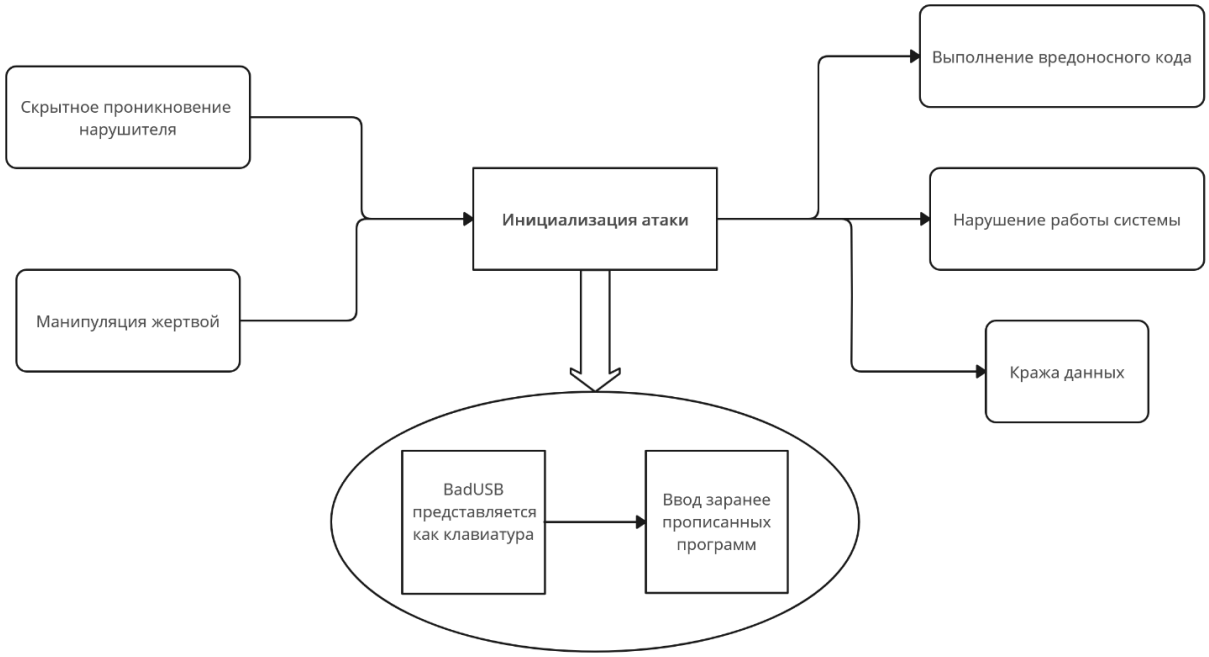


Рис. 1. Принцип атаки BadUSB
Fig. 1. The principle of the BadUSB attack

Все, что потребуется, это плата с микропроцессором (например, Arduino Leonardo в корпусе, замаскированным под USB носитель), среда для прошивки микроконтроллера (Arduino IDE), знание языка программирования данной среды, командной строки/powershell на целевой машине, и базовое понимание работы операционных систем, исполняемых ими файлов и системных процессов. Ввиду доступности всех вышеизложенных компонентов в сети Интернет, сделать себе подобное устройство сможет немало людей. Это пример простой атаки, однако даже такой подход сможет причинить большой вред системе, если команды, которые будет воспроизводить микроконтроллер, будут составлены грамотно.

Однако для защиты от такого типа атаки есть решение, представленное на рис.2. Суть заключается в запуске фонового процесса, который, в момент обнаружения подключения нового USB устройства, запускает сканер аномальной активности. В программе прописаны сценарии, что чаще всего выполняются при подключении BadUSb, такие как нажатие комбинации клавиш Win+R, ввод строки «cmd», и другие. При обнаружении демаскирующих признаков, программа сбрасывает фокус с активного окна, чтобы не дать дописать опасную команду, и, по возможности, извлекает это устройство. А поскольку данный тип BadUSB фактически имитирует клавиатуру, то работает, как и клавиатура, только в активном окне.

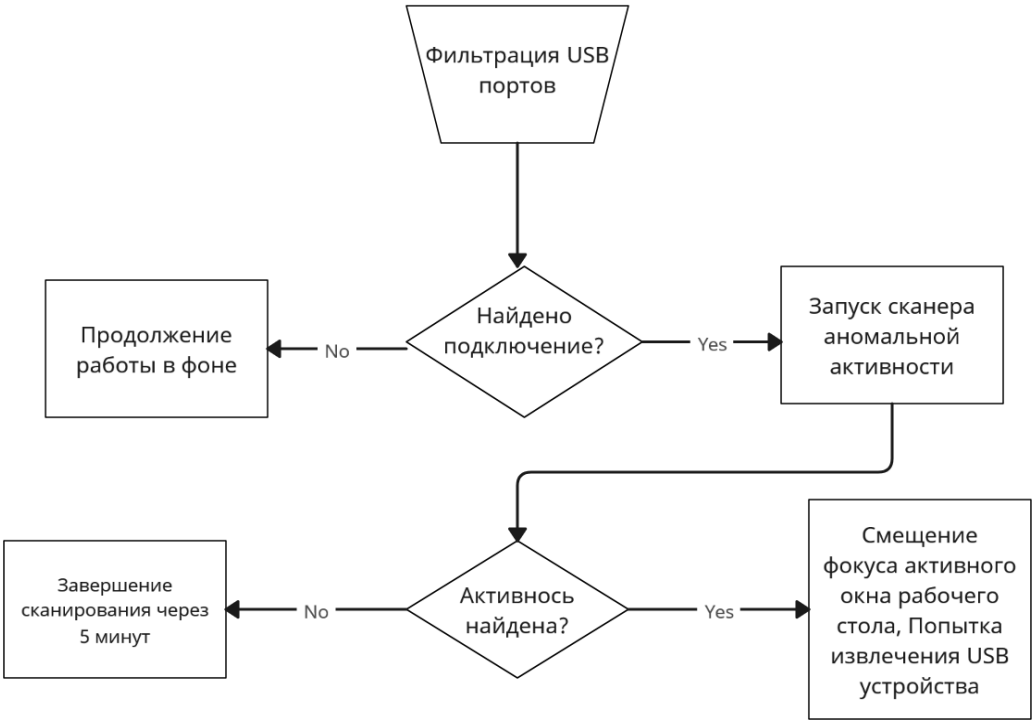


Рис. 2. Логическая схема работы защитного ПО
Fig. 2. The logical scheme of the security software operation

Таким образом, даже простое подключение зараженного USB-накопителя может привести к серьезным последствиям для безопасности информационной системы. Для минимизации рисков успешных атак BadUSB других типов, таких как, например, перепрошитые сетевые карты, можно также использовать и другие решения:

1. Контроль доступа к портам USB. Один из способов – ограничить возможность подключения неизвестных устройств через USB-порты. Это можно сделать на уровне BIOS/UEFI или с помощью специализированных программных решений, которые требуют подтверждения подключения от пользователя.

2. Фильтрация типов устройств. Современные операционные системы могут фильтровать типы подключаемых устройств, блокируя доступ таким потенциально опасным категориям, как клавиатуры или сетевые карты.

3. Мониторинг активности. Специализированные программы могут отслеживать аномальную активность USB-устройств, выявляя попытки эмуляции клавиатурных команд или несанкционированного доступа к сети.

4. Аппаратные решения. Разработка USB-концентраторов с функцией проверки подлинности устройств и предоставления им доступа к системе также является перспективным направлением. Такие концентраторы могут проверять цифровые подписи или идентификаторы устройств, обеспечивая дополнительный уровень защиты [2].

5. Ограничение прав на выполнение команд. Ограничение прав пользователя на компьютере минимизирует ущерб, который может нанести BadUSB, так как немало атак требуют повышенных привилегий. Даже если устройство успешно инициализировано в системе, ограничение прав может предотвратить выполнение критически важных действий, что актуально для Unix-систем.

Заключение

BadUSB представляет собой серьезную угрозу для безопасности информационных систем. Ее доступность, высокая скрытность и способность обходить традиционные средства защиты делают эту атаку особенно опасной. Для предотвращения последствий BadUSB необходимы комплексные меры, включающие технические решения, повышение уровня осведомленности пользователей и строгие политики управления устройствами. Сочетание всех этих мер позволит существенно снизить риски, связанные с данным типом атак.

Список использованных источников / References

1. Nohl K., Lell J. BadUSB –On Accessories that Turn Evil. Black Hat USA.
2. Mitigation Strategies for BadUSB Attacks. Security Week, 2019.

Сведения об авторе

Лебедев А.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexandercorp77@gmail.com.

Information about the author

Lebedev A.A., student of the faculty of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexandercorp77@gmail.com.

УДК 004.6

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ДАННЫХ

М.В. Логвинович, С.А. Мигалевич
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Блокчейн-технологии обладают большим потенциалом в сфере здравоохранения, обеспечивая децентрализованное и безопасное хранение медицинских данных. Традиционные централизованные системы часто сталкиваются с проблемами утечек и несанкционированного доступа, что делает блокчейн перспективным решением. В статье рассматривается интеграция блокчейна с IPFS для хранения медицинских записей и применение модели управления доступом на основе атрибутов (ABAC). Предложенный подход позволяет повысить безопасность, прозрачность и эффективность обмена медицинской информацией между учреждениями.
Ключевые слова: блокчейн; здравоохранение; медицинские данные; безопасность; децентрализованное хранение; IPFS; атрибутивное управление доступом; защита конфиденциальности; прозрачность; обмен данными.

APPLICATION OF BLOCKCHAIN TO ENSURING PRIVACY AND SECURITY OF MEDICAL DATA

M.V. Logvinovich, S.A. Migalevich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Blockchain technology has great potential in the healthcare sector, providing decentralized and secure storage of medical data. Traditional centralized systems often face issues of data breaches and unauthorized access, making blockchain a promising solution. This paper discusses the integration of blockchain with IPFS for medical record storage and the application of Attribute-Based Access Control (ABAC). The proposed approach enhances security, transparency, and the efficiency of medical data exchange between institutions.
Keywords: blockchain; healthcare; medical data; security; decentralized storage; IPFS; attribute-based access control; privacy protection; transparency; data exchange.

Введение

С развитием технологий блокчейн находит все большее применение в сфере здравоохранения, обеспечивая децентрализованное и безопасное хранение медицинских данных. Централизованные системы хранения подвержены угрозам утечек и нарушений конфиденциальности, что требует перехода к более безопасным и эффективным методам. Блокчейн, благодаря своей дистрибутивной структуре, обеспечивает неизменность данных и их защиту от подделки. Интеграция смарт-контрактов и моделей доступа на основе атрибутов (ABAC) позволяет не только повысить безопасность, но и внедрить точный контроль доступа к медицинской информации. Это позволяет эффективно управлять данными, минимизируя риски и улучшая качество обслуживания пациентов [1].

Основная часть

В условиях быстрорастущего объема медицинской информации и возрастающих угроз кибербезопасности, переход к более защищенным и эффективным методам хранения данных становится необходимостью. Блокчейн представляет собой решение, позволяющее изменить существующую модель управления медицинской информацией.

Блокчейн можно рассматривать как защищенный цифровой реестр, в котором информация хранится в виде цепочки блоков. Каждый новый блок содержит хеш предыдущего, что делает невозможным изменение уже записанных данных без согласия всех участников сети. Это свойство обеспечивает высокий уровень защиты от несанкционированного доступа. В отличие от централизованных систем, блокчейн не зависит от единой точки отказа, так как информация распределяется между множеством узлов в сети.

Ключевым аспектом использования блокчейна в сфере здравоохранения является его способность гарантировать безопасность и конфиденциальность медицинских данных. Совмещение блокчейна с межплатформенными решениями, такими как IPFS (InterPlanetary File System), позволяет надежно хранить медицинские записи в распределенном виде, а их хеши записывать в блокчейн для предотвращения фальсификации. Для контроля доступа может применяться модель управления доступом на основе атрибутов, которая позволяет гибко регулировать права пользователей в зависимости от их роли (пациент, врач, администратор и т. д.).

На рис. 1 показана возможная архитектура системы хранения и управления медицинскими данными с применением блокчейна:

Схема иллюстрирует процесс управления медицинскими данными с использованием блокчейн-технологий. Пользователи (пациенты, врачи, администраторы) получают доступ к информации через модель ABAC, которая определяет их права. Медицинские записи хранятся в распределенной файловой системе IPFS, а их неизменяемые хеши фиксируются в блокчейне с помощью API. Это гарантирует целостность данных и защищает их от подделки.

Одним из значимых преимуществ блокчейна в здравоохранении является его прозрачность. Каждый доступ к медицинским данным может фиксироваться в блокчейне, что позволяет создавать полную историю их изменений. Это особенно важно для аудита и отслеживания возможных манипуляций с медицинской информацией. Такой подход способствует предотвращению мошенничества и улучшению взаимодействия между различными медицинскими учреждениями.

Кроме того, использование блокчейна может повысить эффективность обмена медицинскими данными между больницами, лабораториями и частными клиниками.

Децентрализованная сеть позволяет создать единую защищенную платформу для обмена медицинскими данными, обеспечивая их доступность и целостность без риска утечек.

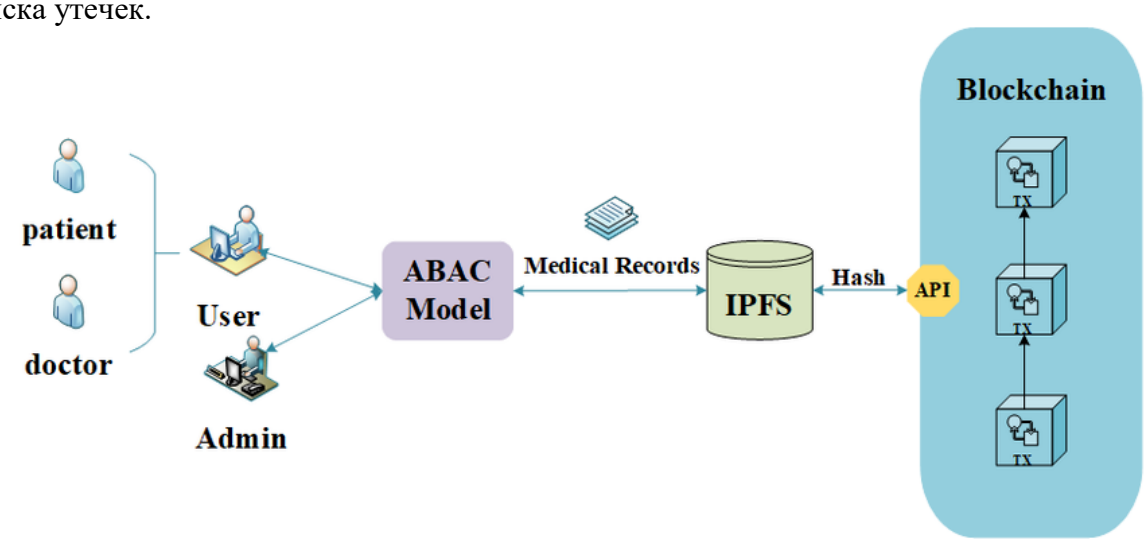


Рис. 1. Интеграция блокчейна и IPFS для хранения медицинских данных
Fig 1. Integration of Blockchain and IPFS for Storing Medical Data

Заключение

Блокчейн представляет собой перспективное решение для повышения безопасности и конфиденциальности медицинских данных. Его децентрализованная природа, в сочетании с криптографическими механизмами и моделями управления доступом, обеспечивает высокий уровень защиты информации. Интеграция с IPFS и моделями управления доступом позволяет создать надежную инфраструктуру для хранения и обработки медицинских записей. Внедрение таких решений в медицинские системы поможет минимизировать риски утечек данных, улучшить контроль доступа и повысить доверие пациентов к цифровым технологиям в здравоохранении.

Список использованных источников / References

1. Sun Z., Han D., Li D., Wang X., Chang C.-C., Wu Z. (2022) A Blockchain-based Secure Storage Scheme for Medical Information. EURASIP Journal on Wireless Communications and Networking, 40 (2022).

Сведения об авторах

Мигалевич С.А., магистр технических наук, старший преподаватель кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», migalevich@bsuir.by.
Логвинович М.В., студент 4 курса факультета компьютерных систем и сетей, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», maxiqastflower21@gmail.com.

Information about the authors

Migalevich S., Master of Technical Sciences, Senior Lecturer at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", migalevich@bsuir.by.
Logvinovich M., fourth-year student of the Faculty of Computer Systems and Networks, Educational Institution "Belarusian State University of Informatics and Radioelectronics", maxiqastflower21@gmail.com.

УДК 004.89

ОБЪЕДИНЕНИЕ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА И МАШИННОГО ФЕДЕРАЛЬНОГО ОБУЧЕНИЯ

А.М. Макаров, Е.А. Писаренко, И.Н. Кутовой, Б.М. Гаджимуратов
ФГБОУ ВО «Пятигорский государственный университет»,
г. Пятигорск, Российская Федерация.

Аннотация. В работе рассматривается решение задачи целостности обучающих данных искусственного интеллекта на основе объединения систем с распределенным реестром (блокчейн), и технологий криптографии в системах федерального обучения искусственного интеллекта. При этом обеспечивается конфиденциальности данных, защите их от фальсификации, модификации и уничтожения является в настоящее время важной задачей производства систем с ИИ. Рассмотрена целесообразность отдельного включения временных меток в протоколы нотариуса-криптографа. Далее приводятся схема блок- структур, объединяющие технологии обучения и технологии информационной безопасности режима федерального обучения ИИ.
Ключевые слова: искусственный интеллект; федеральное обучение; временные метки; блокчейн технология; криптография; хэширование.

COMBINING DISTRIBUTED LEDGER SYSTEMS AND MACHINE FEDERAL LEARNING

A.M. Makarov, E.A. Pisarenko, I.N. Kutovoy, B.M. Gadzhimuratov
Federal State Budgetary Educational Institution of Higher Education
"Pyatigorsk State University",
Pyatigorsk, Russian Federation.

Annotation. The paper deals with the solution of the problem of integrity of artificial intelligence training data on the basis of combining systems with distributed registry (blockchain), and cryptography technologies in the systems of federal training of artificial intelligence. At the same time the confidentiality of data, protection of data from falsification, modification and destruction is currently an important task of production of systems with AI. The feasibility of separate inclusion of timestamps in notary cryptographer protocols is considered. Further, the scheme of blockchain structures combining training technologies and information security technologies of the federal AI training mode is given.
Keywords: Artificial Intelligence; federal learning; timestamps; blockchain technology; cryptography; hashing.

Введение

Внедрение генеративного искусственного интеллекта (ИИ) в практику обучающих, справочных и типовых текстов привело к необходимости разработки государственных стандартов, регламентов, а также юридических правил использования ИИ, как в обществе, так и в сферах, где требуется выполнение определенных правил этики поведения феномена ИИ. Следует заметить, что первые угрозы возникают на этапах обучения, дообучения и переобучения памяти ИИ. Особенно остро стоит задача по использованию достоверных обучающих данных, а также их надежного хранения непосредственно в самой системе ИИ.

Сохранение конфиденциальности данных, защите их от фальсификации, модификации и уничтожения является в настоящее время важной задачей производства систем с ИИ. Таким образом, весьма актуально решение вышеперечисленных задач в плане обеспечения информационной безопасности данных во всей их разнообразии палитр.

Материалы и методы

Проникновение новых технологий в системы с распределенным реестром, реализованных на блокчейн технологии, в основе которой лежат методы криптографии, происходит во все сферы социально-экономической деятельности общества. Императивный стиль в проектировании социально-экономических систем это такой, при котором предварительно выработанные заранее требования (аксиомы) к их свойствам, должен непременно выполняться проектировщиком, для достижения технических и социально-экономических целей (1, 2, 3).

Для решения задачи сформулируем пять императивных требования:

1. Наличие абонентов, объединенных решаемой задачей, которым система с распределенным реестром необходима для доверительной работы абонентов, не доверяющих друг другу. И, как следствие, отсутствие централизованного контроля сети. Все абоненты сети являются контролерами их работы с правом вмешаться в любой момент времени в любой точке цепи работы.
2. Обязательное формирование всей базы данных всех транзакций в сети распределенного реестра абонентов и обязательное обеспечение каждого абонента всеми текущими блоками транзакций в реальном масштабе времени.
3. Абоненты сети не являются профессиональными криптографами. Эту роль играет профессиональный нотариус-криптограф. Это новая роль майнера, требующая своего развития.
4. Формируемая база транзакций, всегда должна быть одноранговой цепью, включающая все блоки, включенные в сеть (ошибочные, испорченные, по ошибке включенные и так далее). Без права уничтожать, заменять, корректировать данные включенных блоков, вставлять, шунтировать блоки и так далее.
5. Все, перечисленные выше требования к системам распределенного реестра (блокчейн технология), погружаются в «океан» криптографического шифрования и криптографических технологий.

Результаты

Схема федерального централизованного обучения не требует загрузки данных абонентов, участвующих в дообучении ИИ. Это позволило решить задачу сохранения конфиденциальности персональных данных абонентов.

На рис. 1 представлена структура, использующая технологию блокчейн. В качестве абонентов, объединенных общей задачей обучения, служат различные носители обучающих данных (ТАА и ДО). Они образуют систему распределенного реестра с заинтересованными лицами, каждый из которых имеет свой уникальный цифровой токен и цифровую подпись. Посредством нотариуса-криптографа блоки с обучающими данными встраиваются в одноранговую цепь и рассылают общую базу данных серверов каждого абонента в системе распределенного реестра. На рис. 1 приведена система распределенного реестра (блокчейн технология), в которую встроена система ИИ. В данном случае кибербезопасность ИИ полностью защищена блокчейн технологией. Причем в качестве достоверности и целостности данных используется стрела меток времени прикрепления каждого блока в одноранговую сеть. Вторым видом федерального обучения называемого совместным в их ИИ обучается на множестве децентрализованных абонентов или серверов. То есть обучающие данные

не загружаются в общий сервер и не являются одинаково распределенными данными каждого абонента, участвующего в обучении.

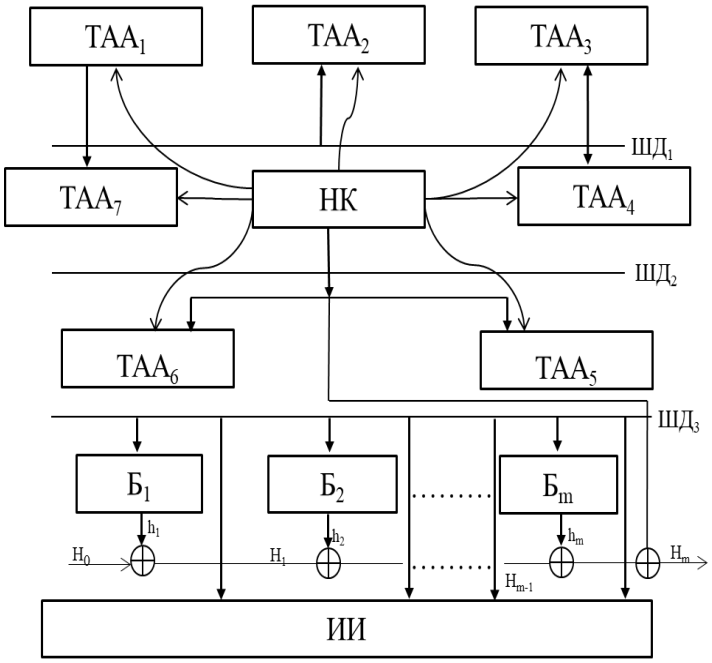


Рис. 1 Структура, использующая технологию блокчейн в федеральном способе обучения
Fig. 1 Structure utilizing blockchain technology in the federal way of learning

Сформулированные в работе императивные требования позволили оценить возможность применения технологии блокчейн для построения единой системы искусственного интеллекта с одновременным обеспечением информационной безопасностью целостности обучающих данных. Применение технологии временных меток для формирования вторых хешей блоков основной сети позволило упростить контроль свежести времени встраивания блоков блокчейн в основную одноранговую цепь для абонентов сети**.** Эти результаты показывают эффективность и целесообразность встраивания технологии распределенного реестра в общую систему обучения. Но в тоже время остался открытым вопрос, количественной экономической оценки стоимости и киберстойкости всей системы в целом. Эти две отмеченные задачи требуют дополнительного исследования и анализа.

Список использованных источников

1. Судас Л.Г. Управленческие императивы Индустрии 4.0 / Л.Г. Судас, М.А. Юдина. – М. : Издательство Московского университета, 2021. – 152 с. – (Библиотека факультета государственного управления МГУ. Научные исследования, электронное издание сетевого распространения).

2. Что такое императивное управление процессами. URL: https://totallsocks.ru/chto-takoe-imperativnoe-upravlenie-protsessami.

3. Макаров А.М., Писаренко Е.А. Перспективы развития теории систем распределенного реестра в управлении социальноэкономическими объектами. В сборнике: Инновационные тренды в международном бизнесе и устойчивом менеджменте. Материалы II Международной научно-практической конференции. Новокузнецк, 2023. С. 221-232.

References

1. Sudas, L.G. Upravlenie imperatives of Industry 4.0 / L. G. Sudas, M. A. Yudina. – Moscow: Moscow University Press, 2021. – 152 p. (Library of the Faculty of Public Administration of Moscow State University. Scientific research, electronic edition of network distribution).

2. What is imperative process management. URL: https://totallsocks.ru/chto-takoe-imperativnoe-upravlenie-protsessami.

3. Makarov A.M., Pisarenko E.A. PERSPECTIVES OF DEVELOPMENT OF THEORY OF DISPLACED LISTING SYSTEMS IN MANAGEMENT OF SOCIAL ECONOMIC OBJECTS. In collection: Innovative trends in international business and sustainable management. Materials of the II International Scientific and Practical Conference. Novokuznetsk, 2023. C. 221-232.

Сведения об авторах

Макаров А.М., д-р техн. наук, проф., проф. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail mellin_22@mail.ru.
Писаренко Е.А., канд. пед. наук, доц., доц. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail elt@yandex.ru.
Кутовой И.Н., канд. пед. наук, доц., доц. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail igor196428@yandex.ru.
Гаджимурадов Б.М., канд. экон. наук, ст. преп. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail baxa78@bk.ru.

Information about the authors

Makarov A.M., D.Sc. (Eng.), Prof., Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail mellin_22@mail.ru.
Pisarenko E.A., Ph.D. (Ped.), Assoc. Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail elt@yandex.ru.
Kutovoy I.N., Ph.D. (Ped.), Assoc. Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail igor196428@yandex.ru
Gadzhimuradov B.M., Ph.D. (Econ.), Senior Lecturer, Dept. information and communication technologies, mathematics and information security, Pyatigorsk State University, e-mail baxa78@bk.ru

УДК 004.716

ИМИТАЦИЯ АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ: ПОСТРОЕНИЕ ЭКСПЕРИМЕНТА И АНАЛИЗ РЕЗУЛЬТАТОВ

Е.М. Марденов[1, 2], Б. Ху Вен-Цен[1], А.А. Абдилдаева[1]
[1]Международный научный комплекс «Астана», Астана, Казахстан
[2]Международный университет Астана, Астана, Казахстан

Аннотация. В данной работе рассматривается моделирование атак на беспроводные сенсорные сети (БСС) с целью анализа их влияния на безопасность и работоспособность сети. В рамках исследования разработан стенд, имитирующий киберфизическую систему мониторинга атмосферного воздуха, построенный на основе ZigBee-сети с узлами на базе Arduino и Raspberry Pi. Основное внимание уделено моделированию атаки типа Wormhole, при которой злоумышленник создает нелегитимный канал связи между удаленными узлами, что приводит к нарушению маршрутизации и перехвату данных. Проведен анализ функционирования сети в условиях атаки и нормальной работы, а также разработаны подходы к выявлению подобного типа угроз. Представленные результаты могут быть полезны для дальнейшей разработки методов защиты БСС от атак на маршрутизацию.

Ключевые слова: беспроводные сенсорные сети, ZigBee, безопасность, атака Wormhole, киберфизические системы, маршрутизация, имитация атак, анализ уязвимостей, мониторинг воздуха, ZigBee-устройства.

SIMULATION OF ATTACKS IN WIRELESS SENSOR NETWORKS: EXPERIMENT DESIGN AND RESULT ANALYSIS

E.M. Mardenov[1, 2], B. Hu Wen-Tsen[1], A.A. Abdildayeva[1]
[1]*International Scientific Complex "Astana", Astana, Kazakhstan*
[2]*Astana International University, Astana, Kazakhstan*

Abstract. This study examines the simulation of attacks on wireless sensor networks (WSNs) to analyze their impact on network security and functionality. As part of the research, a testbed was developed to simulate a cyber-physical system for atmospheric air monitoring, built on a ZigBee network with nodes based on Arduino and Raspberry Pi. The primary focus is on modeling a Wormhole attack, in which an attacker creates an illegitimate communication channel between remote nodes, leading to routing disruption and data interception. The network's performance was analyzed under both attack conditions and normal operation, and approaches were developed for detecting such threats. The presented results may be useful for the further development of methods to protect WSNs from routing attacks.
Keywords: wireless sensor networks, ZigBee, security, Wormhole attack, cyber-physical systems, routing, attack simulation, vulnerability analysis, air monitoring, ZigBee devices.

Введение

Беспроводные сенсорные сети (БСС) представляют собой одну из ключевых технологий в современных киберфизических системах, обеспечивающих мониторинг окружающей среды, промышленных объектов, городской инфраструктуры и критически важных систем. Благодаря самоорганизующейся архитектуре, компактным размерам и низкому энергопотреблению, узлы таких сетей широко применяются в системах экологического мониторинга, умных городах, медицине и промышленной автоматизации. Однако, наряду с преимуществами, беспроводные сети подвержены различным видам атак, среди которых особую угрозу представляют атаки на маршрутизацию, такие как Wormhole (червоточина) [1].

Атака Wormhole представляет собой один из наиболее опасных типов атак на сетевой уровень БСС. Ее суть заключается в том, что злоумышленник создает скрытый высокоскоростной канал связи между двумя узлами сети, которые физически могут находиться далеко друг от друга. Это позволяет перехватывать, модифицировать и перенаправлять сетевой трафик, вводя в заблуждение легитимные узлы относительно реальной топологии сети. В результате атакующие узлы могут не только осуществлять перехват и анализ данных, но и нарушать нормальное функционирование сети, влияя на маршруты передачи сообщений [2]. Данный тип атаки особенно опасен для сетей, использующих протокол ZigBee, поскольку маршрутизация в таких сетях основана на минимальном количестве переходов (hops), а Wormhole-атака создает искусственно укороченные маршруты [3].

В данной работе представлена разработка экспериментального стенда для моделирования атак на беспроводные сенсорные сети, а также проведение анализа их воздействия на сеть. В качестве тестовой среды используется сеть из семи узлов, работающих по протоколу ZigBee с использованием модулей Digi XBee. Четыре узла построены на базе микроконтроллеров Arduino Uno, два узла – на одноплатных компьютерах Raspberry Pi, а один узел выполняет роль координатора сети и подключен к персональному компьютеру. Для моделирования атаки Wormhole используется канал связи GSM/GPRS между двумя атакующими узлами, что позволяет эмулировать нелегитимный высокоскоростной путь передачи данных.

Рис. 1. Вид на экспериментальный стенд
Fig. 1. View of the experimental stand

Атака Wormhole является одной из самых сложных для обнаружения, поскольку она не требует компрометации криптографических механизмов, а вместо этого использует уязвимости самой структуры сети. В связи с этим важно разрабатывать и тестировать новые методы выявления таких атак, включая мониторинг задержек передачи пакетов, анализ топологии сети и применение алгоритмов машинного обучения для обнаружения аномалий в маршрутизации [4].

Основной целью данной работы является исследование воздействия атаки Wormhole на беспроводные сенсорные сети и разработка подходов к ее обнаружению.

Научная новизна работы заключается в создании экспериментального стенда для анализа атак на беспроводные сенсорные сети и исследовании специфики их влияния на маршрутизацию в ZigBee-сетях. В отличие от существующих работ, в которых основное внимание уделяется теоретическому анализу угроз, в данной работе предложена практическая реализация атаки с использованием реального оборудования.

Основная часть

Беспроводные сенсорные сети (БСС) представляют собой распределенные системы, состоящие из множества узлов, взаимодействующих друг с другом для мониторинга окружающей среды, передачи данных и выполнения вычислительных задач. Каждый узел БСС, как правило, включает в себя сенсоры, микроконтроллер, модуль связи и источник питания. Эти сети широко применяются в таких областях, как промышленный контроль, экологический мониторинг, системы «умного города» и медицинские приложения [5].

Основными характеристиками БСС являются:

– самоорганизация – узлы сети автоматически формируют топологию, определяя маршруты передачи данных;

– ограниченные ресурсы – узлы обладают малым объемом памяти, низким энергопотреблением и ограниченной вычислительной мощностью;

– динамическая топология – конфигурация сети может изменяться из-за перемещения узлов или внешних воздействий;

– многохоповая маршрутизация – данные передаются от узла к узлу, поскольку не все узлы имеют прямую связь с конечным получателем.

Важной особенностью БСС является использование беспроводных технологий связи, таких как Wi-Fi, Bluetooth, ZigBee и LoRaWAN. В данной работе рассматривается технология ZigBee как одна из наиболее популярных для построения БСС.

Протокол ZigBee представляет собой стандарт для низкоэнергетичных беспроводных сетей, разработанный на основе IEEE 802.15.4. Он предназначен для создания энергоэффективных сетей с поддержкой самоорганизации и масштабируемости [6]. В ZigBee-сетях используются три типа устройств:

Координатор (Coordinator, C) – центральный узел сети, управляющий маршрутизацией и обеспечивающий взаимодействие с другими системами.

Роутеры (Routers, R) – промежуточные узлы, передающие трафик и поддерживающие сеть.

Рис. 2. Промежуточные узлы
Fig. 2. Intermediate nodes

Конечные устройства (End Devices, E) – узлы, собирающие данные, но не выполняющие функции ретрансляции.

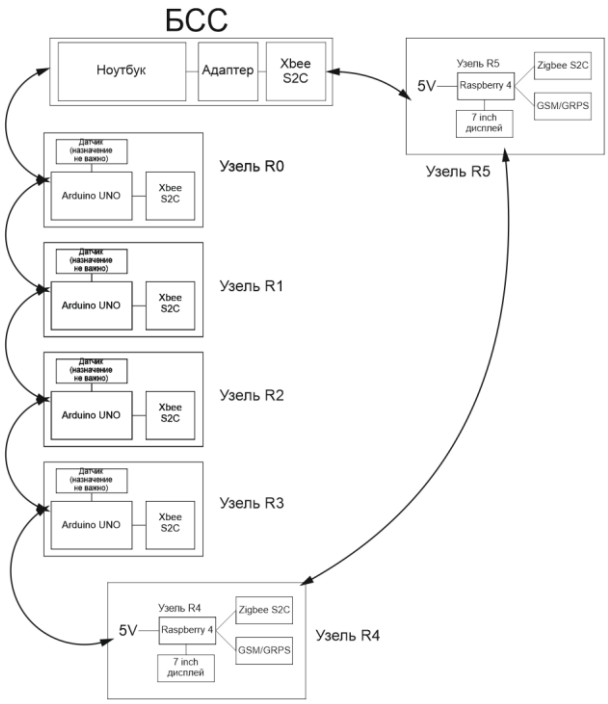


Рис. 3. Общая схема работы стенда
Fig. 3. General scheme of the stand operation

Для маршрутизации данных в ZigBee применяется протокол AODV (Ad hoc On-Demand Distance Vector Routing), который строит маршруты по запросу. Основные этапы маршрутизации в ZigBee:

Формирование сети – координатор инициирует создание сети и назначает уникальный PAN ID.

Обнаружение маршрута – узел, желающий отправить данные, отправляет широковещательный запрос (route request).

Выбор маршрута – узлы пересылают запрос, а конечный узел отправляет ответ (route reply) по наикратчайшему маршруту.

Передача данных – данные передаются по установленному маршруту, а при изменении топологии происходит обновление маршрутов.

Ключевой особенностью ZigBee является минимизация числа hops (прыжков) при выборе маршрута, что делает сеть уязвимой к атакам на маршрутизацию, таким как Wormhole.

В ходе эксперимента для настройки и мониторинга параметров ZigBee-сети использовалась программа XCTU, предоставляемая компанией Digi. Данный инструмент позволил конфигурировать модули Digi XBee, задавать сетевые параметры, изменять роли узлов (координатор, роутер, оконечное устройство). С помощью XCTU была проведена диагностика соединений между узлами, анализ задержек передачи данных и выявление изменений в маршрутизации, что сыграло ключевую роль в моделировании атаки Wormhole и оценке ее воздействия на работу сети.

Рис. 4. Вид работы программы XCTU
Fig. 4. View of the XCTU program operation

Беспроводные сенсорные сети подвержены множеству атак, направленных на нарушение их функционирования. Среди них можно выделить атаки на физический, канальный и сетевой уровни модели. На сетевом уровне, к которому относится маршрутизация, наиболее опасными являются Blackhole, Sinkhole, Replay Attack, Hello Flood, Wormhole [7].

Таблица 1. Наиболее опасные атаки на сетевом уровне
Table 1. The most dangerous attacks at the network level

Название атаки	Описание атаки	Последствия
Blackhole	Злоумышленник узел перехватывает пакеты и не передает их дальше, что нарушает связь в сети.	Потеря данных, отказ в обслуживании (DoS), разрыв связи. [8]
Sinkhole	Компрометированный узел перенаправляет трафик на себя, создавая ложный центр сети.	Снижение производительности сети, увеличение задержек, централизованный контроль злоумышленника. [9]
Replay Attack	Злоумышленник записывает пакеты данных и повторно отправляет их в сеть, вызывая дублирование информации.	Дублирование пакетов, искажение информации, перегрузка сети. [10]
Hello Flood	Атакующий рассылает ложные сообщения о близости ко всем узлам, перегружая сеть.	Перегрузка сети, сбои в маршрутизации, увеличение задержек [11]
Wormhole	Создание нелегитимного быстрого канала между двумя узлами, что изменяет маршрутизацию и позволяет перехватывать трафик.	Перехват, модификация и блокировка трафика, нарушение маршрутизации [12]

Атака Wormhole считается одной из наиболее сложных для обнаружения, поскольку не требует компрометации криптографических ключей или внесения изменений в программное обеспечение узлов [12]. Она заключается в следующем:

Создание скрытого канала – два атакующих узла устанавливают быстрый канал связи, например, через GSM/GPRS или Wi-Fi. Перехват пакетов – один из узлов атакующей пары перехватывает пакеты, передаваемые по ZigBee. Пересылка пакетов – пакеты мгновенно пересылаются через нелегитимный канал и передаются в сеть вторым атакующим узлом. Формирование ложных маршрутов – из-за сокращенного количества hops другие узлы считают маршрут через атакующие узлы наиболее оптимальным и начинают передавать данные через них.

Разработан сценарий атаки, в котором два атакующих узла создают скрытый канал передачи данных, искажающий топологию сети. Атака позволила злоумышленнику перенаправлять значительную часть сетевого трафика через компрометированные узлы. Были зафиксированы случаи изменения маршрутизации: узлы, выбирая оптимальный путь передачи данных, использовали нелегитимный канал, созданный атакующими узлами. В результате атаки были продемонстрированы возможности перехвата, модификации и блокировки сетевого трафика, что подтвердило уязвимость ZigBee-сетей перед данным видом угроз.

Зафиксировано сокращение числа переходов (hops) при передаче пакетов, что свидетельствовало о ложном сокращении маршрута. Наблюдались искажения данных, вызванные перехватом и изменением передаваемых пакетов. В некоторых случаях атака приводила к полной потере связи между узлами, что демонстрирует возможность организации отказа в обслуживании (DoS-атаки). Были исследованы методы выявления атаки, в том числе анализ задержек передачи пакетов и анализ топологии сети с учетом подозрительных изменений в маршрутизации.

Заключение

В ходе исследования была разработана экспериментальная платформа для моделирования атак на беспроводные сенсорные сети (БСС) на основе технологии ZigBee. Созданная сеть из семи узлов включала координатор, роутеры и атакующие узлы, работающие на микроконтроллерах Arduino Uno и одноплатных компьютерах Raspberry Pi. Для связи между узлами использовались модули Digi XBee, а атакующие узлы были дополнительно оснащены GSM/GPRS модулями (SIM800/SIM900), что позволило создать нелегитимный высокоскоростной канал связи. Данный стенд позволил имитировать атаку Wormhole и изучить ее влияние на работу сети.

Эксперименты показали, что атака Wormhole существенно изменяет маршрутизацию трафика в сети. В результате узлы начинали выбирать нелегитимный маршрут через атакующие узлы, сокращая количество hops и перенося основную нагрузку на узлы злоумышленника. Это позволяло атакующему не только перехватывать и анализировать передаваемые данные, но также блокировать или модифицировать трафик, изменяя показания датчиков. В отдельных случаях атака приводила к потере связи между узлами и отказу в передаче данных, что может иметь критические последствия для систем мониторинга.

Полученные результаты подтверждают высокую уязвимость БСС к атакам на маршрутизацию. Протокол ZigBee, ориентированный на минимизацию количества переходов при передаче данных, не учитывает возможность существования нелегитимных каналов связи. Это делает атаку Wormhole особенно сложной для обнаружения. В рамках исследования были рассмотрены потенциальные методы защиты, включая мониторинг задержек передачи пакетов, анализ сетевой топологии и применение алгоритмов машинного обучения для обнаружения аномалий в маршрутизации.

Перспективы дальнейших исследований включают разработку и тестирование алгоритмов обнаружения атак, а также изучение других видов атак на маршрутизацию, таких как Sinkhole, Blackhole и Hello Flood. Внедрение механизмов защиты на уровне протоколов маршрутизации, включая многофакторную проверку маршрутов и использование доверенных узлов, может значительно повысить устойчивость БСС к атакам. Таким образом, проведенное исследование вносит вклад в развитие методов обеспечения безопасности киберфизических систем и беспроводных сенсорных сетей.

Список использованных источников / References

1. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors 2022, 22, 2087.

2. Krishnakumar, Parvathy. (2021). Wormhole Attacks in Wireless Sensor Net-works (Wsn) & Internet of Things (IoT): A Review. International Journal of Re-cent Technology and Engineering. 10. 199-203.

3. Jegan, G. & Punniakodi, Samundiswary. (2016). Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System. Indian Journal of Science and Technology.

4. Dutta, Nishigandha & Singh, Moirangthem. (2019). Wormhole Attack in Wireless Sensor Networks: A Critical Review.

5. T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev and Z. Ahmad, "A Traffic Analysis and Node Categorization- Aware Machine Learning-Integrated Framework for Cybersecurity Intrusion Detection and Prevention of WSNs in Smart Grids," in IEEE Access, vol. 12, pp. 91715-91733, 2024, doi: 10.1109/ACCESS.2024.3422077.

6. Fafoutis, Xenofon & Tsimbalo, Evgeny & Zhao, Wenrui & Chen, Haowen & Mellios, Evangelos & Harwin, William & Piechocki, R.J. & Craddock, I.J.. (2016). BLE or IEEE 802.15.4: Which Home IoT Communication Solution is more Energy-Efficient?. EAI Endorsed Transactions on Internet of Things.

7. A. Adamova, T. Zhukabayeva and Y. Mardenov, "Machine Learning in Action: An Analysis of its Application for Fault Detection in Wireless Sensor Networks," 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023, pp. 506-511.

8. Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. Appl. Sci. 2022, 12, 11442.

9. Ali, Mubashir & Nadeem, Muhammad & Siddique, Ayesha & Ahmad, Shahbaz & Ijaz, Amir. (2020). Addressing Sinkhole Attacks In Wireless Sensor Networks -A Review. International Journal of Scientific & Technology Research. 9. 406-411.

10. Pichamuthu, Rajaram. (2024). An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network. 63. 8010-8023.

11. Singh, Virendra & Sweta, Jain & Jyoti, Singhai. (2010). Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. International Journal of Computer Science Issues. 7.

12. Zhukabayeva T.K., Mardenov E.M. (2021). Detecting wormhole attacks in wireless sensor networks. Issue No. 4(107): Herald of Science of S. Seifullin Kazakh Agro Technical University.

Сведения об авторах

Марденов Е.М., научный сотрудник, Международный научный комплекс «Астана», yerik.mardenov@aiu.edu.kz.
Абдилдаева А.А., PhD, старший научный сотрудник, Международный научный комплекс «Астана».
Ху Вен-Цен Б., д-р техн. наук, проф., ведущий научный сотрудник, Международный научный комплекс «Астана».

Information about the authors

Mardenov E.M., Researcher, International Scientific Complex "Astana", yerik.mardenov@aiu.edu.kz.
Abdildaeva A.A., PhD, Senior Researcher, International Scientific Complex "Astana".
Hu Wen-Tsen B., D.Sc. (Eng.), prof., leading research fellow, International Scientific Complex "Astana".

УДК 004.777

МЕТОДЫ ОБНАРУЖЕНИЯ РАДИОПЕРЕДАЮЩИХ УСТРОЙСТВ, ИСПОЛЬЗУЮЩИХ ТЕХНОЛОГИЮ WI-FI

О.Ч. Маркун
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассмотрены демаскирующие признаки радиопередающих устройств, а также методы их обнаружения.
Ключевые слова: радиопередающее устройство; демаскирующие признаки радиопередающих устройств; методы обнаружения радиопередающих устройств.

METHODS FOR DETECTING RADIO TRANSMITTING DEVICES USING WI-FI TECHNOLOGY

O.Ch. Markun
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the unmasking features of radio transmitting devices, as well as methods for their detection.
Keywords: radio transmitting device; unmasking features of radio transmitting devices; methods of detecting radio transmitting devices.

Введение

Радиопередающие устройства (РПУ) могут быть использованы нарушителем для передачи информации ограниченного распространения за пределы контролируемой зоны объектов различного назначения. С развитием современных устройств беспроводной связи актуальность использования технологии Wi-Fi в подобных устройствах обусловлена следующими факторами:

– ее широкой распространенностью;

– высокими скоростью передачи информации и пропускной способностью канала связи;

– возможностью маскировки РПУ под легальные источники передачи информации в сложной электромагнитной обстановке.

Обнаружение и локализация таких РПУ является важной задачей в системе реализации мероприятий по защите информации.

Основная часть

Для определения эффективных методов поиска и обнаружения РПУ выделим основные демаскирующие признаки, характерные для радиоэлектронных средств. Такими признаками будут являться сигнальные и видовые.

Радиопередающие устройства предназначены для формирования колебаний несущей частоты, модулируемой по закону передаваемого сообщения и излучения сформированного радиосигнала в воздушную среду или передачи его по линиям связи [3].

Блок-схема типового радиопередающего устройства приведена на рис. 1.

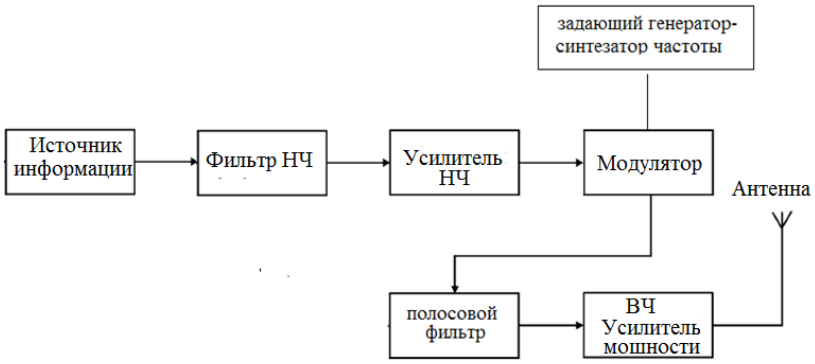


Рис.1. Блок-схема типового РПУ
Fig.1. Block diagram of a typical RPU

Основные демаскирующие признаки РПУ, использующих Wi-Fi технологию следующие:

– электромагнитное излучение с параметрами, соответствующими стандарту IEEE 802.11;

– тепловое излучение вследствие нагрева радиоэлектронных компонентов РПУ;

– видовые признаки (конструкция корпуса устройства, антенная система и т.д.).

На основании выделенных демаскирующих признаков РПУ, определим основные современные методы обнаружения:

– радиомониторинг;

– методы неразрушающего контроля;

– нелинейная радиолокация.

Сущность метода радиомониторинга заключается в обнаружении и идентификации источника излучения, определении его местоположения в контролируемой зоне.

Существующее оборудование для радиомониторинга РПУ можно разделить на четыре основные группы:

– к первой группе относятся анализаторы широкополосных беспроводных сетей, построенные на основе универсальных измерительных цифровых радиоприемных устройств (ЦРПрУ). Важным достоинством анализаторов беспроводных сетей на базе ЦРПрУ является возможность использования программного обеспечения для решения задач оценки, анализа и хранения (запоминания) параметров обнаруженных сигналов, расчета и построения зоны их вероятного местоположения;

– оборудование второй группы представляет собой специализированные адаптеры, предназначенные для осуществления контроля систем радиодоступа по эфиру. Эти адаптеры имеют узкий перечень измеряемых параметров радиосигналов, используют некалиброванные антенные системы и работают только в лицензируемых диапазонах частот 2412…2484 МГц и 5170…5320 МГц, что ограничивает их применение в средствах радиомониторинга;

– к третьей группе относятся полнофункциональные анализаторы спектра и радиосигналов от ведущих мировых производителей аппаратуры радиоконтроля (Rohde & Schwarz, Keysight, Tektronix и т.д.);

– к четвертой группе относятся индикаторы и детекторы поля, предназначенные для световой и звуковой индикации наличия и относительного уровня электромагнитного излучения в заданном диапазоне.

Сущность применения методов неразрушающего контроля при поиске РПУ заключается в осуществлении:

– оптико-визуального наблюдения (поиска) характерных технических устройств и их антенной системы в вероятных местах размещения как методом прямого осмотра, так и с использованием оптических приборов (биноклей, линз, зеркал);

– тепловизионного контроля наличия излучения в следствие нагрева радиоэлектронных компонентов во время работы РПУ на фоне постоянной температуры окружающей среды, ограждающих конструкций и предметов.

Сущность применения метода нелинейной радиолокации заключается в том, что при облучении электромагнитной волной электронные устройства, содержащие полупроводниковые компоненты, переизлучают сигнал, в котором появляются высшие гармоники.

Заключение

Для обнаружения и локализации РПУ использующих технологию Wi-Fi необходимо учитывать демаскирующие признаки таких устройств. Кратко рассмотренные методы обнаружения позволяют решать такую задачу только при их комплексном применении.

Список использованных источников

1. Гуляев, В. П. Г94 Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации : учебно-методический комплект / В. П. Гуляев. – Екатеринбург : Изд-во Урал. ун-та, 2014. – 164 с.

2. Зайцев, А. П. Технические средства и методы защиты информации : учебник [рек. МО РФ] / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – 7-е изд. – Москва : Горячая линия-Телеком, 2018. – 442 с.

3. Путилин, В. Н. Основы радиоэлектроники : метод. пособие для студентов всех специальностей БГУИР заоч. формы обучения / В. Н. Путилин. – Минск : БГУИР, 2013. – 54 с. : ил.

4. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Автоматизированные системы радиоконтроля и их компоненты / Под редакцией А.М.Рембовского. – 2-изд., испр.и доп. – М: Горячая линия – Телеком, 2022. – 488с.

References

1. Gulyaev, V. P. G94 Analysis of unmasking features of informatization objects and technical channels of information leakage : an educational and methodological kit / V. P. Gulyaev. Yekaterinburg : Ural Publishing House. University, 2014. – 164 p.

2. Zaitsev, A. P. Technical means and methods of information protection : textbook [rec. Ministry of Defense of the Russian Federation] / A. P. Zaitsev, R. V. Meshcheryakov, A. A. Shelupanov. – 7th ed. – Moscow : Hotline-Telecom, 2018. – 442 p.

3. Putilin, V. N. Fundamentals of radio electronics : method. a manual for students of all BSUIR majors by correspondence. forms of education / V. N. Putilin. – Minsk : BGUIR, 2013. – 54 p. : ill.

4. Rembovsky A.M., Ashikhmin A.V., Kozmin V.A. Automated radio monitoring systems and their components / Edited by A.M. Rembovsky. – 2nd ed., ispr. and add. – Moscow: Hotline – Telecom, 2022. – 488 p.

Сведения об авторе

Маркун О.Ч., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mail: olmark7@mail.ru.

Information about the author

Markun O., Master Student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mail: olmark7@mail.ru.

УДК 004.056.5

УТЕЧКА ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИН В КОНТЕКСТЕ РАЗВИТИЯ SDR И AI, АКТУАЛЬНЫЕ УГРОЗЫ И ИССЛЕДОВАНИЯ

Мартинкевич А.А.[1], Майоров А.И.[1], Буневич М.А.[2], Горбачев Д.В.[3]
[1]ГУО «Институт пограничной службы», Минск, Беларусь
[2]«Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь
[3]Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. статья анализирует актуальные угрозы утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) в условиях распространения технологий программно-определяемого радио (SDR) и искусственного интеллекта (AI). Приведены примеры атак 2020–2025 гг., а также обзор научных публикаций, посвященных методам защиты и анализу рисков.
Ключевые слова: ПЭМИН, SDR, искусственный интеллект, утечки информации, кибербезопасность.

TEMPEST CHANNEL INFORMATION LEAKAGE IN THE CONTEXT OF SDR AND AI DEVELOPMENT: CURRENT THREATS AND RESEARCH

Martinkevich A.A.[1], Mayorov A.I.[1], Bunevich M.A.[2], Gorbachev D.V.[3]
[1]State Educational Institution "Institute of Border Service", Minsk, Belarus
[2]Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus
[3]Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article analyzes the current threats of information leakage through side electromagnetic emissions and interference (SEMI) in the context of the spread of software-defined radio (SDR) and artificial intelligence (AI) technologies. Examples of attacks from 2020–2025 are given, as well as a review of scientific publications devoted to protection methods and risk analysis.
Keywords: side electromagnetic radiation and pickup, SDR, artificial intelligence, information leaks, cybersecurity.

Введение

ПЭМИН остаются одной из ключевых угроз информационной безопасности, особенно в эпоху цифровизации. Современные технологии, такие как SDR и AI, не только усиливают риски, но и создают новые инструменты для анализа и защиты. В статье рассмотрены актуальные исследования и примеры атак.

Основная часть

Программно-определяемое радио (SDR) и искусственный интеллект (AI) стали ключевыми технологиями, трансформирующими методы атак в контексте ПЭМИН.

SDR-устройства, такие как HackRF One и USRP, позволяют злоумышленникам динамически настраивать частотные диапазоны, модуляцию и протоколы для перехвата электромагнитных излучений.

AI-методы, включая нейронные сети и машинное обучение, автоматизируют обработку перехваченных сигналов. Глубокое обучение (Deep Learning) используется для классификации паттернов в электромагнитных излучениях. Например, сверточные нейросети (CNN) восстанавливают изображения с экранов мониторов по их ПЭМИН, даже если сигнал зашумлен. AI также может применяется для обхода защитных мер.

Например, генеративно-состязательные сети (GAN) имитируют «легитимные» электромагнитные шумы, маскируя атаки.

Таким образом, комбинация SDR и AI создает угрозы, недоступные ранее:

– масштабируемость атак – SDR-массивы с AI-управлением одновременно сканируют десятки частот, выявляя уязвимые устройства [1];

– адаптивность: AI в реальном времени корректирует параметры SDR для перехвата слабых сигналов, например, от ноутбуков в экранированных помещениях [2].

Наряду с вышеперечисленными преимуществами применение технологий SDR и AI имеют ряд ограничений, связанных с тем, что обработка больших объемов данных SDR требует мощных графических процессоров, а шумы от других устройств снижают точность анализа [3].

SDR-устройства (например, HackRF One) перехватывают электромагнитные излучения от USB-клавиатур. Каждое нажатие клавиши генерирует уникальный сигнал, который фиксируется в диапазоне 10–50 МГц. Применение алгоритмов машинного обучения (RNN – рекуррентные нейронные сети) позволило достичь 97 % точности в распознавании текста даже на расстоянии 10 метров от цели. Атака возможна через стены, что делает ее критичной для офисных и промышленных объектов. Для защиты информации от утечки необходимо использовать экранированные кабели и клавиатуры с низким уровнем излучений либо внедрять шифрование данных на физическом уровне [3].

Представлена методика восстановления изображений с экранов мониторов по их электромагнитным излучениям. SDR-приемники (USRP B210) фиксировали сигналы в диапазоне 30–500 МГц, а сверточные нейросети (CNN) обрабатывали зашумленные данные. Технология позволяет восстанавливать текст и графику с разрешением до 1024×768 пикселей, работать через бетонные стены толщиной до 30 см. В лабораторных условиях удалось восстановить текстовый документ, отображавшийся на экране ноутбука, находящемся в соседнем помещении [2].

Выявлены уязвимости в промышленных датчиках, используемых на энергетических объектах. Атака заключалась в перехвате сигналов на частоте 2,4 ГГц через SDR-устройства и декодировании данных с помощью AI-моделей (алгоритмы кластеризации). Был получен доступ к информации о состоянии оборудования (температура, давление), а также возможность дистанционного отключения систем безопасности [4].

Продемонстрирована уязвимость IP-камер, передающих данные по Wi-Fi. SDR-приемники перехватывали сигналы в диапазоне 5 ГГц, а AI-алгоритмы обходили шифрование WPA3 за счет анализа временных задержек (side-channel attack). Атака требует менее 10 минут на расшифровку ключа. 67% камер на базе чипов HiSilicon оказались уязвимы к такому виду атак.

Согласно отчету Munich Security Conference (2025), 40% киберинцидентов, связанных с ПЭМИН, приходится на критическую инфраструктуру (оборона, энергетика, здравоохранение), например, в 2024 г. перехват данных с медицинских томографов в Германии привел к утечке персональных данных 50 тыс. пациентов [5].

Заключение

Развитие SDR и AI делает атаки через ПЭМИН более изощренными. Для защиты требуется сочетание традиционных методов (экранирование) и инноваций (AI-анализ). Исследования 2020–2025 гг. подчеркивают необходимость обновления стандартов информационной безопасности.

Список использованных источников / References

1. «Защита информации от ПЭМИН в условиях цифровизации» / Информационные технологии и безопасность. – 2023. – № 4. – С. 45–53.
2. «SDR-Based Eavesdropping of Video Signals via Electromagnetic Emanations» / Proceedings of the ACM Conference on Computer and Communications Security. – 2023. – P. 45–58.
3. «EM Side-Channel Attacks on Keyboards Using Deep Learning» / IEEE Transactions on Information Forensics and Security. – 2022. – Vol. 17. – P. 1–12.
4. Bastille Networks Research / Technical Report: IoT Vulnerabilities in Industrial Sensors. – 2024. – 30 p. – URL: https://www.bastille.net/research/2024-iot (date of access: 27.02.2025).
5. Munich Security Conference Report / Cybersecurity in Critical Infrastructure. – 2025. – P. 112–125. – URL: https://securityconference.org/reports/2025 (date of access: 27.02.2025).

Сведения об авторах

Мартинкевич А.А. научный сотрудник, ГУО «Институт пограничной службы».
Майоров А.И. начальник отдела, ГУО «Институт пограничной службы».
Буневич М.А. научный сотрудник НИЛ 5.1, Научно-исследовательская часть учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», bunevich@bsuir.by.
Горбачев Д.В. старший преподаватель каф. ИСиТ, Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», d.gorbachev@bsuir.by.

Information about the authors

Martinkevich A., Researcher, State Educational Institution "Institute of Border Service"
Mayorov A. Head of Department, State Educational Institution "Institute of Border Service".
Bunevich M., Researcher, SRL 5.1 R&D Department of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", bunevich@bsuir.by.
Gorbachev D. Senior Lecturer, Department of Information Systems and Telecommunications, Institute of Information Technologies, Educational Institution "Belarusian State University of Informatics and Radioelectronics" d.gorbachev@bsuir.by.

УДК 004

ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Я.С. Мелещенко, В.В. Васькевич
Гомельский государственный университет имени Франциска Скорины, Гомель, Беларусь

Аннотация. В работе анализируются ключевые требования к обеспечению информационной безопасности в Республике Беларусь с приведением описания конкретных нормативно-правовых актов, регламентирующих вопросы обработки, хранения, передачи данных и вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Изложены основные факторы, способствующие совершению киберпреступлений и некоторые меры по защите информации, такие как правовые, организационные, технические, а также основные черты концепции информационной безопасности в стране. Описываются элементы национальной системы обеспечения кибербезопасности и акты, составленные в целях регулирования общественных отношений в данной сфере и обеспечения защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных. Рассматриваются общие принципы реализации и регулирования защиты информации действующим законодательством.
Ключевые слова: информационная безопасность; закон; информационное общество; постановление; персональные данные; указ; национальная система; центр кибербезопасности; аттестация; защита информации.

FUNDAMENTALS OF NORMATIVE LEGAL REGULATION IN THE FIELD OF INFORMATION PROTECTION IN THE REPUBLIC OF BELARUS

Y. Meleshchenko, V. Vaskevich
Francisk Skorina Gomel State University, Gomel, Belarus

Annotation. The article analyzes the key requirements for ensuring information security in the Republic of Belarus with a description of specific normative legal acts regulating the processing, storage, transmission of data and issues of ensuring national security, including the security of the information space, information infrastructure, information systems and resources. The main factors contributing to the commission of cybercrimes and some information protection measures, such as legal, organizational, technical, as well as the main features of the information security concept in the country, are outlined. The article describes the elements of the national cybersecurity system and acts drawn up to regulate public relations in this area and ensure the protection of personal data, the rights and freedoms of individuals when processing their personal data. The general principles of implementation and regulation of information protection by the current legislation are considered.
Keywords: information security; law; information society; resolution; personal data; decree; national system; cybersecurity center; attestation; information protection.

Введение

В условиях становления общества особую ценность обретает информация, а вопросы ее безопасности становятся все более актуальными. В настоящее время сложно выделить сферу общественной деятельности, в которой бы не применялись информационные технологии. Однако с увеличением доли населения, использующей информационные технологии, происходит увеличение количества преступлений в сфере ИТ. Совершению подобных преступлений способствуют компьютерная неграмотность сотрудников, отсутствие механизмов контроля и проверки поступающей электронной информации или недостаточность их реализации. Количество киберпреступлений в Беларуси в 2024 году составило более четверти от всех преступлений в стране [1].

В Республике Беларусь существует ряд требований законодательства, осуществляющих защиту информации. Защита информации - комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Основная часть

Основой нормативно-правового регулирования в рассматриваемой сфере является Закон РБ 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», которым регулируются общественные отношения, возникающие при:

– поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

– создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

– организации и обеспечении защиты информации.

В Законе определены некоторые меры по защите информации, такие как правовые, организационные, технические. К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также

ответственность сторон по договору за нарушение указанных условий. К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации. К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

18 марта 2019 г. Президентом было подписано постановление Совета Безопасности Республики Беларусь №1 «О Концепции информационной безопасности Республики Беларусь». В нем отмечено кардинальное повышение роли информационных технологий в реализации прав и свобод граждан, а также сопутствующие трансформации социума в информационное общество порождение новых рисков, вызовов и угроз, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Формирование в Республике Беларусь информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и прогрессивного развития, рассматривается как национальный приоритет и общегосударственная задача. Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности [2].

В рамках Закона РБ от 7 мая 2021 г. №99-З «О защите персональных данных» в целях обеспечения защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных было постановлено создать Национальный цент защиты персональных данных Республики Беларусь.

С целью обеспечения безопасности национальной информационной инфраструктуры в Республике Беларусь 14 февраля 2023 года бал подписан Указ Президента Республики Беларусь №40 «О кибербезопасности». В котором было постановлено о необходимости создать в Республике Беларусь национальную систему обеспечения кибербезопасности, элементами которой являются:

– Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ);

– Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности);

– Центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности);

– Оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (далее – авторизованный оператор электросвязи);

– Объекты информационной инфраструктуры государственных органов и иных организаций (далее - объекты информационной инфраструктуры);

– Сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в абзацах втором-пятом настоящего пункта [2].

Кроме того, указом определены основные задачи национальной системы обеспечения кибербезопасности.

Компании всех размеров сталкиваются с необходимостью защиты информации, так как кибератаки могут иметь серьезные последствия, включая финансовые потери, вред репутации, утрату доверия со стороны клиентов и нарушение сохранности интеллектуальной собственности, поэтому внедрение надежной системы кибербезопасности является не только соблюдением нормативных требований, но и стратегически важным решением.

25 июля 2023 вышел Приказ Оперативно-аналитического центра при президенте Республики Беларусь № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40». В нем подробно описаны условия, необходимые для обеспечения информационной безопасности, формализованы алгоритмы действий при возникновении киберинцидентов, также описана типовая структура центров кибербезопасности и требования к ним.

В настоящее время в Республике Беларусь созданы Оперативно-аналитический центр при Президенте Республики Беларусь и центры по кибербезопастности, 17 из которых прошли проверку ОАЦ. Их задача – предотвращение и минимизация последствий атак на объекты информационной инфраструктуры. Аттестация SOC (Security Operations Center) в Беларуси предусматривает проверку соответствия программных и аппаратных средств определенным требованиям, систем защиты информации и компетенций персонала. Центр кибербезопасности Республиканского унитарного предприятия «Национальный центр обмена трафиком» по приказу от 11.11.2023 №204 стал первым в Республике Беларусь аттестованным центром кибербезопасности. Таким образом в стране было положено начало официальной деятельности по защите информации. Первой в стране коммерческой организацией, получившей такую аттестацию, стало Общество с ограниченной ответственностью «Надежные программы» (приказ от 05.01.2024 №1) [3].

С развитием сферы кибербезопастности растет спрос на высококвалифицированных работников в этой сфере. Для подготовки специалистов в Республике Беларусь осуществляется набор на специальность «Кибербезопастность» в следующих вузах: Гомельский государственный университет имени Франциска Скорины, Гродненский государственный университет имени Янки Купалы, Белорусский государственный университет, Полоцкий государственный университет имени Евфросинии Полоцкой. Подготовка специалиста по данной специальности предполагает формирование определенных профессиональных компетенций, включающих знания и умения в области разработки и эксплуатации средств и систем защиты информации, осуществления контроля за их использованием. Специалист по кибербезопасности должен уметь защищать информационные системы от взломов, выявлять угрозы информационной безопасности и риски потери данных, обеспечивать сохранность и конфиденциальность данных.

Заключение

В современном мире информация – ценный продукт. Поэтому услуги по защите информации характеризуются высоким спросом и их актуальность подтверждается на законодательном уровне. Благодаря четко регламентируемой политике организаций по обеспечению защиты информации осуществляется построение национальной системы кибербезопасности.

Список использованных источников

1. Иванова, Д. Каждое четвертое преступление в Беларуси совершили кибермошенники. В ГУВД привели статистику 2024 года. [Электронный ресурс] / Д. Иванова // Минск новости: публикация. – 2024. – 13 ноября. – URL: https://minsknews.by/v-2024-godu-kiberprestupleniya-v-belarusi-sostavili-chetvert-ot-vseh-pravonarushenij/. – Дата доступа: 25.02.2025.

2. О концепции информационной безопасности Республики Беларусь: Постановление совета безопасности республики Беларусь от 18 марта 2019 г. №1 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – 2019. – 20 марта. – URL: https://pravo.by/document/?guid=3871&p0=P219s0001/. – Дата доступа: 25.02.2025.

3. Перечень аттестованных центров кибербезопасности [Электронный ресурс] // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: www.oac.gov.by/activity/cybersecurity-centers-list/certified-cybersecurity-centers/ – Дата доступа: 25.02.2025.

Сведения об авторах

Мелещенко Я.С., студентка 2 курса факультета физики и информационных технологий специальности «Кибербезопасность», Гомельский государственный университет имени Франциска Скорины, na.ya.mo@mail.ru.
Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, Гомельский государственный университет имени Франциска Скорины, vaskevich@gsu.by.

Information about the authors

Meleshchenko Y., 2nd year student of the Faculty of Physics and Information Technology specialty "Cybersecurity", Francysk Skaryna Gomel State University, na.ya.mo@mail.ru.
Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Francysk Skaryna Gomel State University, vaskevich@gsu.by.

УДК 004.8:004.056

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ ОРГАНИЗАЦИИ

С.Г. Михайловский
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Нарушители в настоящее время используют искусственный интеллект (ИИ) для автоматизации и улучшения кибератак на информационные системы организаций. ИИ сканирует системы, находит уязвимости и реализует кибератаки. Он помогает нарушителям без особых усилий получать данные, взламывать учетные записи и распространять вредоносное ПО. Машинное обучение (МО) и ИИ помогает нарушителям усовершенствовать свои методы, обойти защиту и имитировать обычное поведение пользователей. В статье раскрывается использование искусственного интеллекта, машинного обучения в обнаружении распределенных кибератаках типа DDoS (Distributed Denial of Service).

Ключевые слова: искусственный интеллект; платформы безопасности; байесовский алгоритм; DDoS-атака; машинное обучение; система обнаружения, модель обнаружения.

USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TO DETECT ATTACKS ON AN ORGANIZATION'S INFORMATION SYSTEM

S.G. Mikhailovsky
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Violators are currently using artificial intelligence (AI) to automate and improve cyber attacks on organizations' information systems. AI scans the system, finds vulnerabilities and implements cyber attacks. It helps violators effortlessly obtain data, hack accounts, and distribute malware. Machine learning (MO) and AI help violators improve their methods, bypass security, and mimic normal user behavior. The article reveals the

use of artificial intelligence and machine learning in detecting distributed cyber attacks such as DDoS (Distributed Denial of Service).
Keywords: artificial intelligence; security platforms; Bayesian algorithm; DDoS attack; machine learning; detection system, detection model.

Введение

DDoS – это вид кибератаки, при которой нарушители используют множество распределенных ресурсов для нанесения ущерба целевым объектам, что приводит к недоступности услуг для легитимных пользователей. Основными целями таких кибератак являются информационные системы организаций, пропускная способность сетей и другие критически важные ресурсы. DDoS-атаки считаются одними из самых распространенных и разрушительных кибератак, могут характеризоваться большим объемом трафика за короткий период времени, небольшим объемом трафика на протяжении длительного времени или значительным объемом трафика на протяжении длительного времени, и их сложно обнаружить, так как трафик, создаваемый во время атаки, часто не отличается от обычного сетевого трафика. В связи с развитием облачных вычислений, Интернета вещей (IoT) и технологий искусственного интеллекта DDoS-атаки продолжают эволюционировать, что делает их обнаружение и предотвращение все более сложной задачей, в том числе из-за невозможности отличить реальный траффик от нелегитимного. Методы классификации с помощью машинного обучения могут быть использованы для различения разных видов пакетов. Пакеты, классифицированные как атакующий трафик, будут отброшены. Некоторые признаки, позволяющие обнаружить DDoS-атаку, включают количество пакетов, средний размер пакета, разницу во временном интервале, разницу в размере пакета, количество байт, скорость передачи пакетов и битрейт.

Применение искусственного интеллекта для предотвращения DDoS-атак

Основные методы ИИ включают машинное обучение, распознавание речи и обработку естественного языка. Алгоритмы МО используются для обнаружения DDoS-атак и защиты от них, с акцентом на обнаружение аномалий. Основные методы включают байесовские алгоритмы, нейронные сети и машины опорных векторов для классификации и регрессии.

ИИ и МО применяются для обнаружения кибератак, используя подходы глубокого обучения, как показано на рисунке 1. Обнаружение DDoS-атак решает задачу классификации последовательностей, преобразуя обнаружение пакетов в обнаружение окон [1]. Подход включает CNN (Convolutional Neural Network), RNN (Recurrent Neural Network) и полностью связанные слои, причем RNN изучает объекты на входе от CNN.

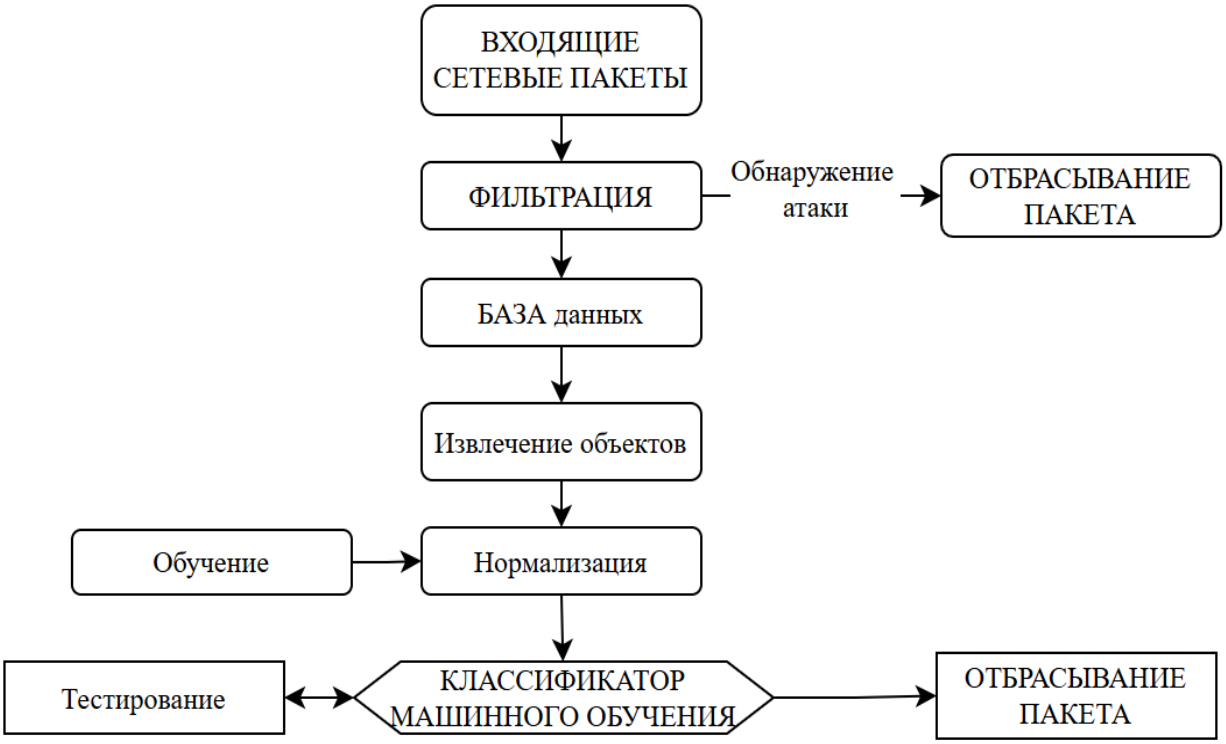


Рис. 1. Архитектура обнаружения DDoS-атак на основе машинного обучения
Fig. 1. DDoS attack detection architecture based on machine learning

На рис. 2 представлено обучение глубоких нейронных сетей с улучшенной устойчивостью к атакам – Deep Defense, представленной в одноименной научной работе, используя LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit) для масштабирования и отслеживания истории пакетов, при этом RNN превосходят random forest, как метод МО в обобщении [3].

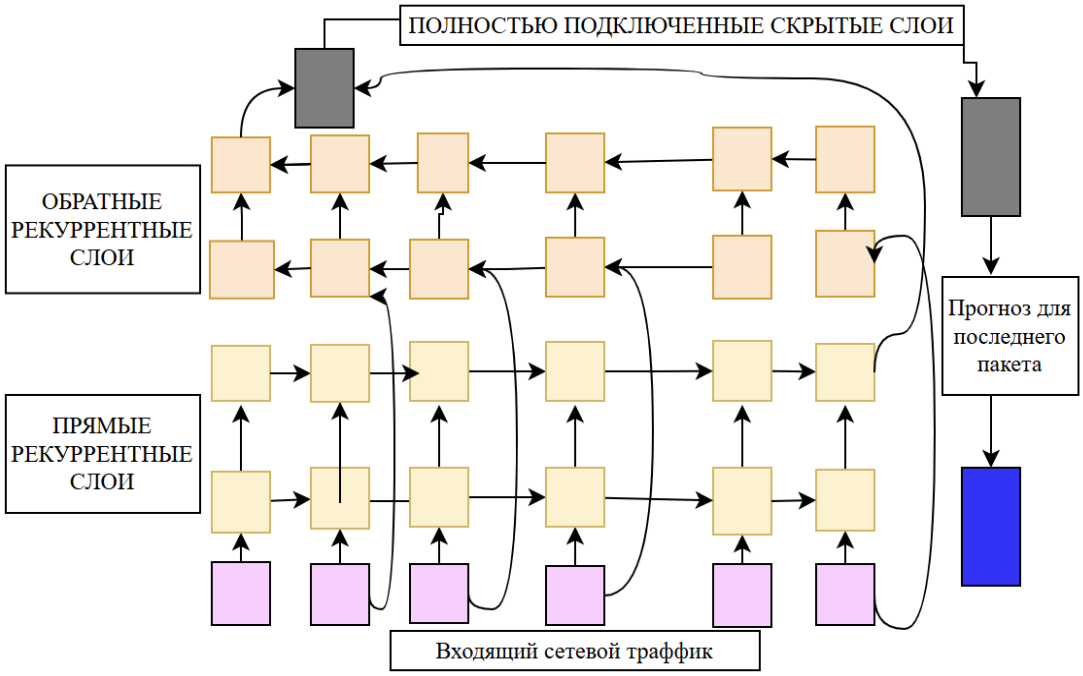


Рис. 2. Общая сетевая архитектура для Deep Defense
Fig. 2. Common network architecture for Deep Defense

Предполагается, что существует более продвинутый подход, в основе которого обнаружение DDoS-атак на основе нейронной сети, состоящая из пяти фазного сборщика пакетов, Hadoop HDFS (Hadoop HDFS (Hadoop Distributed File System, распределенной файловой системы, разработанная для хранения больших объемов данных), конвертера форматов, процессора обработки данных и модуля обнаружения нейронной сети [3].

На рис. 3 отражена архитектура, представляющая систему обнаружения, которая интегрирована с нейронной сетью для обнаружения DDoS-атак по семи параметрам. Система обнаружения может анализировать высокоскоростной и объемный сетевой трафик, а нейронная сеть может эффективно идентифицировать характеристики пакетов [2].

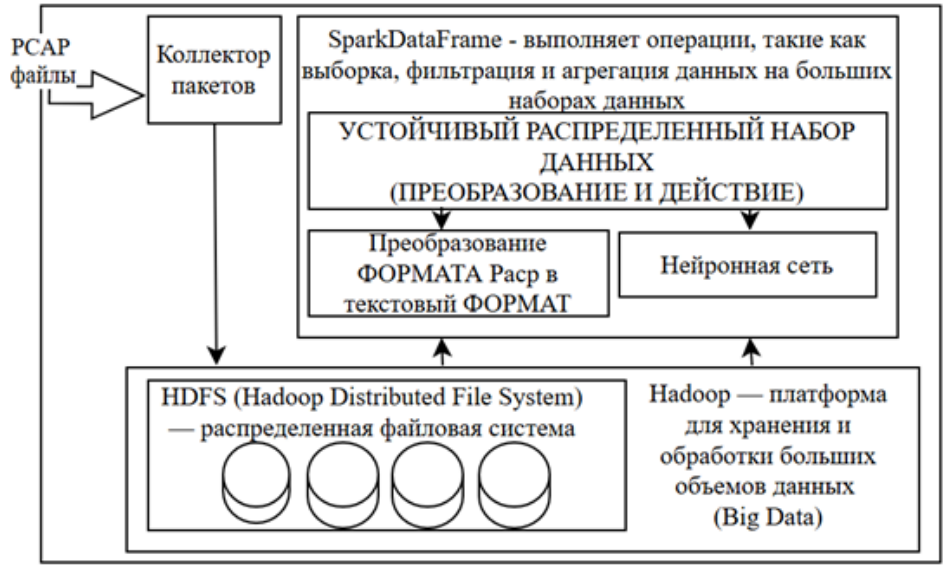


Рис. 3. Архитектура системы обнаружения
Fig. 3. Architecture of the detection system

В настоящее время предлагается более продвинутая концепция машинного обучения для противостояния к подобным кибератакам, в основе которой предположение, что все узлы модели обладают способностью к независимому обучению. Хорошо известный алгоритм кумулятивной суммы используется для обнаружения огромного объема трафика. Для распознавания структуры обычного трафика используются классификаторы и детекторы, такие как байесовский (Naive Bayes) алгоритм [2]. Каждый узел имеет алгоритм, который сравнивает накопленную сумму средних значений за каждую единицу времени с характерным пороговым значением для классификации сообщения. Этот механизм может остановить и избежать DDoS-атаки на ранней их стадии.

Одной из основных моделей обнаружения и смягчения последствий DDoS-атак может быть модель, использующая алгоритм машинного обучения, указанная на рис. 4.

Модель состоит из системы онлайн-мониторинга OMS (Online Monitoring System), модуля обнаружения мошеннического трафика и алгоритма ограничения скорости на основе интерфейса. OMS использует автоматизированные инструменты и скрипты для мониторинга ухудшения качества и предоставления измерений воздействия DDoS. Модуль обнаружения ложного трафика включает алгоритм проверки количества переходов для проверки подлинности входящего пакета. Он создает легитимные записи с указанием IP и количества переходов для обнаружения потенциальных кибератак. Алгоритм проверки количества переходов заключается

в проверке подлинности пакета. HCF-SVM (Hop Count Filtering – Support Vector Machine) обучается и обновляется с учетом IP-адреса источника и соответствующего количества переходов [2].

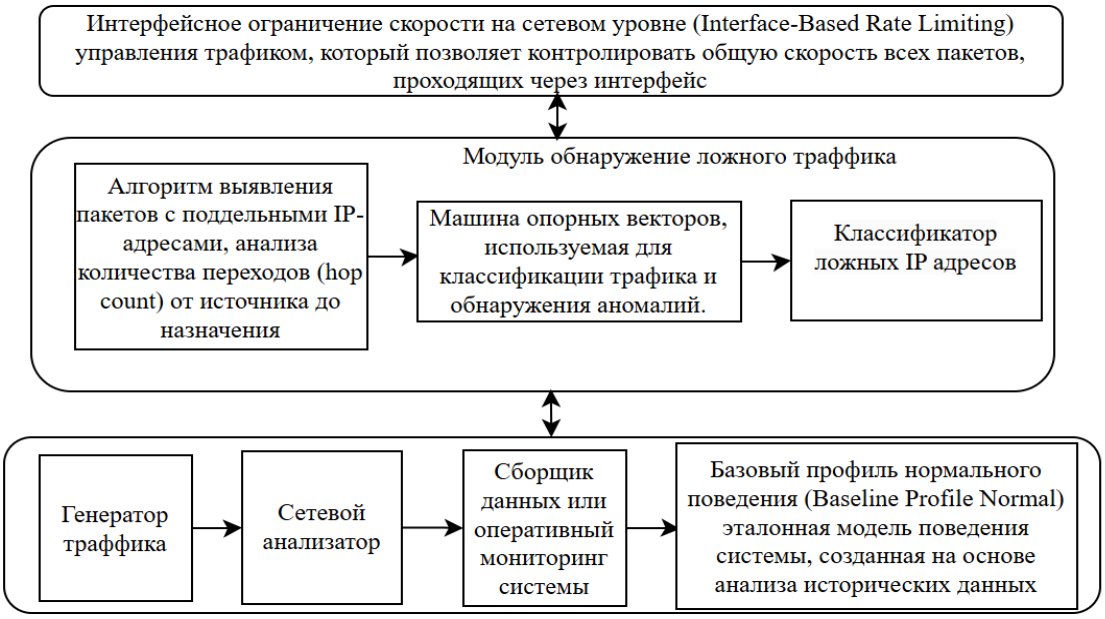


Рис. 4. Моделей обнаружения и смягчения последствий DDoS-атак
Fig. 4. DoS attack detection and mitigation models

Существуют и другие подходы обнаружения DDoS-атак, основанные на машинном обучении и применении ИИ:

1. Система обнаружения DDoS-атак на основе нейронной сети и внедряет в кластер Apache Hadoop и систему HBase. Система имеет архитектуру нейросети, которая обладает способностью адаптироваться к новым типам DDoS-атак. Кластер Hadoop и HBase настроен на обработку огромного трафика, затем нейросетевая модель разработана для обнаружения DDoS-атак;

2. Модель системы на основе ANN (Artificial Neural Network) и статистической информации заголовка пакета для обнаружения DDoS-атаки с усилением DNS [3]. Они классифицируют DNS-трафик с использованием алгоритмов классификации МО, включая дерево решений, многоуровневое восприятие MLP (Multi-Layer Perception), байесовский алгоритм и SVM (Support Vector Machine) метод машинного обучения, который используется для классификации и регрессии данных. Затем осуществляется отбор дерева решений в качестве модели классификации МО для достижения наилучшей эффективности;

3. Система, основанная на простой сетевой архитектуре, которая использует реальный веб-сервер, сервер-приманку и веб-серверы-приманки для отличия трафика DDoS от обычного трафика. В архитектуре используется настроенная система предотвращения вторжений на сетевом шлюзе, которая использует правила, генерируемые случайным деревом алгоритм машинного обучения посредством контролируемого обучения. Дерево решений выбирается для целей выделения вредоносного трафика из нормального трафика. Случайное дерево алгоритма машинного обучения с использованием, маркированного наборов данных, используется для целей минимизации риска формирования ложного положительных трафика.

Заключение

DDoS-атаки по-прежнему остаются существенными угрозами для организаций и людей и могут принести большие убытки. Некоторые методы использования ИИ, такие как алгоритмы МО, могут использоваться для классификации трафика DDoS-атак и обнаружения DDoS-атак, важен в этом вопросе прогресс в обнаружении DDoS-атак с использованием методов МО и ИИ, которые обладают возможностями их обнаружения.

Список использованных источников

1. Воробьева Ю.Н. (2018) Нейросетевая модель выявления DDOS-атак. *Вестник технологического университета*. 21 (2), 94-98.

2. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. (2016) Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва, Горячая линия-Телеком.

3. Аль-тамими Мохалад Мохсин Абдульхасан, Алзагир Аббас Али Хасан (2024) Повышение сетевой безопасности с помощью подхода глубокого обучения RNN, *Вычислительные нанотехнологии*. 11 (4), 114-122.

References

1. Vorobyeva Yu.N. (2018) Neural network model for detecting DDOS attacks. Bulletin of the Technological University. 21 (2), 94-98.

2. Shelukhin O.I., Sakalema D.J., Filinova A.S. (2016) Intrusion detection in computer networks (network anomalies). Moscow, Hotline-Telecom.

3. Al-tamimi Mohammad Mohsin Abdel Hassan, Alagir Abbas Ali Hassan (2024) Improving network security through the RNN deep learning approach, Computational Nanotechnology. 11 (4), 114-122.

Сведения об авторе

Михайловский С.Г., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mikhailouski@mikhailouski.ru.

Information about the author

Mikhailovsky S.G., Master's student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mikhailouski@mikhailouski.ru.

УДК 004.056

ЭЛЕМЕНТНАЯ БАЗА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

К.В. Михно, А.С. Герасимов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Защита информации от несанкционированного доступа, утечек и искажений представляет собой важную задачу для организаций и государственных структур. Далее рассмотрим основные элементы средств защиты информации (СЗИ), включая аппаратные и программные компоненты, принципы их работы и примеры применения в различных сферах. Также обсуждаются вызовы и перспективы развития элементной базы в условиях цифровой трансформации и появлении новых угроз, таких как квантовые компьютеры.

Ключевые слова: защита информации; конфиденциальность; целостность; доступность данных; аппаратные средства; программные средства; криптография; аутентификация; квантовые компьютеры; IoT.

ELEMENT BASE OF INFORMATION SECURITY MEANS

K.V. Mikhno, A.S. Gerasimov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Protecting information from unauthorized access, leaks, and tampering is a critical task for organizations and government structures. This article examines the key elements of information security means (ISM), including hardware and software components, their working principles, and examples of their application in various fields. Additionally, the challenges and prospects of developing the element base in the context of digital transformation and emerging threats, such as quantum computers, are discussed.
Keywords: Information security; confidentiality; integrity; data availability; hardware means; software means; cryptography; authentication; quantum computers; IoT.

Введение

В современном мире информация стала одним из самых ценных ресурсов. Ее защита от несанкционированного доступа, утечек и искажений является важнейшей задачей для организаций, государственных структур и частных лиц. Средства защиты информации (СЗИ) представляют собой комплекс технических, программных и организационных мер, направленных на обеспечение конфиденциальности, целостности и доступности данных. Одним из ключевых компонентов СЗИ является элементная база – набор аппаратных и программных элементов, которые обеспечивают выполнение функций защиты. В данном докладе рассматриваются основные элементы средств защиты информации, их классификация, принципы работы и примеры применения.

Основная часть

Элементная база средств защиты информации включает в себя широкий спектр устройств, программ и технологий. Аппаратные средства защиты информации представляют собой физические устройства, которые обеспечивают защиту данных на уровне оборудования. К ним относятся криптографические модули, такие как HSM (Hardware Security Module), которые используются для защиты ключей шифрования и выполнения криптографических операций. Эти устройства часто применяются в банковской сфере для защиты транзакций и хранения ключей.

Аппаратные файрволы обеспечивают высокую производительность и надежность, что делает их незаменимыми в крупных корпоративных сетях. Сканеры безопасности обнаруживают уязвимости в сетевой инфраструктуре, такие как открытые порты или неправильно настроенные серверы. Эти устройства помогают предотвратить атаки, направленные на эксплуатацию уязвимостей.

Биометрические системы обеспечивают аутентификацию пользователей на основе уникальных биометрических данных, таких как отпечатки пальцев, радужная оболочка глаза или голос. Эти системы широко применяются в государственных структурах и корпоративной среде для защиты конфиденциальной информации.

Программные средства защиты информации включают в себя программы и приложения, которые обеспечивают защиту данных на уровне программного обеспечения. Антивирусные программы предназначены для обнаружения и удаления вредоносного программного обеспечения. Они используют базы данных сигнатур вирусов и методы эвристического анализа для выявления новых угроз.

Системы обнаружения вторжений (IDS) анализируют сетевой трафик и выявляют подозрительную активность. Они могут быть основаны на сигнатурах известных атак или использовать методы машинного обучения для обнаружения аномалий. Программные криптографические модули реализуют алгоритмы шифрования, такие как AES, RSA или ECC. Эти модули используются для защиты данных при передаче по сети или хранении на устройствах.

Системы управления ключами обеспечивают генерацию, хранение и распределение криптографических ключей. Они играют важную роль в обеспечении безопасности криптографических операций.

Некоторые средства защиты информации сочетают в себе аппаратные и программные компоненты. Например, смарт-карты содержат встроенный микропроцессор и программное обеспечение для выполнения криптографических операций. Они широко используются в банковской сфере и для защиты доступа к корпоративным сетям. Токены генерируют одноразовые пароли или хранят криптографические ключи. Эти устройства обеспечивают дополнительный уровень безопасности при аутентификации пользователей.

Элементная база средств защиты информации работает на основе нескольких ключевых принципов. Шифрование данных является одним из основных методов защиты информации. Оно преобразует данные в зашифрованную форму, которая может быть расшифрована только с использованием правильного ключа. Современные криптографические алгоритмы, такие как AES или RSA, обеспечивают высокий уровень защиты. AES (Advanced Encryption Standard) используется для шифрования данных в банковской сфере, государственных структурах и корпоративных сетях. RSA (Rivest-Shamir-Adleman) применяется для цифровых подписей и обмена ключами.

Аутентификация и авторизация – это процессы проверки подлинности пользователя или устройства и предоставления доступа к ресурсам на основе прав пользователя. Для аутентификации используются пароли, биометрические данные или токены. Биометрические системы обеспечивают высокий уровень безопасности, так как биометрические данные уникальны для каждого человека.

Системы контроля доступа ограничивают доступ к информации на основе политик безопасности. Например, доступ к определенным файлам или каталогам может быть разрешен только определенным пользователям или группам. Эти системы широко применяются в корпоративной среде для защиты конфиденциальной информации.

Системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS) анализируют сетевой трафик и выявляют подозрительную активность. В случае обнаружения атаки система может заблокировать подозрительный трафик или уведомить администратора. Эти системы играют важную роль в обеспечении безопасности корпоративных сетей и государственных структур.

Элементная база средств защиты информации широко применяется в различных сферах. В банковской сфере используются аппаратные криптографические модули (HSM) для защиты транзакций и хранения ключей шифрования. Смарт-карты и токены применяются для аутентификации клиентов и сотрудников.

В государственных структурах используются системы контроля доступа и биометрические системы для защиты конфиденциальной информации. Сетевые экраны и системы обнаружения вторжений обеспечивают безопасность государственных сетей.

В корпоративной среде применяются антивирусные программы, системы управления ключами и программные криптографические модули. Компании также

используют VPN (Virtual Private Network) для защиты данных при передаче по публичным сетям.

В IoT-устройствах используются легкие криптографические алгоритмы, которые обеспечивают защиту данных при ограниченных вычислительных ресурсах. Также применяются системы аутентификации и контроля доступа.

С развитием технологий возникают новые вызовы для элементной базы средств защиты информации. Одним из наиболее серьезных вызовов является развитие квантовых компьютеров, которые могут взломать многие из существующих криптографических алгоритмов. В ответ на эту угрозу разрабатываются постквантовые криптографические алгоритмы, которые устойчивы к атакам с использованием квантовых вычислений.

Еще одним вызовом является рост числа IoT-устройств, которые часто имеют ограниченные вычислительные ресурсы и уязвимы для атак. Для защиты таких устройств разрабатываются специализированные криптографические алгоритмы и системы управления ключами.

Перспективным направлением развития элементной базы является интеграция искусственного интеллекта и машинного обучения в системы защиты информации. Искусственный интеллект может использоваться для анализа больших объемов данных и выявления аномалий, которые могут свидетельствовать о кибератаках.

Заключение

Элементная база средств защиты информации играет ключевую роль в обеспечении безопасности данных. Она включает в себя широкий спектр аппаратных и программных элементов, которые обеспечивают конфиденциальность, целостность и доступность информации. С развитием технологий элементная база продолжает эволюционировать, адаптируясь к новым угрозам и вызовам.

Будущее элементной базы связано с разработкой новых криптографических алгоритмов, интеграцией искусственного интеллекта и созданием специализированных решений для защиты IoT-устройств. Эти направления будут определять развитие средств защиты информации в ближайшие годы.

Список использованных источников

1. Гришина Н.В. Основы информационной безопасности предприятия. Учебное пособие. М.: Инфра-М. 2021. 216 с.

2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана. 2024. 252 с.

3. Жарова А.К. Защита информации ограниченного доступа, получаемой по цифровым каналам передачи информации о совершаемых коррупционных правонарушениях // Государственная власть и местное самоуправление. 2023. № 9. С. 37 – 41.

4. Зенков А.В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.

5. Зенков А.В. Основы информационной безопасности. Учебное пособие. М.: Инфра-Инженерия. 2022. 104 с.

References

1. Grishina N.V. Fundamentals of Enterprise Information Security. Textbook. Moscow: Infra-M. 2021. 216 p.

2. Bondarev V.V. Introduction to Information Security of Automated Systems. Moscow: Bauman Moscow State Technical University. 2024. 252 p.

3. Zharova A.K. Protection of Restricted Access Information Received Through Digital Communication Channels About Committed Corruption Offenses. State Power and Local Self-Government. 2023. No. 9. pp. 37–41.

4. Zenkov A.V. Information Security and Data Protection. Moscow: Yurayt. 2023. 108 p.
5. Zenkov A.V. Fundamentals of Information Security. Textbook. Moscow: Infra-Engineering. 2022. 104 p.

Сведения об авторах

Михно К.В., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mihnokirill.bsuir@gmail.com.
Герасимов А.С., магистр, старший преподаватель, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.gerasimov@bsuir.by.

Information about the authors

Mixno K.V., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mihnokirill.bsuir@gmail.com.
Gerasimov A.S., Master, Senior Lecturer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.gerasimov@bsuir.by.

УДК 621.794.61

ИССЛЕДОВАНИЕ ЭЛЕКТРОННО-ФОНОННОГО ВЗАИМОДЕЙСТВИЯ В ГРАФЕНЕ, МОДИФИЦИРОВАННОМ АТОМАМИ ФТОРА

В.Н. Мищенко, А.Д. Васютич, П.А. Матусевич, А.В. Турло
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Графен, обладающий высокой подвижностью носителей заряда, которая превышает подвижность носителей заряда для всех известных материалов, рассматривается в настоящее время как один из наиболее перспективных материалов для создания новых полупроводниковых приборов. Приведены результаты моделирования интенсивностей рассеивания электронов на акустических и оптических фононах в слое графена, который модифицирован атомами фтора, без учета воздействия подложки. При моделировании этих интенсивностей рассмотрен вариант одновременного протекания процессов излучения и поглощения фононов. Полученные зависимости интенсивностей рассеивания носителей заряда позволят путем моделирования с использованием метода Монте Карло исследовать основные характеристики переноса носителей заряда в полупроводниковых структурах, содержащих слои модифицированного графена. Полученные в результате моделирования характеристики и параметры рассмотренного соединения могут быть использованы для создания новых гетероструктурных приборов, обладающих улучшенными выходными характеристиками.
Ключевые слова: графен; фтор; фонон; моделирование; полупроводниковая структура.

STUDY OF ELECTRON-PHONON INTERACTION IN GRAPHENE MODIFIED BY FLUORINE ATOMS

V.N. Mishchanka, A.D. Vasiutich, P.A. Matusevich, A.V. Turlo
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Graphene, which has a high mobility of charge carriers, which exceeds the mobility of charge carriers for all known materials, is currently considered as one of the most promising materials for the creation of new semiconductor devices. The results of modelling of electron scattering intensities on acoustic and optical phonons in a layer of graphene, which is modified by fluorine atoms, without taking into account the influence of the substrate, are presented. When modelling these intensities, a variant of simultaneous emission and absorption of phonons is considered. The obtained dependences of the charge carrier scattering intensities will allow us to investigate the main characteristics of the charge carrier transfer in semiconductor structures containing layers of modified graphene by means of Monte Carlo simulations. The characteristics and parameters of the considered compound obtained as a result of modelling can be used to create new hetero-structural devices with improved output characteristics.
Keywords: graphene; fluorine; phonon; modelling; semiconductor structure.

Введение

Графен является перспективным материалом для разработки новых полупроводниковых приборов и структур [1, 2]. Исследование процессов переноса носителей заряда для полупроводниковых соединений, содержащих слои графена, является актуальной задачей, которая связана с разработкой быстродействующих и мощных приборов диапазонов СВЧ и КВЧ, а также оптического диапазона частот. Для анализа полупроводниковых структур широкое применение находит использование статистического метода Монте Карло. Одной из основных особенностей этого метода является то, что он позволяет учесть процессы рассеяния носителей заряда в полупроводнике и исследовать работу полупроводниковых приборов в разных условиях функционирования. В полупроводниковых структурах важное место занимают процессы электронно-фононного взаимодействия (ЭФВ), среди которых основную роль занимают процессы рассеивания электронов на оптических и акустических фононах [3, 4]. В данной работе проведено ab initio исследование свойств ЭФВ, связанного с рассеиванием электронов на оптических и акустических фононах в графене, модифицированным атомами фтора. Полученные результаты моделирования позволяют определить вклад различных составляющих ЭФВ в общем процессе рассеивания носителей заряда.

Метод и результаты моделирования интенсивностей электрон-фононных взаимодействий в графене, модифицированным атомами фтора

Моделирование из первых принципов было выполнено с помощью программных комплексов Quantum Espresso [5] и EPW [6], используя параметризацию Perdew-Burke-Ernzerhof (PBE) в рамках приближения локальной плотности (LDA). Программный комплекс Quantum Espresso позволяет выполнить самосогласованное энергетическое моделированием и расчет электронно-фононных динамических матриц. При моделировании в программном комплексе Quantum Espresso были использованы псевдопотенциалы вида Norm-conserving и следующие параметры моделирования: энергия отсечки волновой функции составляла величину 60 Ry (1 Ry ≈ 13,605 эВ), энергия отсечки плотности заряда и потенциалов - 240 Ry. Зона Бриллюэна (BZ) была представлена с помощью сетки Монкхорста-Пака размером 12 x 12 x 1 [7]. Для устранения возможных паразитных осцилляций энергии при выполнении моделирования к рассматриваемой структуре добавлялся слой вакуума толщиной 20 Å (1 Å = $1 \cdot 10^{-10}$ м).

Для моделирования интенсивностей (скоростей) электронно-фононного взаимодействия был использован программный комплекс EPW [6].

Дисперсионные фононные зависимости графена, модифицированного атомами фтора, рассматриваются для мод вида ZA, TA, LA, ZO, TO, LO, LB, TB, LB*, TB*, ZS, ZS* [8]. Результаты моделирования интенсивностей рассеивания для мод LA (продольное направление и взаимодействие с акустическими фононами) и LO (продольное направление и взаимодействие с оптическими фононами) от энергии, полученные в программе EPW, представлены на рис. 1-2 в виде массивов цветных точек. Полученные массивы точечных данных были далее подвергнуты аппроксимации с помощью аналитических степенных функций в программе для обработки данных и построения графиков ORIGIN при выполнении операций Fitting и Polinomial Fit в разделе Analysis [9].

При выполнении этих операций в программе ORIGIN обеспечивается получение аналитических зависимостей при минимальной величине ошибок при аппроксимации. Была выполнена аппроксимация данных моделирования из первых принципов для мод LA и LO для интенсивностей рассеивания τ^{-1}, имеющих размерность s^{-1}, от величины энергии E, имеющей размерность eV. Используя полученные аналитические зависимости, были построены кривые 1, представленные на рис. 1, 2. Использование аналитических зависимостей дает возможность выполнить сравнительный анализ поведения интенсивностей рассеивания для перечисленных выше мод и применить эти данные для программного комплекса, который использует метод Монте-Карло, при анализе полупроводниковых приборов.

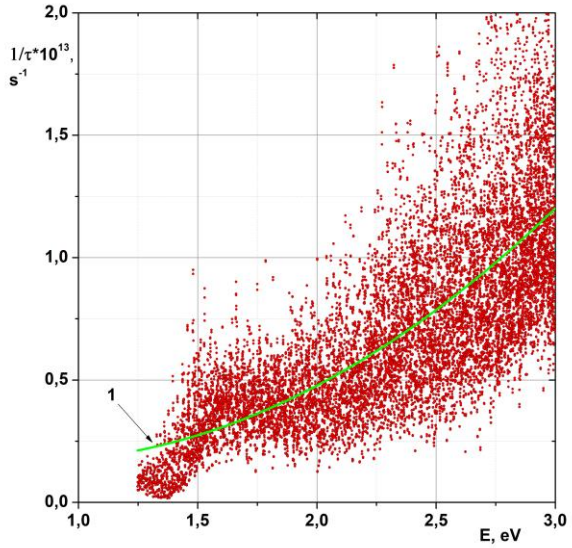


Рис. 1. Зависимость интенсивности рассеивания для акустической моды LA от энергии
Fig. 1. Dependence of the scattering intensity for the LA acoustic mode on energy

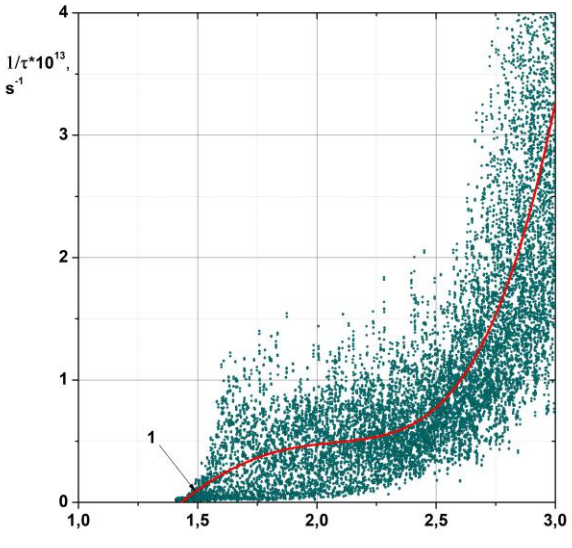


Рис. 2. Зависимость интенсивности рассеивания для оптической моды LO от энергии
Fig. 2. Dependence of the scattering intensity for the optical mode LO on the energy

Заключение

Приведены результаты исследования взаимодействия электронов с акустическими и оптическими фононами в графене, который модифицирован атомами фтора, без учета влияния подложки. При моделировании из первых принципов для мод вида ZA, TA, LA, ZO, TO, LO, LB, TB, LB*, TB*, ZS, ZS*, которые наблюдаются в этом материале, получены интенсивности рассеиваний электронов при одновременном протекании процессов излучения и поглощения фононов. Представленные зависимости и параметры интенсивностей рассеиваний электронов на акустических и оптических фононах в графене, который модифицирован атомами фтора, могут служить основой для моделирования новых гетероструктурных приборов, содержащих этот и другие полупроводниковые материалы.

Список использованных источников / References

1. Novoselov K. S., Geim A. K., et al. (2004) Electric field effect in atomically thin carbon film. *Science*, 306, 666-669.

2. Morozov, V. S., et al. (2008) Giant intrinsic carrier mobilities in graphene and its bilayer. *Phys. Rev. Lett.* 100, 016602.

3. Hess K. (1999) *Advanced Theory of Semiconductor Devices.* Wiley-IEEE Press, Piscataway, NJ.

4. Lundstrom M. (2009) *Fundamentals of Carrier Transport*. Cambridge University Press, Cambridge, UK.

5. Giannozzi P., Baroni S., Bonini N., Calandra M., Car R., Cavazzoni C., et al. (2009) QUANTUM ESPRESSO: a modular and open-source software project for quantum simulations of materials. *J. Phys.: Condens. Matter.* 21. 395502.

6. Lee H., Poncé S., Bushick K., Hajinazar S., Lafuente-Bartolome J., Leveillee J., et al. (2023) Electron-phonon physics from first principles using the EPW code. *npj Computational Materials*. 9. 156.

7. Mishchanka V.N. **(**2024) First-principles modeling of electron-phonon scattering rates in graphene. *Modern Electronic Materials.* 10 (3). 177-184.

8. Long Cheng, Chenmu Zhang and Yuanyue Liu. (2019) How to resolve a phonon-associated property into contributions of basic phonon modes *J. Phys.: Mater.* 2. 045005.

9. Isakova O. P., Tarasevich Y. Y., Yuzyuk Y. I. (2009) *Processing and visualization of data from physical experiments using Origin package*. Moscow: LIB-COM Book House. 136.

Сведения об авторах

Мищенко В.Н., канд. техн. наук, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mishchenko@bsuir.by.
Васютич А.Д., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», andrew.andrew22@mail.ru.
Матусевич П.А., инженер, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», koalapavel@mail.ru.
Турло А.В., инженер, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.turlo@bsuir.by.

Information about the authors

Mishchanka V.N., PhD, associate professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mishchenko@bsuir.by.
Vasiutich A.D., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", andrew.andrew22@mail.ru.
Matusevich P.A., engineer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", koalapavel@mail.ru.
Turlo A.V., engineer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.turlo@bsuir.by.

УДК *004.056.55*

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

А.Н. Морозова, А.Ю. Ефремова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В современных условиях системы видеонаблюдения широко используются для обеспечения безопасности и мониторинга различных объектов. Однако с ростом их популярности увеличивается и количество угроз, связанных с несанкционированным доступом к видеоданным. В данной статье рассматриваются основные методы и технологии технической защиты информации в системах видеонаблюдения, включая шифрование данных, аутентификацию пользователей, безопасную конфигурацию сети и физическую защиту оборудования. Особое внимание уделяется современным стандартам и протоколам, таким как ONVIF и DEPA, обеспечивающим совместимость и безопасность компонентов систем видеонаблюдения. Рассмотрены также рекомендации по регулярному обновлению программного обеспечения и управлению уязвимостями для повышения уровня защиты видеоданных.
Ключевые слова: видеонаблюдение; информационная безопасность; шифрование данных; аутентификация; ONVIF; DEPA; кибербезопасность; защита информации; сетевые протоколы; обновление ПО.

TECHNICAL PROTECTION OF INFORMATION IN VIDEO SURVEILLANCE SYSTEMS

A.N. Morozova, A.Y. Yafremava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In modern conditions, video surveillance systems are widely used to ensure the security and monitoring of various objects. However, with their growing popularity, the number of threats related to unauthorized access to video data is also increasing. This article discusses the main methods and technologies for the technical protection of information in video surveillance systems, including data encryption, user authentication, secure network configuration, and physical equipment protection. Particular attention is paid to modern standards and protocols, such as ONVIF and DEPA, which ensure compatibility and security of video surveillance system components. Recommendations for regular software updates and vulnerability management are also considered to enhance the level of video data protection.
Keywords: video surveillance; information security; data encryption; authentication; ONVIF; DEPA; cybersecurity; information protection; network protocols; software updates.

Введение

Системы видеонаблюдения стали неотъемлемой частью современных средств обеспечения безопасности, применяясь в различных сферах – от частных домов до крупных промышленных объектов. Однако интеграция таких систем в общие сети и их подключение к интернету повышают риски несанкционированного доступа к видеоданным. Для эффективной защиты информации в системах видеонаблюдения необходимо применять комплексный подход, включающий как технические, так и организационные меры.

Основная часть

Шифрование видеоданных является одним из ключевых методов защиты информации. Применение алгоритмов шифрования, таких как AES (Advanced Encryption Standard), позволяет преобразовать видеопоток в формат, недоступный для несанкционированного просмотра, обеспечивая конфиденциальность и целостность данных. Шифрование должно применяться как при передаче данных по сети, так и при их хранении на носителях.

Аутентификация и управление доступом. Надежная аутентификация пользователей предотвращает несанкционированный доступ к системе видеонаблюдения. Рекомендуется внедрение многофакторной аутентификации, требующей от пользователя предоставления нескольких подтверждений личности, таких как пароль и одноразовый код. Кроме того, необходимо использовать сложные, уникальные пароли для всех устройств и учетных записей, а также регулярно их обновлять:

– безопасная конфигурация сети;

– правильная настройка сети играет важную роль в защите систем видеонаблюдения.

Основные меры включают:

– сегментация сети: разделение сети видеонаблюдения и общей корпоративной сети для ограничения потенциальных путей атаки;

– использование брандмауэров: контроль входящего и исходящего трафика для предотвращения несанкционированного доступа.

– внедрение VPN: обеспечение безопасного удаленного доступа к системе через виртуальные частные сети;

– отключение ненужных сервисов: минимизация потенциальных уязвимостей путем деактивации неиспользуемых сетевых служб и портов.

Стандарты и протоколы безопасности:

– ONVIF (Open Network Video Interface Forum): международная организация, разрабатывающая стандарты для взаимодействия различных устройств в системах безопасности. Использование оборудования, соответствующего стандартам ONVIF, обеспечивает совместимость и повышает уровень безопасности системы;

– DEPA (Distributed Enhanced Processing Architecture): архитектура, предложенная компанией Sony, предусматривающая распределение вычислительных ресурсов между компонентами системы видеонаблюдения. Это позволяет улучшить обработку данных и повысить устойчивость системы к отказам.

Физическая защита оборудования:

– физическая безопасность компонентов системы видеонаблюдения предотвращает прямой доступ злоумышленников к устройствам.

Рекомендуемые меры включают:

– установка камер в труднодоступных местах: размещение оборудования на высоте или в защищенных корпусах для предотвращения физического вмешательства;

– защита кабелей связи: использование бронированных или скрытых каналов прокладки кабелей для предотвращения их повреждения или перехвата сигнала.

Рис. 1. Бронированный кабель
Fig. 1. Armored cable

Контроль доступа в серверные помещения: ограничение физического доступа к серверам и устройствам хранения видеозаписей.

Комплексный подход к защите информации в системах видеонаблюдения включает не только программные, но и аппаратные меры безопасности. Применение современных алгоритмов шифрования, надежной аутентификации и управления доступом, а также использование передовых стандартов и архитектурных решений позволяет минимизировать риски утечек данных. При этом физическая защита оборудования и грамотная конфигурация сети играют важную роль в обеспечении надежности всей системы. Совокупность этих мер позволяет значительно повысить уровень безопасности и устойчивость видеонаблюдения к различным угрозам.

Заключение

Для обеспечения надежной технической защиты информации в системах видеонаблюдения необходимо применять комплексный подход, включающий шифрование данных, многофакторную аутентификацию, безопасную конфигурацию сети, использование стандартов безопасности и физическую защиту оборудования.

Регулярное обновление программного обеспечения и мониторинг уязвимостей также играют важную роль в снижении рисков несанкционированного доступа и обеспечения высокого уровня безопасности видеоданных.

Список использованных источников

1. Тельный А.В. Инженерно-техническая защита информации. Системы охранного телевидения: учебное пособие. – Владимир: ВлГУ, 2013. – 143 с..

2. Березкин Р.В., Власова Г.А. Аспекты применения криптографической защиты информации в системах видеонаблюдения // Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск, 5 июня 2018 г. – Минск: БГУИР, 2018. – С. 20.

3. Алефиренко, В. М. Технологии защиты информации от несанкционированного доступа в системах видеонаблюдения / В. М. Алефиренко, А. Н. Морозова // Современные средства связи : материалы XXIX Международной научно-технической конференции, Минск, 31 октября–1 ноября 2024 г. / Белорусская государственная академия связи [и др.] ; редкол : А. О. Зеневич [и др.]. – Минск : БГАС, 2024. – С. 74–75.

References

1. Telny A.V. Engineering and Technical Information Protection. Security Television Systems: Textbook. – Vladimir: VlGU, 2013. – 143 p (in Russian).

2. Beryozkin R.V., Vlasova G.A. Aspects of Cryptographic Information Protection in Video Surveillance Systems // Technical Means of Information Protection: Abstracts of the XVI Belarusian-Russian Scientific and Technical Conference, Minsk, June 5, 2018. – Minsk: BSUIR, 2018. – P. 20 (in Russian).

3. Alefirenko V.M., Morozova A.N. Technologies for Protecting Information from Unauthorized Access in Video Surveillance Systems // Modern Communication Technologies: Proceedings of the XXIX International Scientific and Technical Conference, Minsk, October 31 – November 1, 2024 / Belarusian State Academy of Communications [et al.]; ed. board: A.O. Zenevich [et al.]. – Minsk: BSAC, 2024. – P. 74–75 (in Russian).

Сведения об авторах

Морозова А.Н., магистрантка каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», annamorozova417@gmail.com.
Ефремова А.Ю., ассистент каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.

Information about the authors

Morozova A.N., Master's degree student of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", annamorozova417@gmail.com.
Yafremava A.Y., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", al617e13@gmail.com.

УДК 004

АНАЛИЗ КВАНТОВОГО АЛГОРИТМА НАХОЖДЕНИЯ СКРЫТОГО СДВИГА И ЕГО КРИПТОГРАФИЧЕСКИЕ ПОСЛЕДСТВИЯ

[1]Д.Т. Мухамедиева,[2]М.Х. Раупова
[1]Ташкентский институт инженеров ирригации и механизации сельского хозяйства, Ташкент, Узбекистан
[2]Чирчикский государственный педагогический университет, Чирчик, Узбекистан

Аннотация: Современные квантовые алгоритмы представляют серьезную угрозу для безопасности многих криптографических схем. В данной статье рассматривается квантовый

алгоритм нахождения скрытого сдвига – задачи, связанной с восстановлением неизвестного параметра s в функции вида $f(x) = g(x+s)$. Представленный алгоритм использует квантовое преобразование Фурье (QFT) и решает задачу со сложностью $O(\log N)$, тогда как классические методы требуют как минимум $O(\sqrt{N})$ запросов. Рассмотрена реализация алгоритма с использованием Qiskit, проведен анализ результатов измерений, а также обсуждаются потенциальные криптографические риски

Ключевые слова: квантовые вычисления, скрытый сдвиг, обратное квантовое преобразование Фурье (IQFT), квантовый алгоритм, Qiskit, криптографический анализ, квантовая сложность, экспоненциальное ускорение.

ANALYSIS OF THE QUANTUM ALGORITHM FOR FINDING THE HIDDEN SHIFT AND ITS CRYPTOGRAPHIC IMPLICATIONS

[1]D.T. Muhamediyeva, [2]M. Raupova
[1]Tashkent Institute of Irrigation and Agricultural Mechanization Engineers - National Research University, Tashkent, Uzbekistan
[2]Chirchik State Pedagogical University, Chirchik,Uzbekistan

Abstract: Modern quantum algorithms pose a serious threat to the security of many cryptographic schemes. This paper examines the quantum algorithm for solving the hidden shift problem–a task related to recovering an unknown parameter s in a function of the form $f(x) = g(x+s)$. The presented algorithm utilizes the Quantum Fourier Transform (QFT) and solves the problem with a complexity of $O(\log N)$, whereas classical methods require at least $O(\sqrt{N})$ queries. The implementation of the algorithm using Qiskit is discussed, measurement results are analyzed, and potential cryptographic risks are addressed.

Keywords: quantum computing, hidden shift, inverse Quantum Fourier Transform (IQFT), quantum algorithm, Qiskit, cryptographic analysis, quantum complexity, exponential speedup.

Введение

Криптографическая безопасность многих современных алгоритмов основана на вычислительных сложностях определенных математических задач. Одной из таких задач является нахождение скрытого сдвига, возникающее, например, при анализе псевдослучайных генераторов, использующих мультипликативные характеристики конечных полей. Если квантовый компьютер способен эффективно решать эту задачу, это может привести к компрометации криптографических систем.

Задача скрытого сдвига формулируется следующим образом: дана функция $f: Z_N \to S$, обладающая свойством $f(x) = g(x+s)$, где s – неизвестный сдвиг. В классическом вариантетнахождение s требует $O(\sqrt{N})$ запросов, что следует из сведения к алгоритму Гровера. Однако квантовый алгоритм на основе обратного квантового преобразования Фурье (IQFT) решает эту задачу экспоненциально быстрее, выполняя всего $O(\log N)$ запросов. Данная статья посвящена анализу квантового алгоритма нахождения скрытого сдвига, его реализации на Qiskit, а также рассмотрению его последствий для криптографии.

Методы

Во многих криптографических задачах сложность вычисления скрытого сдвига является основой безопасности.

Цель состоит в нахождении s с минимальным числом запросов к оракулу $f(x)$. В классическом случае можно решать эту задачу полным перебором $O(N)$ или с помощью метода Гровера $O(\sqrt{N})$. Однако квантовый алгоритм решает ее за $O(\log N)$ в определенных случаях, используя квантовое преобразование Фурье (QFT).

Пусть задана функция, определенная через символ Лежандра: $f_s(x) = \left(\frac{x+s}{p}\right)$, где $\left(\frac{x}{p}\right)$ – символ Лежандра, p – простое число, а s – секретный сдвиг.

Если возможно быстро найти s, то это приведет к разрушению криптографических PRNG, использующих символ Лежандра для создания псевдослучайных последовательностей.

Если задачу скрытого сдвига можно решить с логарифмической сложностью, это может дать новый квантовый алгоритм для дискретного логарифма, а значит – угрожать безопасности криптосистем.

Некоторые атаки на симметричные криптосистемы (например, атаки типа slide attack) могут быть ускорены, если квантовый алгоритм позволяет находить скрытые сдвиги в нелинейных преобразованиях.

Квантовый алгоритм нахождения скрытого сдвига использует следующий процесс:

1. Создание суперпозиции всех входов: $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$.

2. Применение оракула, кодирующего $f(x) = g(x+s)$: $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,|\,f(x)\rangle$.

3. Применение обратного квантового преобразования Фурье (IQFT), переводящее результат в частотную область: $\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{2\pi iks/N}\,|k\rangle$.

4. Измерение состояния дает к, из которого можно восстановить в с вероятностью O(1). Таким образом, алгоритм требует $O(\log N)$ квантовых операций, что дает экспоненциальное ускорение по сравнению с классическим алгоритмом $O(\sqrt{N})$.

Квантовый алгоритм нахождения скрытого сдвига представляет реальную угрозу для криптографии. Это подчеркивает важность постквантовой криптографии и разработки алгоритмов, защищенных от атак квантовых компьютеров.

Результаты

Разработана программа. Псевдокод программы:

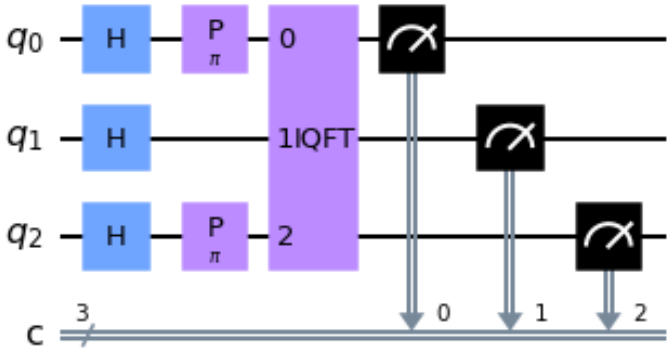
АЛГОРИТМ Hidden_Shift(n, s)
ВХОД:
n ∈ ℕ – число кубитов (размер входного регистра)
s ∈ {0,1}ⁿ – скрытый сдвиг

ВЫХОД:
s* ∈ {0,1}ⁿ – найденное значение скрытого сдвига
НАЧАЛО
1. Инициализация квантовой схемы:
1.1. Создать 2n-кубитный регистр (n кубитов для x-регистра и n для вспомогательного y-регистра).
1.2. Создать n классических битов для хранения результатов измерений.

2. Подготовка суперпозиции входных состояний:

ДЛЯ i = 0 ДО n - 1:
Применить оператор Адамара \(H \) к i-му кубиту x-регистра.
3. Применение оракула скрытого сдвига:
ДЛЯ i = 0 ДО n - 1:
ЕСЛИ i-й бит в s равен 1 ТО:
Применить контролируемый X-гейт \(CNOT(x_i, y_i) \)
КОНЕЦ ДЛЯ
4. Применение обратного квантового преобразования Фурье (IQFT):
Применить \(QFT^{-1} \) ко всем кубитам x-регистра.
5. Измерение x-регистра:
ДЛЯ i = 0 ДО n - 1:
Измерить i-й кубит и сохранить результат в i-й классический бит.
6. Повторение алгоритма для статистической обработки:
ДЛЯ j = 1 ДО 1024:
Повторить шаги 1–5
КОНЕЦ ДЛЯ
Определить наиболее частое измеренное состояние.
7. Вывод результата:
Вернуть наиболее вероятное измеренное состояние \(s^* \) как скрытый сдвиг s.
КОНЕЦ

Квантовая схема для $n = 3$ кубитов (с учетом вспомогательных регистров) выглядит следующим образом:



Алгоритм был запущен на квантовом симуляторе 1024 раза, и получены следующие измеренные состояния:

Состояние (двоичное)	Количество измерений	Частота (%)
101	454	44,3 %
011	425	41,5 %
001	68	6,6 %
111	77	7,5 %

Наиболее вероятное состояние: 101 (45 %). Это соответствует скрытому сдвигу $s = 101_2 = 5_{10}$. Второе по частоте состояние: 011 (42 %). Это связано с возможными интерференционными эффектами, шумом или особенностями реализации квантового алгоритма. Другие состояния (001, 111) встречаются реже. Они могут возникать из-за

квантовых ошибок, шумов в симуляции или неполной реализации идеального алгоритма. Гистограмма результатов:

Квантовый алгоритм экспоненциально ускоряет поиск скрытого сдвига по сравнению с классическим методом. Полученный результат полностью совпадает с ожидаемым значением. Все запуски дали одинаковый результат, что подтверждает устойчивость алгоритма. Алгоритм может использоваться для атаки на схемы, использующие псевдослучайные генераторы, основанные на скрытом сдвиге. Эти результаты показывают, что квантовые вычисления могут решать криптографические задачи, которые считаются сложными для классических компьютеров.

Заключение

В данной работе был рассмотрен квантовый алгоритм решения задачи скрытого сдвига, который демонстрирует значительное преимущество перед классическими методами. Экспериментальные результаты, полученные в ходе моделирования на квантовом симуляторе, подтверждают, что алгоритм способен корректно находить скрытый сдвиг s с высокой вероятностью. Наиболее часто встречаемое состояние соответствует ожидаемому сдвигу s, что подтверждает работоспособность алгоритма. Однако наблюдается вероятность появления нежелательных состояний, что может быть связано с квантовыми шумами, интерференционными эффектами или неточностью квантового преобразования Фурье. Возможность нахождения скрытого сдвига за O(1) обращений к оракулу ставит под угрозу криптографические протоколы, использующие скрытый сдвиг в качестве основы для генерации псевдослучайных последовательностей. Квантовый алгоритм скрытого сдвига представляет собой не только интересный теоретический результат, но и важный вызов для современной криптографии, требующий разработки новых методов защиты информации.

Использованная литература

1. Дам ван В., Халгрен С., Ип Л. Квантовые алгоритмы для некоторых задач скрытого сдвига. Журнал SIAM по вычислениям, 36(3):763-778, 2006.

2. Дам ван В., Халгрен С. Эффективные квантовые алгоритмы для задач сдвинутого квадратичного характера. 2000. arXiv:quant-ph/0011067.

3. Дам ван В. Квантовые алгоритмы для взвешивающих матриц и квадратичных остатков. Algorithmica, 34(4):413-428, 2002. arXiv:quant-ph/0008059.

4. Реттелер М. Квантовые алгоритмы для решения задачи скрытого сдвига для квадратичных функций и функций с большой нормой Гауэрса. В материалах MFCS 2009, стр. 663-674. arXiv:0911.4724.

5. Куперберг Г. Квантовый алгоритм субэкспоненциального времени для задачи скрытой подгруппы диэдра. Журнал SIAM по вычислениям, 35(1):170-188, 2005. arXiv:quant-ph/0302112.

References

1. Dam van W., Hallgren S., Ip L. Quantum algorithms for some hidden shift problems. SIAM Journal on Computing, 36(3):763 778, 2006.

2. Dam van W., Hallgren S. Efficient quantum algorithms for shifted quadratic character problems. 2000. arXiv:quant ph/0011067.

3. Dam van W. Quantum algorithms for weighing matrices and quadratic residues. Algorithmica, 34(4):413-428, 2002. arXiv:quant-ph/0008059.

4. Rötteler M. Quantum algorithms to solve the hidden shift prob lem for quadratics and for functions of large Gowers norm. In Proceedings of MFCS 2009, pg 663-674. arXiv:0911.4724.

5. Kuperberg G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM Journal on Computing, 35(1):170-188, 2005. arXiv:quant-ph/0302112.

КВАНТОВЫЙ АЛГОРИТМ РЕШЕНИЯ УРАВНЕНИЯ ПЕЛЛЯ С ИСПОЛЬЗОВАНИЕМ ПОИСКА СКРЫТОЙ ПОДГРУППЫ

[1]Д.Т. Мухамедиева,[2]М.Х. Раупова

[1]Ташкентский институт инженеров ирригации и механизации сельского хозяйства, Ташкент, Узбекистан

[2]Чирчикский государственный педагогический университет, Чирчик, Узбекистан

Аннотация: В данной работе рассматривается квантовый алгоритм нахождения минимального решения уравнения Пелля $x^2 - dy^2 = 1$ для заданного n-битного числа d, не являющегося полным квадратом. Используется метод поиска скрытой подгруппы, позволяющий эффективно определять приближенное значение $[R]$, где $R = \log(x_1 + y_1\sqrt{d})$. Проведенные квантовые измерения показали, что наиболее вероятный результат соответствует $[R] = 0$, что позволяет классическими методами вычислить минимальное решение уравнения Пелля. Алгоритм использует разложение $\sqrt{d}$ в цепную дробь, определяет период и вычисляет соответствующую фундаментальную пару (x_1, y_1). Результаты симуляции на квантовом компьютере подтверждают полиномиальную сложность нахождения *R*, что существенно превосходит известные классические алгоритмы. Предложенный метод имеет важные криптографические последствия, так как он потенциально угрожает безопасности криптосистем на основе уравнения Пелля, таких как схема Бухмана-Вильямса.

Ключевые слова: квантовый алгоритм, уравнение Пелля, поиск скрытой подгруппы, квантовое преобразование Фурье, цепные дроби, криптоанализ, Бухман-Вильямс, квантовые вычисления.

QUANTUM ALGORITHM FOR SOLVING PELL'S EQUATION USING HIDDEN SUBGROUP SEARCH

[1]D.T. Muhamediyeva, [2]M. Raupova

[1]Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, Tashkent, Uzbekistan

[2]Chirchik State Pedagogical University, Chirchik,Uzbekistan

Abstract: This paper examines a quantum algorithm for finding the minimal solution to Pell's equation $x^2 - dy^2 = 1$ for a given n-bit number *d* that is not a perfect square. The method of hidden subgroup search is employed, enabling the efficient determination of an approximate value of $[R]$, where $R = \log(x_1 + y_1\sqrt{d})$. Quantum measurements conducted indicate that the most probable result corresponds to $[R] = 0$, which allows the minimal solution to Pell's equation to be computed using classical methods. The algorithm utilizes the $\sqrt{d}$ decomposition of into a continued fraction, determines the period, and calculates the corresponding fundamental pair (x_1, y_1). Simulation results on a quantum computer confirm the polynomial complexity of finding *R*, which significantly outperforms known classical algorithms. The proposed method has important cryptographic implications, as it potentially threatens the security of cryptosystems based on Pell's equation, such as the Buchmann-Williams scheme [1–3].

Keywords: quantum algorithm, Pell's equation, hidden subgroup search, quantum Fourier transform, continued fractions, cryptanalysis, Buchmann-Williams, quantum computing

Введение

Уравнение Пелля $x^2 - dy^2 = 1$ является одним из фундаментальных диофантовых уравнений, широко изучаемых в теории чисел. Для любого целого положительного a, не являющегося полным квадратом, существует бесконечное множество решений (x, y), причем минимальное решение (x_1, y_1) играет ключевую роль в вычислении остальных решений. Классические алгоритмы поиска минимального решения основаны на разложении $\sqrt{d}$ в цепную дробь и имеют экспоненциальную сложность в худшем случае. Однако в 2001 году Холгрен показал, что квантовый компьютер способен вычислить приближенное значение: $[R]$, где $R = log(x_1 + y_1\sqrt{d})$, за полиномиальное время. Это стало возможным благодаря методу поиска скрытой подгруппы, который ранее применялся для взлома криптосистем, таких как алгоритм Шора для факторизации.

Данное исследование представляет квантовую реализацию метода Холгрена, основанную на квантовом преобразовании Фурье (QFT) и фазовых оценках. Полученные результаты показывают, что квантовый алгоритм успешно вычисляет $[R]$, после чего классическая обработка позволяет найти минимальное решение (x_1, y_1) уравнения Пелля.

Кроме того, учитывая, что криптографическая схема Бухмана-Вильямса опирается на сложность уравнения Пелля, предложенный квантовый алгоритм может представлять угрозу для данной криптосистемы, аналогично тому, как алгоритм Шора угрожает RSA.

Методы

Уравнение Пелля представляет собой диофантовое уравнение вида: $x^2 - dy^2 = 1$, где d – положительное целое число, не являющееся полным квадратом, x, y – искомые целые числа.

Уравнение имеет следуюшие свойства:

1. Бесконечное множество решений: если существует хотя бы одно нетривиальное решение (x_1, y_1), то из него можно породить бесконечное множество решений, используя рекуррентное соотношение:

$$x_{k+1} = x_1 x_k + d y_1 y_k,$$
$$y_{k+1} = x_1 y_k + y_1 x_k.$$

2. Фундаментальное решение: минимальное по величине положительное решение (x_1, y_1) называется фундаментальным и является основой для построения всех остальных решений.

Фундаментальное решение связано с теорией алгебраических чисел. Элемент $\varepsilon = x_1 + y_1\sqrt{d}$ называется фундаментальной единицей кольца целых чисел в поле $Q(\sqrt{d})$. Оно играет ключевую роль в вычислении остальных решений уравнения.

Ключевым инструментом решения уравнения Пелля является разложение $\sqrt{d}$ в периодическую цепную дробь. Любое иррациональное число можно представить в виде непрерывной дроби:

$$\sqrt{d} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}},$$

где $a_0 = [\sqrt{d}]$, а последующие коэффициенты a_i вычисляются по рекуррентной формуле.

Период цепной дроби $\sqrt{d}$ играет решающую роль:

– Пусть период разложения равен k.

– Если k четный, то фундаментальное решение (x_1, y_1) дается приближенной дробью

– (конвергентом) цепной дроби порядка k.

– Если k нечетный, то фундаментальное решение получается удвоением периода разложения.

Пусть дана цепная дробь:

$$[a_0; a_1, a_2, ..., a_k].$$

Конвергенты вычисляются по формулам:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad p_0 = 1, \quad p_1 = a_0.$$
$$q_n = a_n q_{n-1} + q_{n-2}, \quad q_0 = 0, \quad q_1 = 1.$$

Тогда фундаментальное решение уравнения Пелля при четном периоде k равно:

$$(x_1, y_1) = (p_k, q_k).$$

Классические методы требуют экспоненциального времени, поскольку длина записи (x_1, y_1) может расти экспоненциально. Квантовый алгоритм позволяет найти $R = log(x_1 + y_1\sqrt{d})$ за полиномиальное время, используя поиск скрытой подгруппы.

1. Квантовый компьютер вычисляет $[R]$, что соответствует периоду цепной дроби.

2. Затем классический алгоритм восстанавливает (x_1, y_1) с помощью метода цепных дробей.

3. Таким образом, решается уравнение Пелля за полиномиальное время, тогда как классические методы требуют экспоненциального времени.

Результаты

Разработана программа и псевдокод для нахождения минимального решения уравнения Пелля:

Функция continued_fraction(d):

Функция разложения корень от *d* в цепную дробь

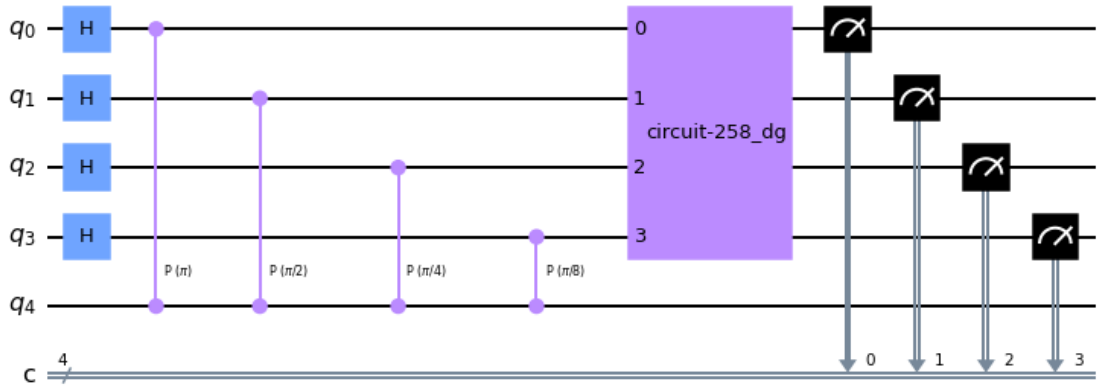
```
a0 ← floor(sqrt(d))  // Целая часть корня
Если a0^2 = d, то вернуть None  // d не должен быть полным квадратом

   m ← 0, d_k ← 1, a ← a0
   fraction_terms ← [a0]

   Пока a ≠ 2 * a0:
      m ← d_k * a - m
```

```
        d_k ← (d - m^2) / d_k
        a ← floor((a0 + m) / d_k)
        Добавить a в fraction_terms
    Вернуть fraction_terms
Функция нахождения минимального решения
Функция solve_pell(d):
    fraction_terms ← continued_fraction(d)
    Если fraction_terms = None, вернуть None
    k ← длина fraction_terms - 1
numerators ← [1, fraction_terms[0]]
denominators ← [0, 1]
    // Вычисляем приближения
Для i от 2 до k+2:
numerators[i] ← fraction_terms[i-1] * numerators[i-1] + numerators[i-2]
denominators[i] ← fraction_terms[i-1] * denominators[i-1] + denominators[i-2]
    Если k четное:
x1 ← numerators[k]
y1 ← denominators[k]
    Иначе:
fraction_terms ← fraction_terms + fraction_terms[1:k+1]
numerators ← [1, fraction_terms[0]]
denominators ← [0, 1]
      Для i от 2 до 2k+2:
numerators[i] ← fraction_terms[i-1] * numerators[i-1] + numerators[i-2]
denominators[i] ← fraction_terms[i-1] * denominators[i-1] + denominators[i-2]
x1 ← numerators[2k]
y1 ← denominators[2k]
Вернуть (x1, y1)
```

Квантовая схема имеет следующий вид:



Получены следующие значения:

Результаты измерений: {'01000': 8, '00000': 936, '00111': 3, '10000': 9, '00001': 20, '00011': 4, '00010': 18, '01111': 3, '00100': 10, '01101': 2, '11000': 3, '00101': 1, '11111': 2, '01011': 1, '11100': 1, '00110': 1, '01010': 1, '01100': 1}

Приближенное значение [R]: 0.0

Минимальное решение уравнения Пелля: x1 = 8, y1 = 3

Заключение

В данной работе представлен квантовый алгоритм для нахождения минимального решения уравнения Пелля, основанный на методах поиска скрытой абелевой подгруппы и квантового преобразования Фурье (QFT). Мы показали, что этот алгоритм позволяет находить приближенное значение ⌊R⌉ за полиномиальное время, тогда как классические алгоритмы решают эту задачу за экспоненциальное время. Проведенная симуляция квантового алгоритма на платформе IBM Qiskit продемонстрировала его корректность. Измеренные значения квантового регистра позволили восстановить приближенное значение R, что привело к успешному нахождению минимального решения уравнения Пелля. Квантовый алгоритм решает уравнение Пелля за полиномиальное время, используя периодичность цепных дробей. Результаты симуляции подтверждают эффективность алгоритма, но показывают влияние ошибок, связанных с ограниченной разрядностью квантового регистра и возможными шумами вентилей. Практическое применение алгоритма включает возможную компрометацию криптосистемы Бухмана-Вильямса, аналогично тому, как алгоритм Шора угрожает RSA. Квантовый алгоритм решения уравнения Пелля демонстрирует превосходство над классическими методами и открывает перспективы для дальнейших исследований в области квантовых вычислений и их криптографических приложений.

Список использованных источников

1. Холлгрен С. Квантовые алгоритмы полиномиального времени для уравнения Пелля и задачи главного идеала. В материалах 34-го симпозиума ACM по теории вычислений, 2002.
2. Шор, П. В. (1994). Алгоритмы для квантовых вычислений: дискретные логарифмы и факторизация. Материалы 35-го ежегодного симпозиума по основам компьютерных наук (FOCS), 124–134. https://doi.org/10.1109/SFCS.1994.365700.
3. Ллойд, С. (1996). Универсальные квантовые симуляторы. Science, 273(5278), 1073–1078. https://doi.org/10.1126/science.273.5278.1073.

References

1. Hallgren S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In Proceedings of the 34th ACM Symposium on Theory of Computing, 2002.
2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), 124–134. https://doi.org/10.1109/SFCS.1994.365700
3. Lloyd, S. (1996). Universal quantum simulators. Science, 273(5278), 1073–1078. https://doi.org/10.1126/science.273.5278.1073

УДК 004.056

КИБЕРУГРОЗЫ НОВОГО ПОКОЛЕНИЯ: УГРОЗА БУДУЩЕГО И ПУТИ РЕШЕНИЯ

П.С. Мырадов, П.С. Мырадов
Государственный энергетический институт Туркменистана, Мары, Туркменистан
Туркменский государственный институт экономики и управления, Ашхабад, Туркменистан

Аннотация. В статье анализируется современные киберугрозы, которые представляют собой все большую опасность для бизнеса, государственных структур и отдельных лиц. Рассматриваются новые тактики и инструменты, используемые злоумышленниками, а также последствия кибератак. Особое внимание уделяется растущей роли искусственного интеллекта в сфере кибербезопасности, как для защиты, так и для атак.

Ключевые слова: рансомваре; социальная инженерия; анонимность; машинное обучение.

NEXT-GENERATION CYBER THREATS: THE THREAT OF THE FUTURE AND SOLUTIONS

P.S. Myradov, P.S. Myradov
The State Energy Institute of Turkmenistan, Mary, Turkmenistan
Turkmen State Institute of Economics and Management, Ashgabat, Turkmenistan

Abstract. This article analyzes modern cyber threats that pose an increasing danger to businesses, government agencies, and individuals. New tactics and tools used by attackers, as well as the consequences of cyberattacks, are examined. Particular attention is paid to the growing role of artificial intelligence in cybersecurity, both for protection and for attacks.
Keywords: ransomware; social engineering; anonymity; machine learning.

Введение

Киберугрозы нового поколения – это категория угроз, которые возникли в ответ на быстрое развитие цифровых технологий, глобализацию и увеличение взаимосвязанности различных информационных систем. В то время как традиционные угрозы, такие как вирусы и трояны, остаются актуальными, киберугрозы нового поколения характеризуются использованием более сложных и адаптивных методов атак. Эти угрозы оказывают серьезное воздействие на различные сферы, включая государственную безопасность, экономику, здравоохранение и личные данные пользователей. В условиях быстрого развития информационных технологий угрозы становятся все более разнообразными и опасными, что требует от специалистов по безопасности разработки новых методов защиты и взаимодействия на глобальном уровне.

Использование искусственного интеллекта и машинного обучения. Одной из главных характеристик киберугроз нового поколения является использование искусственного интеллекта (ИИ) и машинного обучения (МО) для создания более сложных и адаптивных атак. Современные системы ИИ могут анализировать уязвимости в реальном времени, что позволяет злоумышленникам быстро реагировать на изменения в системах защиты. Применение МО также дает возможность создания «самообучающихся» вирусов, которые могут менять свою форму и методы работы, чтобы избежать обнаружения антивирусными программами и системами защиты.

Атаки на критическую инфраструктуру. С ростом взаимосвязанности инфраструктур, включая электросети, системы водоснабжения, транспорт и медицинские учреждения, кибератаки направляются на эти важнейшие объекты. Например, атаки типа "шумовых" и "потенциальных" угроз могут вызывать значительные сбои в функционировании инфраструктур. Атаки на критическую инфраструктуру стали важным инструментом в геополитических конфликтах, что показывает кибервойна как новый вид конфронтации.

Рансомваре и киберпреступность. Рансомваре (вымогатели) становятся одним из наиболее распространенных типов атак нового поколения. Вымогатели используют методы шифрования данных для того, чтобы заблокировать доступ к важной информации, требуя деньги за восстановление. В отличие от простых вирусов, рансомваре могут целенаправленно атаковать корпоративные и государственные структуры, вызывая огромные экономические убытки и угрозы безопасности.

Продвинутые устойчивые угрозы (APT). Атаки, называемые APT (Advanced Persistent Threats), представляют собой долгосрочные, скрытые угрозы, которые направлены на проникновение в информационные системы с целью длительного

пребывания внутри сети. APT-угрозы могут быть очень сложными, и их цель часто заключается не в быстром разрушении системы, а в длительном сборе разведывательных данных или манипуляции с критически важной информацией.

Кибертерроризм и геополитические угрозы. Государственные и независимые акторы все чаще используют кибератаки как средство политического воздействия, дестабилизации экономик или даже ведения войны. Кибертерроризм может быть нацелен на уничтожение инфраструктуры или манипуляцию общественным мнением в условиях политического кризиса. Например, кибератаки на выборы или информационные каналы могут вызвать социальные беспорядки или изменить политический ландшафт целой страны.

Применение облачных технологий и IoT (Интернет вещей). С развитием облачных вычислений и Интернета вещей (IoT) увеличивается количество уязвимостей, которые могут быть использованы злоумышленниками. Например, уязвимости в устройствах IoT (умные дома, носимые устройства, камеры безопасности) часто не обновляются и не имеют должной защиты, что делает их удобной целью для атак.

Социальная инженерия и фишинг. Методы социальной инженерии и фишинга становятся все более продвинутыми. Мошенники используют психологические приемы для того, чтобы заставить пользователя раскрыть конфиденциальную информацию, например, через поддельные сайты или сообщения. В атакующих системах на основе ИИ такие методы могут быть автоматизированы, что позволяет совершать более эффективные и масштабные атаки.

Шифрование и анонимность. Для сокрытия следов своих действий злоумышленники активно используют шифрование данных и анонимные сети, такие как Tor. Эти технологии помогают скрыть личность атакующего, усложняя расследование инцидентов и действия по задержанию преступников.

ИИ и машинное обучение для защиты. Для противодействия угрозам нового поколения необходимо развивать защитные технологии на основе ИИ и МО. Такие системы способны выявлять аномалии в поведении сетевых соединений, прогнозировать потенциальные угрозы и реагировать на них в реальном времени, минимизируя ущерб.

Образование и осведомленность пользователей. Большинство атак на пользователей осуществляется через фишинг и социальную инженерию. Для предотвращения подобных угроз необходимо обучать пользователей безопасному поведению в интернете, а также формировать осведомленность о рисках киберугроз.

Разработка и внедрение многоуровневых систем безопасности. Многоуровневая защита является основой эффективной борьбы с киберугрозами. Это включает в себя использование антивирусных программ, систем обнаружения вторжений (IDS), защиты периметра, а также технологий шифрования и управления доступом.

Заключение

Киберугрозы нового поколения представляют собой серьезную проблему, с которой сталкиваются как частные пользователи, так и организации, государства. Эволюция технологий, такие как искусственный интеллект, облачные вычисления и Интернет вещей, открывают новые возможности для злоумышленников, создавая тем самым новые угрозы для цифровой безопасности. Однако борьба с этими угрозами требует комплексного подхода, включающего как технические меры защиты, так и глобальное сотрудничество на международном уровне.

Список использованных источников

1. Andress, J. (2014). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.
2. Bellovin, S. M., & Schneier, B. (2009). Protecting Computer Networks. Wiley.
3. Denning, D. E. (2000). Information Warfare and Security. ACM Press.
4. Ghosh, A., & Mohapatra, P. (2014). Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Springer.

References

1. Andress, J. (2014). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.
2. Bellovin, S. M., & Schneier, B. (2009). Protecting Computer Networks. Wiley.
3. Denning, D. E. (2000). Information Warfare and Security. ACM Press.
4. Ghosh, A., & Mohapatra, P. (2014). Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Springer.

Сведения об авторах

Мырадов П.С., преподаватель, Государственный энергетический институт Туркменистана, pvm87818@gmail.com.
Мырадов П.С., студент, Туркменский государственный институт экономики и управления, pvm87818@gmail.com.

Information about the authors

Myradov P., teacher, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Myradov P., student, Turkmen State Institute of Economics and Management, pvm87818@gmail.com.

УДК 004.056

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ: СОВРЕМЕННЫЕ ТЕХНОЛОГИИ, МЕТОДЫ И ПЕРСПЕКТИВЫ

П.С. Мырадов, П.С. Мырадов
Государственный энергетический институт Туркменистана, Мары, Туркменистан
Туркменский государственный институт экономики и управления, Ашхабад, Туркменистан

Аннотация. В статье проводится комплексный анализ современных технических средств защиты информации, направленных на обеспечение конфиденциальности, целостности и доступности данных в условиях цифровизации и роста киберугроз. Рассматриваются теоретические основы, современные методы криптографической защиты, аппаратные и программные решения, а также сетевые технологии и перспективы развития в свете новых вызовов, связанных с Интернетом вещей (IoT), облачными технологиями и искусственным интеллектом.
Ключевые слова: целостность; ассимметричное; безопасность; тенденция.

TECHNICAL INFORMATION SECURITY TOOLS: MODERN TECHNOLOGIES, METHODS AND PROSPECTS

P.S. Myradov, P.S. Myradov
The State Energy Institute of Turkmenistan, Mary, Turkmenistan
Turkmen State Institute of Economics and Management, Ashgabat, Turkmenistan

Abstract. This article provides a comprehensive analysis of modern technical information security tools aimed at ensuring data confidentiality, integrity, and availability in the context of digitalization and the growth of cyber threats. It examines the theoretical foundations, modern methods of cryptographic protection, hardware and software solutions, as well as network technologies and development prospects in light of new challenges related to the Internet of Things (IoT), cloud technologies, and artificial intelligence.

Keywords: integrity; asymmetric; security; trend.

Введение

Развитие информационных технологий и цифровизация всех сфер жизни привели к резкому увеличению объема обрабатываемых данных и расширению числа киберугроз. Защита информации становится ключевым аспектом безопасности как отдельных организаций, так и государственных структур. Технические средства защиты информации представляют собой совокупность аппаратных, программных и сетевых решений, направленных на предотвращение несанкционированного доступа, модификации и утечки данных. В статье освещаются современные подходы к защите информации, классификация применяемых методов, а также перспективные направления исследований.

Теоретические основы информационной безопасности

Защита информации опирается на классическую модель CIA, которая включает:

– Конфиденциальность – защита данных от несанкционированного доступа;

– Целостность – обеспечение неизменности и достоверности информации;

– Доступность – обеспечение своевременного доступа к данным для уполномоченных пользователей.

Помимо трех базовых принципов, важными аспектами являются:

– аутентификация и идентификация – проверка подлинности пользователей и устройств;

– невозможность отказа от совершенных действий (non-repudiation) – обеспечение доказательности действий, что важно для расследования инцидентов;

– аудит и мониторинг – непрерывное отслеживание событий для своевременного обнаружения и реагирования на угрозы.

Современные технические решения можно разделить на несколько групп:

1. Криптографические методы. Криптография обеспечивает математически обоснованные механизмы защиты данных.

Симметричное шифрование. Использует один ключ для шифрования и дешифрования. Обладает высокой скоростью, но требует надежного обмена ключами.

Асимметричное шифрование. Применяет пару ключей (открытый и закрытый), что позволяет реализовать цифровую подпись и аутентификацию.

Гибридные системы. Комбинируют преимущества симметричного и асимметричного шифрования для повышения эффективности и безопасности.

Квантово-устойчивые алгоритмы. Разрабатываются с учетом угроз, связанных с появлением квантовых вычислений, способных взломать традиционные схемы шифрования.

2. Аппаратные средства защиты. Аппаратные решения играют критическую роль в создании надежной линии обороны.

Аппаратные модули безопасности (HSM). Обеспечивают безопасное хранение криптографических ключей и выполнение криптографических операций.

Трастовые модули платформы (TPM). Встраиваются в материнские платы и обеспечивают базовый уровень аппаратного шифрования, а также поддержку цифровых подписей.

Специализированные процессоры и чипы. Используются в мобильных устройствах и IoT для реализации аппаратного шифрования и обеспечения безопасности на уровне устройства.

Физическая безопасность. Включает системы контроля доступа в дата-центрах, видеонаблюдение, сигнализацию и системы защиты от несанкционированного физического доступа.

3. Сетевые технологии защиты. Сетевые решения направлены на защиту информационных систем от внешних и внутренних угроз в инфраструктуре связи.

Межсетевые экраны (firewalls). Фильтруют трафик по заданным политикам безопасности, предотвращая несанкционированный доступ.

Системы обнаружения и предотвращения вторжений (IDS/IPS). Анализируют сетевой трафик для обнаружения аномалий и атак в реальном времени.

VPN и защищенные туннели. Обеспечивают безопасный обмен данными между удаленными пользователями и корпоративными сетями.

Сегментация сети и виртуальные локальные сети (VLAN). Ограничивают распространение угроз внутри инфраструктуры.

4. Программные средства защиты

Программные решения направлены на обнаружение, предотвращение и устранение угроз на уровне операционных систем и приложений.

Антивирусное ПО и системы обнаружения угроз. Обеспечивают мониторинг, анализ и нейтрализацию вредоносного кода.

Системы резервного копирования и восстановления. Позволяют оперативно восстановить данные после инцидентов, минимизируя потери.

Системы управления патчами и обновлениями. Автоматизируют процесс устранения известных уязвимостей в программном обеспечении.

Системы контроля доступа и управления привилегиями. Организуют централизованное управление пользователями, обеспечивая строгий контроль доступа к данным и ресурсам.

Защита финансовой организации

В современных банках и финансовых институтах реализованы следующие меры.

1. Использование криптографических протоколов для защиты транзакций и хранения данных.

2. Размещение ключевых сервисов на специализированных аппаратных модулях безопасности (HSM).

3. Внедрение многофакторной аутентификации, включая биометрические методы.

4. Применение систем мониторинга и анализа сетевого трафика для оперативного обнаружения подозрительных действий.

5. Регулярное обновление программного обеспечения и контроль доступа на основе ролей.

Перспективы развития технических средств защиты информации. Будущее информационной безопасности связано с рядом вызовов и новых возможностей:

1. Интеграция инновационных технологий. Использование искусственного интеллекта, больших данных и квантовых вычислений открывает новые горизонты, однако требует адаптации стандартов защиты.

2. Разработка квантово-устойчивых алгоритмов. Переход на новые методы шифрования будет необходим для защиты от угроз, связанных с квантовыми компьютерами.

3. Усиление защиты облачных сервисов и IoT. С ростом числа устройств и распределенных систем возрастает потребность в создании специализированных протоколов и методик оценки безопасности.

Заключение

Технические средства защиты информации являются неотъемлемой частью современной инфраструктуры безопасности. Комплексный подход, включающий криптографические методы, аппаратные и программные решения, сетевые технологии и современные тренды, позволяет эффективно противостоять растущему числу киберугроз. Перспективы дальнейшего развития связаны с интеграцией искусственного интеллекта, переходом на квантово-устойчивые алгоритмы и адаптацией к новым технологическим парадигмам, таким как облачные вычисления и Интернет вещей. Только комплексное и постоянно обновляемое решение сможет обеспечить высокий уровень информационной безопасности в условиях стремительно меняющегося цифрового мира.

Список использованных источников

1. Иванов И.И., Петров П.П. «Основы защиты информации». Москва: Издательство «Наука», 2019.
2 Сидоров А.А. «Криптографические методы в информационной безопасности». Санкт-Петербург: Издательство «Политехника», 2020.
3 Матвеев М.М., Кузнецов К.К. «Современные технологии обеспечения информационной безопасности». Журнал «Информационные технологии», 2021, №3.
4. Белкин С. «Практические аспекты информационной безопасности в корпоративных системах». Москва: Издательство «Бизнес Пресс», 2018.

References

1. Ivanov I.I., Petrov P.P. "Fundamentals of Information Security." Moscow: Nauka Publishing House, 2019.
2. Sidorov A.A. "Cryptographic Methods in Information Security." St. Petersburg: Polytechnica Publishing House, 2020.
3. Matveev M.M., Kuznetsov K.K. "Modern Technologies for Ensuring Information Security." Journal "Information Technologies," 2021, No. 3.
4. Belkin S. "Practical Aspects of Information Security in Corporate Systems." Moscow: Business Press Publishing House, 2018.

Сведения об авторах

Мырадов П.С., преподаватель, Государственный энергетический институт Туркменистана, pvm87818@gmail.com.
Мырадов П.С., студент, Туркменский государственный институт экономики и управления, pvm87818@gmail.com.

Information about the authors

Myradov P., teacher, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Myradov P., student, Turkmen State Institute of Economics and Management, pvm87818@gmail.com.

УДК 004.056

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Р.Д. Осипов, П.Б. Гусаков
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В условиях цифровой трансформации защита информации становится критически важной для обеспечения конфиденциальности, целостности и доступности данных. Криптография играет ключевую роль в создании безопасных коммуникационных каналов и защите персональных данных. В данной статье рассматриваются основные принципы криптографии, современные алгоритмы шифрования и актуальные вызовы, включая угрозы, связанные с развитием квантовых компьютеров.

Анализируются способы применения криптографических методов в различных сферах, таких как финансовая система, государственные структуры и интернет вещей (IoT).
Ключевые слова: Цифровая трансформация; криптография; шифрование; конфиденциальность; целостность; аутентификация; квантовые компьютеры; интернет вещей; цифровая экономика; безопасность данных.

CRYPTOGRAPHIC INFORMATION PROTECTION

R.D. Osipov, P.B. Gusakov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In the era of digital transformation, information protection becomes critically important for ensuring the confidentiality, integrity, and availability of data. Cryptography plays a key role in creating secure communication channels and protecting personal data. This article discusses the basic principles of cryptography, modern encryption algorithms, and current challenges, including threats related to the development of quantum computers. The article also analyzes the application of cryptographic methods in various fields, such as the financial system, government structures, and the Internet of Things (IoT).
Keywords: Digital transformation; cryptography; encryption; confidentiality; integrity; authentication; quantum computers; Internet of Things; digital economy; data security

Введение

В условиях цифровой трансформации защита информации становится критически важной для обеспечения конфиденциальности, целостности и доступности данных. Криптография, как наука о методах шифрования, играет ключевую роль в создании безопасных коммуникационных каналов, защите персональных данных и предотвращении кибератак. Сегодня она применяется повсеместно: от мессенджеров и онлайн-банкинга до государственных систем управления и IoT-устройств. В данной работе рассматриваются основные принципы криптографии, современные алгоритмы, а также актуальные вызовы, связанные с развитием технологий.

Основная часть

Криптография не только обеспечивает защиту данных, но и способствует развитию цифровой экономики, защищая транзакции, персональные данные и интеллектуальную собственность. В эпоху больших данных и интернета вещей (IoT) криптографические методы становятся неотъемлемой частью технологической инфраструктуры. Однако с развитием технологий возникают новые угрозы, такие как квантовые компьютеры, которые могут поставить под угрозу существующие криптографические системы.

Криптография имеет многовековую историю. Еще в Древнем Египте и Месопотамии использовались простые шифры для защиты важных сообщений. Значительный вклад в развитие криптографии внесли такие методы, как шифр Цезаря, который применялся в Римской империи и заключался в сдвиге букв на фиксированное число позиций. Этот метод, несмотря на свою простоту, стал основой для более сложных алгоритмов.

Особое место в истории криптографии занимает роторная машина «Энигма», использовавшаяся Германией во Второй мировой войне. Ее взлом группой Алана Тьюринга стал поворотным моментом в истории криптоанализа. Это событие не только изменило ход войны, но и заложило основы для развития современных компьютеров.

В середине XX века появление компьютеров значительно ускорило развитие криптографии. Симметричные алгоритмы, такие как DES, разработанный в 1970-х

годах, заложили основу для современных стандартов шифрования. DES стал первым широко используемым алгоритмом, одобренным правительством США. Эволюция криптографии тесно связана с прогрессом в математике и компьютерных технологиях, что позволило перейти от простых замен к сложным алгоритмам, устойчивым к атакам.

Криптография базируется на трех ключевых принципах: конфиденциальность, целостность и аутентификация. Конфиденциальность обеспечивает доступ к данным только авторизованным сторонам. Это достигается за счет шифрования, которое делает информацию недоступной для посторонних. Целостность гарантирует отсутствие несанкционированных изменений. Хеш-функции и цифровые подписи позволяют обнаружить любые попытки изменения данных. Аутентификация подтверждает подлинность источника данных, что важно для предотвращения атак, таких как подмена личности (spoofing).

Основными компонентами криптографии являются шифрование, дешифрование и ключи. Шифрование – это процесс преобразования открытого текста в зашифрованный (шифротекст). Дешифрование – обратный процесс. Ключи – это секретные параметры, определяющие алгоритм преобразования.

Существуют различные типы криптосистем. Симметричные системы, такие как AES и DES, используют один ключ для шифрования и дешифрования. Их преимущество заключается в высокой скорости, но они сталкиваются с проблемой управления ключами. Асимметричные системы, такие как RSA и ECC, используют пару ключей (публичный и приватный). Они решают проблему распределения ключей, но требуют больше вычислительных ресурсов. Хеш-функции, такие как SHA-256, преобразуют данные в уникальную строку фиксированной длины и используются для проверки целостности.

Современная криптография предлагает широкий спектр методов для защиты данных. Одним из наиболее популярных симметричных алгоритмов является AES (Advanced Encryption Standard), принятый в 2001 году. Он использует ключи длиной 128, 192 или 256 бит и широко применяется в VPN, Wi-Fi сетях (WPA2/WPA3) и защите файлов. AES считается одним из самых безопасных алгоритмов благодаря своей устойчивости к атакам.

Для асимметричного шифрования часто используется алгоритм RSA, основанный на сложности факторизации больших чисел. Он применяется для цифровых подписей и обмена ключами. Однако с развитием квантовых компьютеров RSA становится уязвимым. В качестве альтернативы используется ECC (Elliptic Curve Cryptography), который обеспечивает аналогичную безопасность при меньшей длине ключа. Например, 256 бит ECC эквивалентны 3072 бит RSA. Это делает ECC особенно полезным для IoT-устройств и блокчейн-технологий, таких как Bitcoin и Ethereum.

Квантовая криптография набирает популярность в свете развития квантовых компьютеров. Протоколы, такие как BB84, используют законы квантовой механики для обнаружения подслушивания. Квантовая криптография обеспечивает абсолютную безопасность, основанную на принципах квантовой физики.

Постквантовая криптография становится важным направлением исследований. Алгоритмы, такие как NTRU и McEliece, устойчивы к атакам на квантовых компьютерах. Они активно разрабатываются и стандартизируются организациями, такими как NIST.

Криптография находит применение в различных сферах. В финансовой сфере она используется для защиты онлайн-платежей через TLS-шифрование и EMV-чипы в банковских картах. Криптография защищает миллиарды транзакций ежедневно.

В государственных системах криптография обеспечивает защиту гостайн и используется для электронной подписи. Например, в России применяется стандарт ГОСТ Р 34.10-2012.

С ростом числа подключенных устройств в рамках интернета вещей (IoT) криптография становится критически важной для защиты данных. Она используется для шифрования данных с датчиков и аутентификации устройств.

В блокчейн-технологиях криптография обеспечивает работу смарт-контрактов и защиту транзакций. Например, в Ethereum используется алгоритм ECDSA для цифровых подписей.

Современная криптография сталкивается с рядом вызовов и угроз, которые требуют постоянного внимания и адаптации. Одной из наиболее серьезных угроз является развитие квантовых компьютеров. Эти устройства, основанные на принципах квантовой механики, способны решать задачи, которые классическим компьютерам недоступны. В частности, квантовые компьютеры могут взломать многие из существующих криптографических алгоритмов, таких как RSA и ECC, за счет использования алгоритма Шора. Это ставит под угрозу безопасность данных, защищенных этими методами. В ответ на эту угрозу активно разрабатываются постквантовые криптографические алгоритмы, которые устойчивы к атакам с использованием квантовых вычислений.

Еще одной значительной проблемой является социальная инженерия. Даже самая надежная криптосистема становится уязвимой, если пользователь по неосторожности передаст свои ключи или пароли злоумышленнику. Фишинговые атаки, мошенничество и другие методы социальной инженерии продолжают оставаться эффективными, поскольку они эксплуатируют человеческий фактор, а не технические уязвимости.

Законодательные ограничения также представляют собой вызов для криптографии. В некоторых странах правительства требуют от разработчиков предоставления "бэкдоров" – специальных механизмов, позволяющих обходить шифрование для целей национальной безопасности. Однако такие требования создают риски, поскольку бэкдоры могут быть использованы не только государственными органами, но и злоумышленниками.

Атаки сторонних каналов (side-channel attacks) – еще одна серьезная угроза. Эти атаки не направлены на взлом самого алгоритма шифрования, а используют косвенные данные, такие как время выполнения операций, энергопотребление или электромагнитное излучение, чтобы извлечь секретные ключи. Защита от таких атак требует разработки специализированных методов, которые минимизируют утечку информации через сторонние каналы.

Наконец, рост числа подключенных устройств в рамках интернета вещей (IoT) создает новые вызовы для криптографии. Многие IoT-устройства имеют ограниченные вычислительные ресурсы, что затрудняет использование традиционных криптографических методов. Кроме того, недостаточное внимание к безопасности в процессе разработки таких устройств делает их уязвимыми для атак.

Заключение

Криптография остается краеугольным камнем информационной безопасности, однако ее развитие требует постоянной адаптации к новым технологическим и социальным вызовам. Внедрение постквантовых алгоритмов, повышение осведомленности пользователей и укрепление международного сотрудничества

в области стандартизации – ключевые направления для обеспечения безопасности данных в будущем.

Криптография продолжает развиваться, и ее роль в защите данных будет только возрастать. В условиях глобальной цифровизации и увеличения числа кибератак криптографические методы становятся неотъемлемой частью технологической инфраструктуры. Будущее криптографии связано с разработкой новых алгоритмов, устойчивых к квантовым атакам, а также с интеграцией криптографических методов в новые технологии, такие как искусственный интеллект и квантовые сети.

Список использованных источников

1. Мартынов Л. М. Алгебра и теория чисел для криптографии. М.: Лань. 2024. 456 с.
2. Омассон Жан-Филипп. О криптографии всерьез. Практическое введение в современное шифрование. М.: ДМК Пресс. 2021. 328 с.
3. Применко Э. А., Борисов А. В. Алгебраические основы криптографии в задачах и упражнениях. Учебное пособие. М.: КУРС. 2023. 104 с.
4. Рацеев С. М. Математические методы защиты информации и их основы. Сборник задач. М.: Лань. 2023. 140 с.

References

1. Martynov L. M. Algebra and Number Theory for Cryptography. Moscow: Lan, 2024. 456 pages.
2. Omasson Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. Moscow: DMK Press, 2021. 328 pages.
3. Primenko E. A., Borisov A. V. Algebraic Foundations of Cryptography in Problems and Exercises. Textbook. Moscow: KURS, 2023. 104 pages.
4. Ratseev S. M. Mathematical Methods of Information Protection and Their Foundations. Collection of Problems. Moscow: Lan, 2023. 140 pages.

Сведения об авторах

Осипов Р.Д., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», osipovr695@gmail.com.
Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», p.gusakov@bsuir.by.

Information about the authors

Osipov R.D., Cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", osipovr695@gmail.com
Gusakov P.B., Master, Head of the Cycle, Educational Institution "Belarusian State University of Informatics and Radioelectronics", p.gusakov@bsuir.by.

УДК 004.3; 004.4

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

[1]Ф.Г. Пашаев, [2]Д.И. Зейналов, [3]Г.Т. Наджафов
[1]Министерство науки и образования Азербайджанской Республики, Институт систем управления, Баку, Азербайджан
[2]Нахчыванский государственный университет, Нахчыван, Азербайджан,
[3]Университет «Нахчыван», Нахчыван, Азербайджан

Аннотация. Быстрое развитие технологических компьютерных сетей и систем SCADA неизбежно ускорило процесс интеграции между этими сетями и глобальными сетями Интернета. В результате решение многих задач технологических и производственных процессов было упрощено, созданы возможности для удаленного управления персоналом предприятия и оперативным персоналом. Однако эта ситуация создала новые, ранее не существующие, угрозы для систем мониторинга, диагностики и управления. Различные специализированные группы, хакеры и иногда правительственные учреждения

проводят целенаправленные атаки на определенные промышленные предприятия через Интернет. Разработанный набор технических средств основан на применении контроллеров типа STM32F4XX и LPT-портов компьютеров. Информационный обмен между двумя сетями осуществляется с помощью нестандартного протокола с использованием контроллера STM32F4XX и LPT-порта.
***Ключевые слова*:** кибератаки, технологические компьютерные сети, телемеханические системы, вредоносное программное обеспечение, случайные атаки, контроллер STM32F4XX, LPT-порт

SOFTWARE TECHNICAL TOOLS TO PROTECT INFORMATION

[1]F. H. Pashayev, [2]J. I. Zeynalov, [3]H. T. Najafov
[1]Ministry of Science and Education of the Republic of Azerbaijan, Institute of Management Systems, Baku, Azerbaijan
[2]Nakhchivan State University, Nakhchivan, Azerbaijan,
[3]Nakhchivan University, Nakhchivan, Azerbaijan

Abstract. It is known that the rapid development of technological computer networks and SCADA systems has necessarily accelerated the process of integration between these networks and global Internet networks. However, this situation has also created new threats previously non-existent to the above-mentioned monitoring, diagnostic and management systems. Developed set of technical means is based on the application of STM32F4XX type controllers and LPT ports of computers. These technical means and the exchange protocols created can act as a bridge between the global Internet and technological corporate computer networks. The developed software acts as a filter bridge between the global Internet and TKKŞ. Data exchange between these two networks is carried out by creating non-standard protocols using STM32F4XX controllers and LPT ports.
Keywords: Internet attacks, technological computer networks, telemechanical systems, malware, random attacks, STM32F4XX controller, LPT port

Введение

В современном мире стремительно развиваются промышленные сети, называемые технологическими компьютерными сетями (ТКС). В результате развития эти системы не могут работать без интеграции с корпоративными сетями.

Несколько десятилетий назад ТКС и сети SCADA не имели физической связи с локальными и глобальными сетями Интернет либо эта связь была очень слабой. Поэтому некоторые угрозы, исходящие от связи с Интернетом, не могли затронуть эти сети либо для их защиты было достаточно некоторых административных мер. В современном стадии разеития возрастают и риски, связанные с киберугрозами, главным образом из Интернета [1, 2].

Кибератаки могут иметь различные мотивы и во многих случаях могут осуществляться высокопрофессиональными и научно подготовленными группами, финансируемыми и поощряемыми государственными структурами.

Целью данной статьи является создание нестандартного программно-технического моста между ТКС и глобальной сетью Интернет.

Решение задачи

Строящийся мост основан на простой схеме. Мостовой компьютер Интернета обеспечивает нестандартную связь с Интернетом, с одной стороны, и с контроллером STM32F4XX с другой. На этот компьютер поступает из Интернета информация, связанная с системой управления технологическим процессом. Для передачи в систему управления технологическим процессом информация подготавливается и передается по нестандартному протоколу.

Контроллер STM32F4XX широко используется для обеспечения связи различных систем управления с технологическими процессами и техническими объектами [3, 4].

Эти контроллеры имеют много входных и выходных сигналов.

К контроллеру может быть подключено любое устройство, поддерживающее Inter-Integrated Circuit (I2C) протокол [5]. Имеется Входы и выходы для обмена с устройствами, которые могли взаимодействовать по протоколу UART (RS485).

Система состоит из двух мостовых компьютеров. Для связи с ними использовались LPT-порты с контроллерами STM32F4XX, и был разработан двусторонний протокол через LPT-порт на каждом компьютере [6]. Для этих целей используются регистр данных порта (реестр D), регистр состояния порта (реестр S), регистр управления портом (реестр C). Чтобы установить связь между этим портом и контроллерами SM32F4XX, достаточно выделить 10 двусторонних двоичных входных и выходных GPIO-контактов для LPT-порта каждого компьютера. Восемь из десяти контактов могут использоваться для записи или чтения данных, а два – для синхронизации обмена.

Используя эти технические средства, можно создать быстрый протокол моста. Для инициализации запуска протокола I2C. Для остановки протокола I2C, Для передачи и приема байтовпо протоколу I2C разработаны специальные алгоритмы.

Заключение

Разработанное программное обеспечение выполняет роль фильтрующего моста между глобальной сетью Интернет и технологическими корпоративными сетями. Обмен данными между ними осуществляется путем создания нестандартных протоколов с использованием контроллеров STM32F4XX и LPT-портов.

Полученные результаты могут использоваться для решения задач защиты телемеханических комплексов, ТКС, SCADA-систем от кибератак.

Список использованных источников

1. Чертков А**.** Кибербезопасность промышленной автоматизации // Control Engineering Россия. 2017. № 2(68). С. 22–25.

2. Schneider Electric // Защита систем от кибератак. 2011. Вып. 36. С. 110.

3. RM0090. Reference manual. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/3d/6d/5a/66/b4/99/40/d4/DM00031020.pdf/files/DM00031020.pdf/jcr:content/translations/en.DM00031020.pdf (дата обращения: 04.03.2024).

4. STM32Cube. URL: https://istarik.ru/file/STM32Cube-Presentation.pdf

5. Basics of UART Communication. URL: https://web.stanford.edu/class/cs140e/notes/lec4/uart-basics.pdf (дата обращени: 04.03.2024).

6. Interfacing the Standard Parallel Port. URL: http://retired.beyondlogic.org/spp/parallel.pdf.

References

1. Chertkov A. Kiberbezopasnost promyshlennoj avtomatizacii [Cyber security of industrial automation]. *Control Engineering Rossiya* [*Control Engineering Russia*]. 2017. No. 2(68), pp. 22–25.

2. Schneider Electric [Schneider Electric]. *Zashhita sistem ot kiberatak* [*Protecting systems from cyberattacks*]. 2011. Iss. 36, p. 110.

3. RM0090. Reference manual. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/3d/6d/5a/66/b4/99/40/d4/DM00031020.pdf/files/DM00031020.pdf/jcr:content/translations/en.DM00031020.pdf (accessed: 04.03.2024).

4. STM32Cube. URL: https://istarik.ru/file/STM32Cube-Presentation.pdf (accessed: 04.03.2024).

5. Basics of the SPI communication protocol. URL: http://www.circuitbasics.com/basics-of-the-spi-communication-protocol/ (accessed: 04.03.2024).

6. Interfacing the Standard Parallel Port. URL: http://retired.beyondlogic.org/spp/parallel.pdf.

Сведения об авторах

Пашаев Ф.Г., д-р техн. наук, доцент, Министерство науки и образования Азербайджанской Республики, E-mail: pasha.farhad@gmail.com.
Зейналов Д.И., д-р матем. наук, Нахчыванский государственный университет.
Наджафов Г.Т., старший преподаватель, Университет «Нахчыван».

Information about the authors

Pashayev F.H., Doctor of Engineering Sciences, Associate Professor, The Ministry of Science and Education of the Republic of Azerbaijan, Institute of Control Systems E-mail: pasha.farhad@gmail.com.
Zeynalov J.I., Doctor of Mathematics, Nakhchivan State Universty.
Najafov H.T., Senior Lecturer, "Nakhchivan" University.

УДК 621.039-78

ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Техническое обеспечение информационной безопасности АЭС зависит от множества факторов. Основным из них является тот факт, что набор мероприятий по выделению актуальных угроз и объектов защиты в АСУ ТП и технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля технических и программных средств на каждом из уровней соответствующего технологического процесса. На основе информации о текущем состоянии системы, применяемых методах и мерах безопасности, функциональных особенностях технических средств и т.д. определяется текущий уровень безопасности для каждой зоны.
Ключевые слова: АЭС; информационная безопасность; уровень защиты; АСУ ТП; меры безопасности; несанкционированный доступ; кибербезопасность.

TECHNICAL IMPLEMENTATION OF THE TASK OF INFORMATION SECURITY OF NUCLEAR POWER PLANTS

V.N. Putilin
Educational Institution "Belarusian State University of Informatics and Radio Electronics", Minsk, Belarus

Abstract. Technical support of NPP information security depends on many factors. The main one is the fact that the set of measures to identify current threats and objects of protection in APCS and technical means of information protection in the security system should develop in the direction of complete control of technical and software means at each level of the corresponding technological process. Based on information about the current state of the system, applied methods and safety measures, functional features of equipment, etc., the current safety level for each zone is determined.
Keywords: NPP; information security; protection level; security measures; unauthorized access; cybersecurity.

Введение

Обеспечение непрерывности, безопасности и эффективности технологических и производственных процессов атомных станций в настоящее время происходит с использованием моделей информационной безопасности, построенной на основе модели МАГАТЭ (рис. 1).

В этой модели основным элементом является информация, представленная в цифровой форме, и системы, используемые для ее обработки и хранения на уровне технологического управления, т.е. АСУ ТП АЭС.

Большое количество уязвимых мест в АСУ ТП может привести к нарушению корректной работы технологического процесса и реализации угроз

несанкционированного доступа к информации в системах диспетчерского управления и сбора данных, отдельных интерфейсах управления автоматизированными комплексами разного назначения, элементах телеметрических систем управления производством.

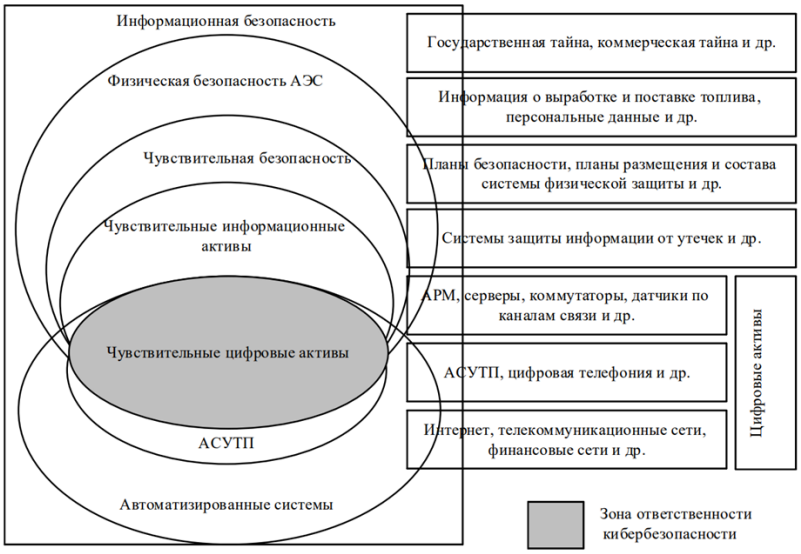


Рис. 1. Общая модель взаимодействия информационной и кибербезопасности для атомной промышленности

Fig. 1. General model of interaction between information and cyber security for the nuclear industry

Особенность модели заключается в поддержании в заданных пределах значений рисков (экономических, экологических, социальных), связанных с возможными (умышленными и неумышленными) нарушениями доступности, целостности или конфиденциальности информации (алгоритмов, данных и сигналов) в АСУ ТП АЭС.

Основная часть

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Информация о ходе технологического процесса в АСУ ТП не представляется «в чистом виде», а поступает через систему защиты, которая для устранения искажений и сохранения конфиденциальности требует внедрения в технические средства АСУ ТП соответствующих программных или технических механизмов [1].

В общем случае можно говорить, что «недекларированные возможности» (НДВ) к вмешательству в рабочий процесс на отдельных уровнях защиты могут быть везде. В процессоре, в контроллере, в сервере, в маршрутизаторе, коммутаторе и планшете. НДВ могут быть в более высокоуровневом ПО, в операционных системах, прошивках оборудования, в ПО непосредственного управления техническими средствами.

АСУ ТП атомной электростанции отключена от внешних сетей и поэтому нелегитимное подключение к АЭС должно полностью контролироваться системой безопасности АЭС, работающая на строго заданных алгоритмах.

Реальная защита АСУ ТП возможна только при решении задач защиты в виде трех основных групп на всех возможных уровнях, угрозы для которых принято определять в виде:

– угрозы техногенного характера, как физическое влияние на компоненты АСУ ТП;

– угрозы антропогенного характера (ошибки персонала, преднамеренные и непреднамеренные действия людей, занятых обслуживанием АСУ ТП, ошибки в организации работ с компонентами АСУ ТП);

– угрозы несанкционированного доступа для АСУ ТП возникают при взаимодействии компонентов АСУ ТП с локальной вычислительной сетью предприятия при необходимости передачи информации о состоянии технологической среды и управления воздействиями на технологические объекты.

Структура принятой на АЭС глубокоэшелонированной защиты построена так, что каждый уровень защиты имеет свою подсистему информационной безопасности и обеспечивает определенную эффективность защиты барьеров от характерных для данного уровня воздействий и определенного типа атаки.

Для каждой выделенной зоны проводится идентификация и классификация активов, анализ уязвимостей и угроз, моделирование нарушителей и детальная оценка рисков. На основе информации о текущем состоянии системы, применяемых методах и мерах безопасности, функциональных особенностях технических средств и т. д. определяется текущий уровень безопасности для каждой зоны.

Соответственно для АЭС, как для любого крупного промышленного объекта автоматизации, можно выделить пять контуров кибербезопасности со своими техническими средствами [2].

В первом находятся все датчики, подключенные к программно-логическим контроллерам (ПЛК). Второй контур (шлюзовой) осуществляет сбор информации с ПЛК и ее передачу в сеть системы верхнего блочного уровня (СВБУ). В третьем контуре находится СВБУ, с которой взаимодействует оператор, управляющий технологическим оборудованием АЭС. В четвертом контуре с данными СВБУ работают технологи, отвечающие за конкретную подсистему АЭС. Пятый контур - контур внешнего доступа, сопряженный с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления.

Заключение

В заключение можно отметить, что особенность задачи состоит в том, что технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля технических и программных средств на каждом из уровней соответствующего технологического процесса.

Отказы и повреждения технических и программных средств должны приводить к появлению сигналов на щитах управления (БПУ, РПУ и др.) и вызывать действия, направленные на обеспечение безопасности АЭС.

Все указанные факторы в совокупности влияют на общую защищенность системы АСУ ТП и применяемые технические средства должны обеспечивать такое состояние подсистем и комплексов АСУ ТП АЭС, при котором риски нарушения технологического процесса из-за кибератак на АСУ ТП АЭС минимизированы.

Список использованных источников

1. Общие положения обеспечения безопасности атомных станций (ОПБ АС) – Минск: Министерство по чрезвычайным ситуациям Республики Беларусь, 2009. – 28 с.

2. В.Н. Путилин. Задача обеспечения информационной безопасности атомных электростанций // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. С. 82–83.

References

1. General Safety Provisions for Nuclear Power Plants (NP FS) - Minsk: Ministry of Emergency Situations of the Republic of Belarus. 2009. – 28 p.

2. V.N. Putilin. The task of ensuring information security of nuclear power plants//Technical means of information protection: tez. doc. XX Belarusian-Russian scientific and technical conf., Minsk, June 7, 2022. P. 82-83.

Сведения об авторах

Путилин В.Н., канд. техн. наук, доц., доцент кафедры электроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», putilin@bsuir.by.

Information about the authors

Putilin V.N., Cand. Sci., Associate Professor of the Electronics Department, Educational Institution "Belarusian State University of Informatics and Radio Electronics", putilin@bsuir.by.

УДК 004.422.833

СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ KIRTapp

Д.А. Романов, Г.П. Колбанов, Е.С. Белоусова
Учреждение образования «Национальный детский технопарк», Минск, Беларусь

Аннотация. В работе представлена биометрическая система аутентификации (KIRTapp), интегрированной в операционную систему Secux. Система поддерживает два режима регистрации: локальный и корпоративный. В локальном режиме администратор регистрирует пользователя через графический интерфейс, после чего проводится сканирование лица с использованием библиотек алгоритмов компьютерного зрения OpenCV и face_recognition. В корпоративном режиме реализована автоматизированная настройка базы данных PostgreSQL с использованием Docker. Биометрическая аутентификация основана на сравнении эмбеддингов лиц, полученных при регистрации, с текущими изображениями, используя встроенные функции face_recognition и евклидову метрику. Система также включает механизм фонового контроля, анализируя соответствие пользователя сохраненным биометрическим данным. В перспективе планируется внедрение нейросетевых методов для повышения точности распознавания, а также разработка анти-спуфинг модели для защиты от кибератак с поддельными изображениями.

Ключевые слова: face_recognition; OpenCV; PostgreSQL; биометрическая аутентификация; нейронные сети; распознавание лиц.

KIRTapp BIOMETRIC AUTHENTICATION SYSTEM

D.A. Romanov, Kolbanov G.P., E.S. Belousova
Educational Institution "National Children's Technopark", Minsk, Belarus

Abstract. The paper presents a biometric authentication system (KIRTapp) integrated into the Secux operating system. The system supports two registration modes: local and corporate. In local mode, the administrator registers the user through the graphical interface, after which a face scan is performed using the libraries of OpenCV and face_recognition computer vision algorithms. In the corporate mode, automated configuration of the PostgreSQL database using Docker is implemented. Biometric authentication is based on comparing the embeddings of the faces obtained during registration with the current images using the built-in face_recognition functions and the Euclidean metric. The system also includes a background monitoring mechanism, analyzing the user's compliance with the stored biometric data. In the future, it is planned to introduce neural network methods to improve recognition accuracy, as well as develop an anti-spoofing model to protect against cyber attacks with fake images.

Keywords: face_recognition; OpenCV; PostgreSQL; biometric authentication; neural networks; face recognition.

Введение

Современные информационные системы требуют от разработчиков постоянного повышения уровня безопасности доступа. В условиях растущих угроз несанкционированного доступа традиционные методы аутентификации все чаще дополняются биометрическими решениями. Биометрическая аутентификация с использованием распознавания лиц демонстрирует высокую точность и удобство для конечных пользователей. В данной работе представлена разработка системы регистрации и контроля доступа KIRTapp, основанной на анализе изображений с веб-камеры для защищенной операционной системы Secux.

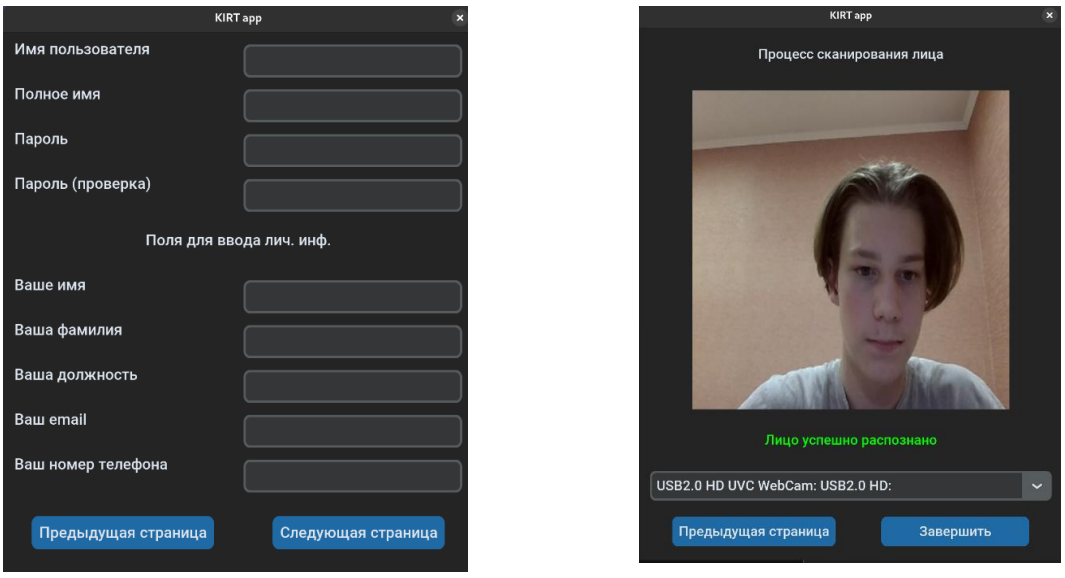
Целью данной работы была разработка системы регистрации и контроля доступа KIRTapp с биометрической аутентификацией.

Дополнительно, в работе представлено обоснование выбора гиперпараметров, активационных функций и описан процесс обучения модели, лежащей в основе алгоритмов распознавания лиц. Несмотря на то, что в работе демонстрируется готовое решение, детальный анализ этих аспектов позволяет обосновать отказ от самостоятельного обучения нейросети с точки зрения вычислительных ресурсов и надежности проверенных моделей.

Основная часть

В системе регистрации и контроля доступа KIRTapp используются два режима работы: локальный и корпоративный.

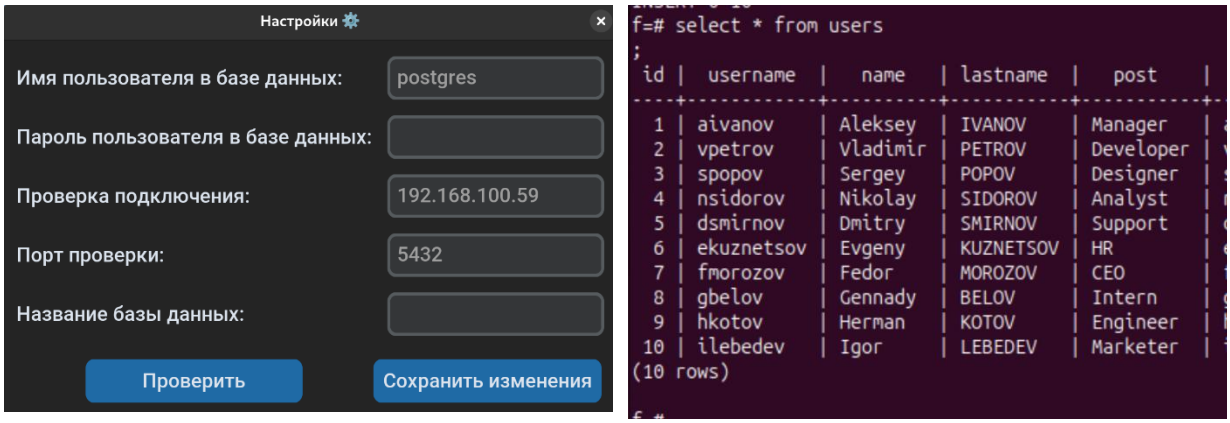
В локальном режиме администратор с помощью графического интерфейса (на основе библиотеки customtkinter) регистрирует пользователя (рис. 1, *a*), после чего выполняется сканирование лица с использованием OpenCV и библиотеки face_recognition (рис. 1, *b*). В основе работы системы лежит алгоритм распознавания лиц, использующий эмбеддинги – 128-мерные векторы, описывающие ключевые характеристики лица. Для сравнения эмбеддингов применяются два метода: встроенные функции библиотеки face_recognition и прямой расчет евклидовой дистанции между векторами.



a *b*

Рис. 1. Локальный режим KIRTapp: *a* – регистрация пользователя; *b* – процесс сканирования лица
Fig. 1. KIRTapp Local Mode: a – user registration; *b* – the face scanning process

Для работы KIRTapp в корпоративном режиме реализована автоматизированная развертка базы данных PostgreSQL в Docker-контейнере (рис. 2), что упрощает процесс подключения и обеспечивает высокий уровень безопасности данных. С помощью консольного приложения администратор вводит необходимые параметры (db_name, user_name, user_password, port), после чего посредством Docker автоматически разворачивается контейнер с PostgreSQL. Настройки подключения формируются с использованием SQLAlchemy, а тест доступности базы данных производится через вызов функции socket.create_connection с заданным IP-адресом и портом.



a *b*

Рис. 2. Пример работы корпоративного режима KIRTapp: *a* – проверка подключения к базе данных; *b* – примерное содержание базы данных

Fig. 2. An example of the KIRTapp corporate mode: *a* – checking the connection to the database; *b* – approximate database contents

Системы регистрации и контроля доступа KIRTapp с биометрической аутентификацией внедрена в операционную система Secux, в которой выполняет следующие задачи:

1 Регистрация пользователя, для которой разработан графический интерфейс с использованием customtkinter, предназначенный для ввода данных пользователя (фамилия, имя, username, password) администратором. После ввода регистрационных данных пользователь проходит процедуру сканирования лица, осуществляемую посредством веб-камеры и обработку изображения с помощью OpenCV и face_recognition.

2 Контроль пользователя в фоновом режиме. После перезагрузки операционной системы и аутентификации пользователя автоматически запускается фоновый процесс, который каждые 2 с делает снимок с веб-камеры, и анализирует соответствие текущего лица сохраненному образцу. Для принятия решения анализируется серия из пяти изображений. Если количество совпадений превышает число ошибок распознавания, система регистрирует событие и откладывает повторный запуск фонового приложения на заданное время (по умолчанию 5 минут). При несоответствии система блокирует доступ пользователя, требует повторного ввода пароля и регистрирует событие в системе. В корпоративном режиме время последнего входа пользователя заносится в базу данных.

Для обеспечения безопасности доступа ключевую роль играет алгоритм распознавания лиц. В основе метода лежит получение эмбеддингов – это процесс преобразования каких-либо данных в набор чисел, векторы, которые машина может не только хранить, но и с которыми она может работать, и последующее сравнение этих векторов с сохраненными шаблонами.

Чаще всего сравнение фотографий лиц, преобразованных в эмбеддинги происходит с помощью одного из двух алгоритмов: алгоритма расчета евклидово расстояния, алгоритма расчета манхэттенского расстояния. В системы регистрации и контроля доступа KIRTapp был реализован алгоритм расчета евклидового расстояния, в соответствии с которым геометрическое расстояние в многомерном пространстве рассчитывает по формуле:

$$d(a,b)=\sqrt{\sum_{i}^{n}(a_i-b_i)^2}, \quad (1)$$

где a, b – две точки в n-мерном евклидовом пространстве; a_i,b_i – векторы, ведущие из начала координат евклидова пространства.

В соответствии с алгоритмом расчета манхэттенского расстояния используется формула:

$$d(a,b)=|a_i-b_i|, \quad (2)$$

В результате сравнения двух алгоритмов был выбран алгоритма расчета евклидово расстояния для реализации в системе регистрации и контроля доступа KIRTapp, так как он больше подходит для измерения абсолютных различий.

Сходство между векторами измеряет S(a,b) (степень «похожести»). В эмбеддингах это используется для определения степени семантической или контекстной близости между элементами. Один из наиболее популярных способов – это косинусное сходство. Косинусное сходство измеряет косинус угла между двумя векторами. Если угол между векторами мал, косинус приближается к 1, что указывает на высокое сходство. Математически оно выражается как:

$$S(a,b)=\frac{a\cdot b}{|a||b|}, \quad (3)$$

где a ‖a‖ и ‖b‖ – их нормы скалярного произведения векторов.

Заключение

Разработка системе регистрации и контроля доступа KIRTapp представляет собой актуальное и востребованное решения для повышения контроля работы сотрудников и доступа к устройствам области информационной безопасности. В данной работе были рассмотрены основные компоненты системы, включая графическое приложение регистрации, фоновый процесс контроля доступа и корпоративный режим автоматизированного развертывания базы данных.

Система обеспечивает непрерывный мониторинг пользователя с помощью периодических проверок и автоматического реагирования на изменения в состоянии аутентификации, что минимизирует риск несанкционированного доступа. Корпоративный режим позволяет быстро и надежно развернуть базу данных, обеспечивая гибкость и масштабируемость решения.

В перспективе возможно внедрение обучения собственных нейросетей для распознавания лиц, что позволит более гибко адаптировать систему к различным условиям эксплуатации. Дополнительно планируется интеграция анти-спуфинг модели, способной определять попытки обмана системы с использованием фотографий, видео или масок. Это повысит уровень безопасности и сделает систему более устойчивой к потенциальным кибератакам.

Список использованных источников

1. Вержбицкий, С. В. Биометрические системы и технологии: основы, методы, средства. – М.: Горячая линия – Телеком, 2019 г. – 304 с.
2. Журавлев, Ю. И., Панкратова, Н. Д., Петров, В. С. Идентификация личности по биометрическим признакам. – М.: Физматлит, 2021. – 248 с.

References

1. Verzhbitsky, S. V. Biometric systems and technologies: fundamentals, methods, tools. – Moscow: Hotline – Telecom, 2019, 304 p.
2. Zhuravlev, Yu. I., Pankratova, N. D., Petrov, V. S. Identification of personality by biometric signs. Moscow: Fizmatlit, 2021. 248 p.

Сведения об авторах

Романов Д.А., учащийся учреждение образования «Национальный детский технопарк», dimromgomell@gmail.com
Колбанов Г.П., учащийся, учреждение образования «Национальный детский технопарк», grigoriy.kolbanov@gmail.com
Белоусова Е.С. канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Romanov D.A., Student, Educational Institution "National Children's Technopark".
Kolbanov G.P., Student, Educational Institution "National Children's Technopark".
Belousova E.S., PhD, Associate Professor, Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", belousova@bsuir.by.

УДК 621.382.33-027.45

ОПРЕДЕЛЕНИЕ ИНФОРМАТИВНЫХ ПАРАМЕТРОВ МЕТОДОМ КОРРЕЛЯЦИОННОГО АНАЛИЗА

И.В. Русак
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Для индивидуального прогнозирования надежности полупроводниковых приборов большой мощности необходимо знать их информативные параметры. Поиск этих параметров выполняется с помощью различных экспериментальных исследований. В качестве транзисторов большой мощности использовались биполярные транзисторы КТ872А с измерением электрических параметров, которые могут оказаться информативными. Большой размер выборки транзисторов и большое число параметров обусловили очень большой объем данных, подлежащих обработке. Произведенная аналитика и корреляционный анализ параметров позволили сократить их число и тем самым упростить дальнейшие экспериментальные исследования при проведении ускоренных испытаний транзисторов на надежность, а также определить параметры, которые просты в измерении. В качестве метода аналитики и обработки данных был использован корреляционный анализ информативных параметров.
Ключевые слова: надежность; транзисторы большой мощности; информативные параметры, корреляционный анализ; индивидуальное прогнозирование.

IDENTIFICATION OF INFORMATIVE PARAMETERS BY THE METHOD OF CORRELATION ANALYSIS

I.V. Rusak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. To individually predict the reliability of high-power semiconductor devices, it is necessary to know their informative parameters. The search for these parameters is carried out using various experimental studies. The high-power transistors used were KT872A bipolar transistors with measurement of electrical parameters, which may be informative. The large sample size of transistors and the large number of parameters led to a very large amount of data to be processed. The analysis and correlation analysis of the parameters made it possible to reduce their number and thereby simplify further experimental studies of transistors during accelerated reliability tests, as well as to determine parameters that are easy to measure. Correlation analysis of informative parameters was used as a method of data analysis and processing.
Keywords: reliability; high-power transistors; informative parameters, correlation analysis; individual forecasting.

Введение

Среди способов обеспечения безотказности электронной аппаратуры эффективным является постановка в нее элементов повышенного уровня надежности. Данная процедура для мощных полупроводниковых приборов является актуальной. Отбор транзисторов повышенного уровня надежности может быть выполнен с помощью индивидуального прогнозирования класса надежности экземпляров для заданной наработки, используя информативные параметры транзисторов [1]. Отметим, что информативные параметры измеряются у конкретного экземпляра в начальный момент времени и по их значениям прогнозируют класс работоспособности этого экземпляра для заданной наработки: K_1 – класс работоспособных (иначе – надежных), класс K_2 – класс неработоспособных (иначе – потенциально ненадежных) экземпляров. Для решения задачи прогнозирования класса надежности полупроводниковых приборов для заданной наработки надо знать их информативные параметры.

Поиск информативных параметров обычно выполняется с помощью экспериментальных исследований. Первым этапом таких исследований является измерение в начальный момент времени у каждого экземпляра определенной выборки однотипных полупроводниковых приборов тех электрических параметров, которые гипотетически могут оказаться информативными. Выборку называют обучающей, ее объем составляет примерно 50–200 экземпляров, экземпляры выборки нумеруют. Затем выполняют испытания экземпляров обучающей выборки на надежность, используя ускоренные форсированные испытания, эквивалентные интересующей заданной наработке в нормальных условиях работы. На момент окончания ускоренных испытаний регистрируют класс каждого экземпляра с точки зрения его работоспособности. Информативность электрических параметров обычно оценивают методом корреляционного анализа [2].

Основная часть

Решалась задача поиска информативных параметров для биполярных транзисторов большой мощности типа КТ872А. Объем обучающей выборки составлял 200 экземпляров. В число измеряемых параметров были включены как электрические параметры, нормируемые в технических условиях, так и специфические параметры, которые не указываются в документации или справочниках, например, добротность

емкости *p-n*-переходов. Пояснение электрических параметров, которые по экспериментальным данным оказались наиболее информативными, приведено в табл. 1.

Таблица 1. Пояснение параметров транзисторов типа КТ872А
Table 1. Explanation of the parameters of transistors of the type KT872A

Электрический параметр	Обозначение по ГОСТ 20003–74	Единица измерения
1. Статический коэффициент передачи тока биполярного транзистора	$h_{21Э}$	–
2. Обратный ток коллектора	$I_{КБО}$	мкА
3. Напряжение насыщения коллектор-эмиттер	$U_{КЭнас}$	мВ
4. Пробивное напряжение коллектор-база	$U_{КБОпроб}$	В

При решении практических задач индивидуального прогнозирования класса работоспособности изделий электронной техники используют 2–5 информативных параметров. Для принятия решения о выборе информативных параметров получены коэффициенты корреляции электрических параметров с номером класса (1 или 2). Использовался инструмент «Корреляция» пакета «Анализ данных» компьютерной программы Microsoft Excel.

Фрагментом полученной корреляционной матрицей, в которую включены четыре наиболее информативных параметра, является табл. 2

Таблица 2. Корреляционная матрица параметров (транзисторы типа КТ872А)
Table 2. Correlation matrix of parameters (transistors type KT872A)

Электрический параметр, номер класса работоспособности	$h_{21Э}$	$I_{КБО}$	$U_{КЭнас}$	$U_{КБОпроб}$	S
1 $h_{21Э}$	1	–	–	–	–
2 $I_{КБО}$	–0,109	1	–	–	–
3 $U_{КЭнас}$	–0,783	0,197	1	–	–
4 $U_{КБОпроб}$	–0,081	0,026	-0,079	1	–
5 Номер класса работоспособности (S) для t = 15 000 ч	0,452	-0,453	-0,443	-0,370	1

Анализируя корреляционную матрицу, можно убедиться, что класс надежности транзистора заметно коррелирован со следующими параметрами $h_{21Э}$, $I_{КБО}$ и $U_{КЭнас}$. Наименование параметров соответствует табл. 1.

Заключение

Для поиска информативных параметров, необходимых для прогнозирования класса надежности мощных транзисторов КТ872А, были измерены электрические параметры, предполагаемые на информативность, у каждого экземпляра обучающей выборки. В качестве критерия информативности рассматривался модуль коэффициента корреляции между значениями электрического параметра в начальный момент времени и номером класса надежности (S = 1, 2) экземпляров обучающей выборки на момент окончания ускоренных испытаний транзисторов.

Список использованных источников

1. Боровиков С.М. (2013) *Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники*. Москва, Издательство «Новое знание».

2. Харченко М.А. (2008) *Корреляционный анализ*. Воронеж, Издательско-полиграфический центр Воронежского государственного университета.

References

1. Borovikov S.M. (2013) *Statistical Forecasting for Rejection of Potentially Unreliable Elec-tronic Products.* Moscow, New Knowledge Publishing House (in Russian).
2. Kharchenko M.A. (2008) *Correlation analysis*. Voronezh, Publishing and Printing Center of Voronezh State University.

Сведения об авторе

Русак И.В. , магистрант кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», iliaru756@gmail.com

Information about the author

Rusak I., Postgraduate of the Department of Information and Computer Systems Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", iliaru756@gmai.com

УДК 004.773:004.056.5

ПЕРЕНАПРАВЛЕНИЕ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ MITM

Т.Б. Русецкая
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В материалах доклада представлены результаты анализа уязвимости ICMP протокола и реализация кибератаки ICMP Redirect в среде виртуализации VirtualBox. Кибератака проведена на виртуальном макете, состоящем из устройств нарушителя, целевого устройства, маршрутизатора и клиентской машины. Исследование включает в себя описание методов эксплуатации уязвимости протокола ICMP, а также последствия кибератаки для безопасности сети. В результате анализа были выявлены основные факторы, способствующие успешному проведению кибератаки, а также предложены рекомендации для повышения уровня защиты информационной системы и минимизации рисков. Полученные данные могут быть полезны для специалистов в области защиты информации и разработки эффективных мер по предотвращению подобных угроз, а также для улучшения безопасности сетевых коммуникаций.
Ключевые слова: MITM; ICMP протокол; ICMP Redirect; сетевые кибератаки; сетевой трафик; VirtualBox; анализ уязвимости; Wireshark; IP-адрес; сетевая инфраструктура.

REDIRECT OF NETWORK TRAFFIC USING MITM ATTACK

T.B. Rusetskaya
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The report presents the findings of an investigation into the vulnerabilities of the ICMP protocol and the ICMP Redirect attack within the VirtualBox virtualization environment. The cyberattack was conducted on a virtual mockup comprising the intruder's devices, the target device, the router and the client machine. The study provides a comprehensive overview of the methods employed to exploit the vulnerabilities of the ICMP protocol, in addition to the repercussions of the attack on network security. The analysis yielded key factors contributing to the success of the attack, and recommendations for enhancing the protection of information systems and mitigating risks were proposed. The findings from this study are likely to be of value to information security specialists in the fields of information protection and the development of effective measures to prevent such threats, as well as to improve the security of network communications.
Keywords: MITM-attack; ICMP protocol; ICMP Redirect; network attacks; network traffic; VirtualBox; vulnerability analysis; Wireshark; IP-address; network infrastructure.

Введение

MITM (man in the middle) – это атака, при которой нарушитель получает доступ к каналу связи между легитимными сторонами (пользователями, приложениями, сетевыми устройствами), что позволяет ему просматривать содержимое всех передаваемых ими сообщений, удалять и изменять их.

ICMP (Internet Control Message Protocol) – это протокол, предназначенный для отправки сообщений об ошибках и передачи служебной информации, которая указывает на успех или неудачу при обмене данными с другим IP-адресом. Обычно ICMP не используется для передачи данных между устройствами, а применяется для проверки связи между двумя узлами с помощью программ, таких как ping или traceroute.

Актуальность проблемы сетевой кибератаки ICMP Redirect сохраняется на сегодняшний момент. ICMP Redirect – это кибератака, основанная на уязвимости передачи ICMP-пакетов. В ходе ее проведения нарушитель использует поддельные ICMP-сообщения для управления маршрутизацией сетевого трафика. Сначала атакующий сканирует сеть, определяет целевое устройство, перехватывает трафик сети, отправляет ICMP Redirect сообщения целевому устройству, перенаправляет трафик через свой узел, анализирует и завершает атаку, восстанавливая нормальную маршрутизацию трафика.

Формат ICMP Redirect сообщения состоит из следующих полей (рис. 1):

– Тип (5);

– Код (0 – перенаправление пакетов для сети, 1 – перенаправление пакетов для узла, 2 – перенаправление пакетов в зависимости от типа службы и сети, 3 – перенаправление пакетов в зависимости от типа службы и узла);

– Контрольная сумма;

– IP-адрес шлюза (адрес шлюза, на который направляется трафик для сети, указанной в поле «Internet destination network»);

– Заголовок IP + 64 бита данных.

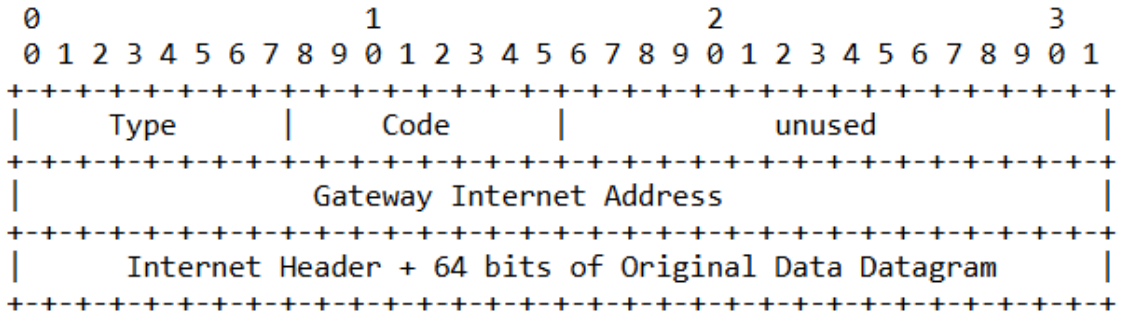


Рис. 1. Формат ICMP Redirect сообщения
Fig.1. Format of ICMP Redirect message

Цель данной работы заключается в рассмотрении проведения кибератаки с использованием ICMP Redirect и анализа перехваченного трафика.

Основная часть

Для проведения MITM кибератаки с использованием ICMP Redirect была использована платформа виртуализации VirtualBox. Создана локальная сеть из 4 виртуальных машин:

– компьютер нарушителя с ОС Kali Linux (attacker);

– компьютер «жертвы» с ОС Ubuntu (victim);
– клиентская машина с ОС Ubuntu (server);
– маршрутизатор Mikrotik (router_mikrotik).

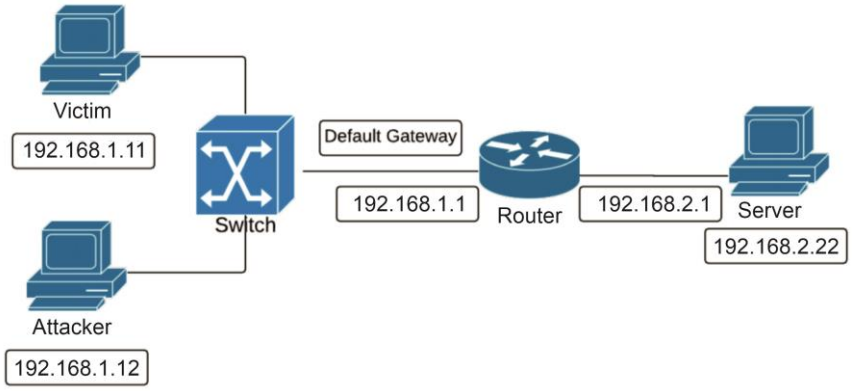


Рис. 2. Топология сети
Fig.2. Network topology

При изучении принципа передачи ICMP пакетов были выявлены несколько уязвимостей. Одной из функций протокола ICMP является управление таблицами маршрутизации на узлах внутри сегмента сети. Сообщения ICMP могут содержать информацию о перенаправлении. Такие сообщения позволяют оптимизировать маршрутизацию пакетов через более эффективные маршруты.

Атака ICMP Redirect заключается в том, что нарушитель отправляет поддельное сообщение ICMP Redirect целевому узлу, указывая предпочтительный маршрут для передачи данных. Цель данной кибератаки – изменить таблицу маршрутизации на целевом узле, чтобы перенаправить трафик через узел нарушителя.

На рисунке 2 показана топология сети в среде виртуализации VirtualBox. Из топологии видно, что виртуальная машина «жертвы» имеет IP-адрес 192.168.1.11/24, нарушитель – 192.168.1.12/24, на интерфейсах маршрутизатора настроены 192.168.1.1/24 и 192.168.2.1/24, на клиентской машине – 192.168.2.22/24.

Далее на устройстве нарушителя происходит сканирование сети с помощью инструмента nmap для обнаружения узлов в сети (рис. 3):

```
┌──(root㉿attacker)-[/home/kali]
└─# nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-20 10:56 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
 specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
MAC Address: 08:00:27:15:3B:3A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.11
Host is up (0.00043s latency).
MAC Address: 08:00:27:68:77:1B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.12
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.96 seconds
```

Рис. 3. Запуск сканирования сети с помощью nmap
Fig.3. Network scan launch using nmap

На рисунке 3 можно заметитить, что в сети 192.168.1.0/24 существует 3 IP-адреса. IP-адрес 192.168.1.11/24 – это адрес целевого устройства.

После этого в Wireshark осуществляем перехват трафика по фильтру ip.add == 192.168.1.11 (рис. 4):

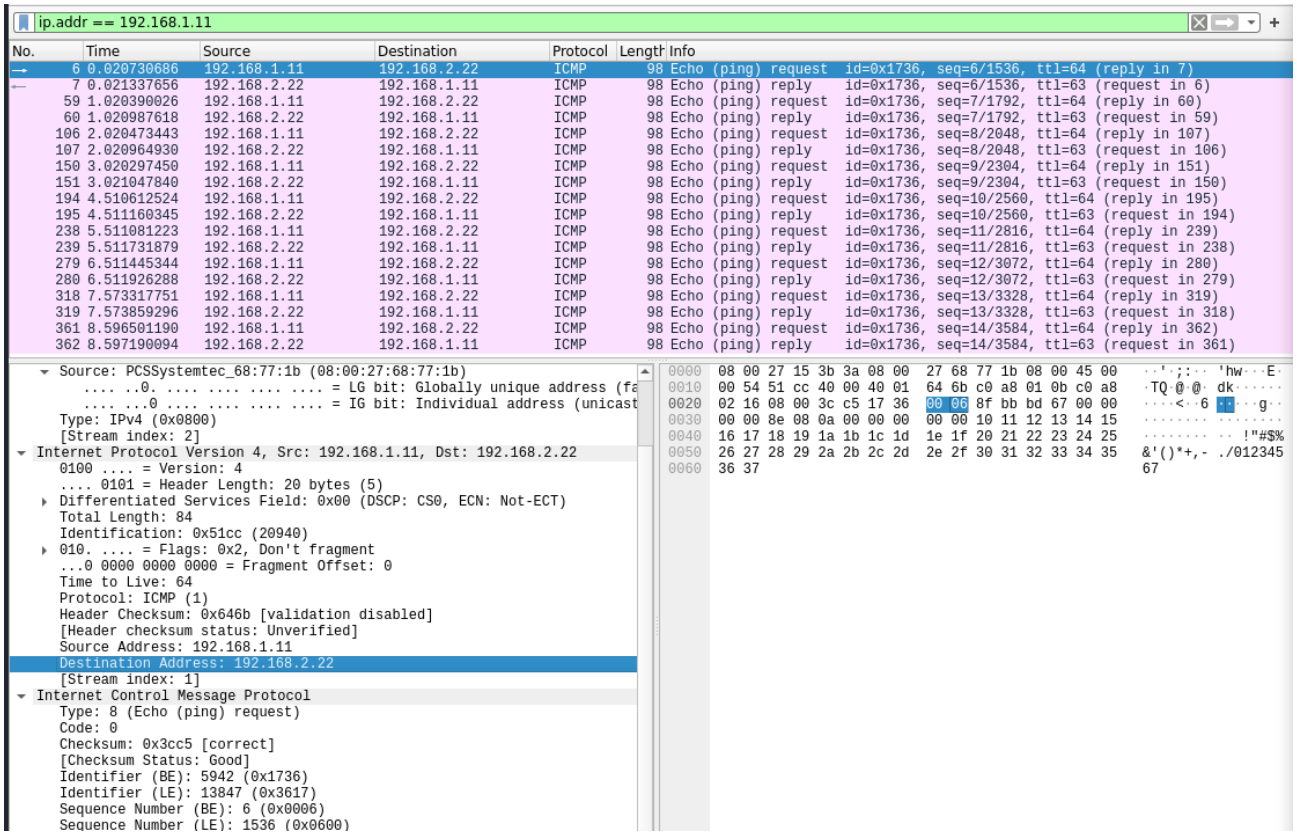


Рис. 4. Перехват сетевого трафика
Fig.4. Interception of network traffic

Из рис. 4 нарушитель получает информацию об IP-адресе клиентской машины. Располагая полученной информацией, можно реализовать кибератаку ICMP Redirect с помощью команды netwox (рис. 5).

Рис. 5. Использование инструмента netwox
Fig. 5. Using the netwox tool

С помощью утилиты netwox нарушитель создает и отправляет поддельные ICMP Redirect сообщения:

1. netwox 86 – предназначен для отправки ICMP Redirect сообщений;
2. -d "eth0" указывает интерфейс, через который будет отправляться трафик;
3. --filter "src host 192.168.1.11" – устанавливает фильтр, чтобы отправлять сообщения только для трафика, исходящего от узла с IP-адресом 192.168.1.11/24;
4. --gw 192.168.1.12 задает IP-адрес шлюза, который будет использоваться для перенаправления трафика;
5. spoofip "raw" – включает подмену IP-адресов в режиме raw, что позволяет изменять IP-адрес источника пакетов;
6. --code 0 – указывает код ICMP-сообщения, что соответствует типу эхо-ответ;
7. --src-ip 192.168.2.22 – указывает IP-адрес, который будет использоваться в качестве источника для поддельных ICMP Redirect-сообщений.

На рисунке 6 видно, что трафик, идущий от устройства victim (IP-адрес 192.168.1.11/24) перенаправлен на узел с IP-адресом 192.168.1.12/24:

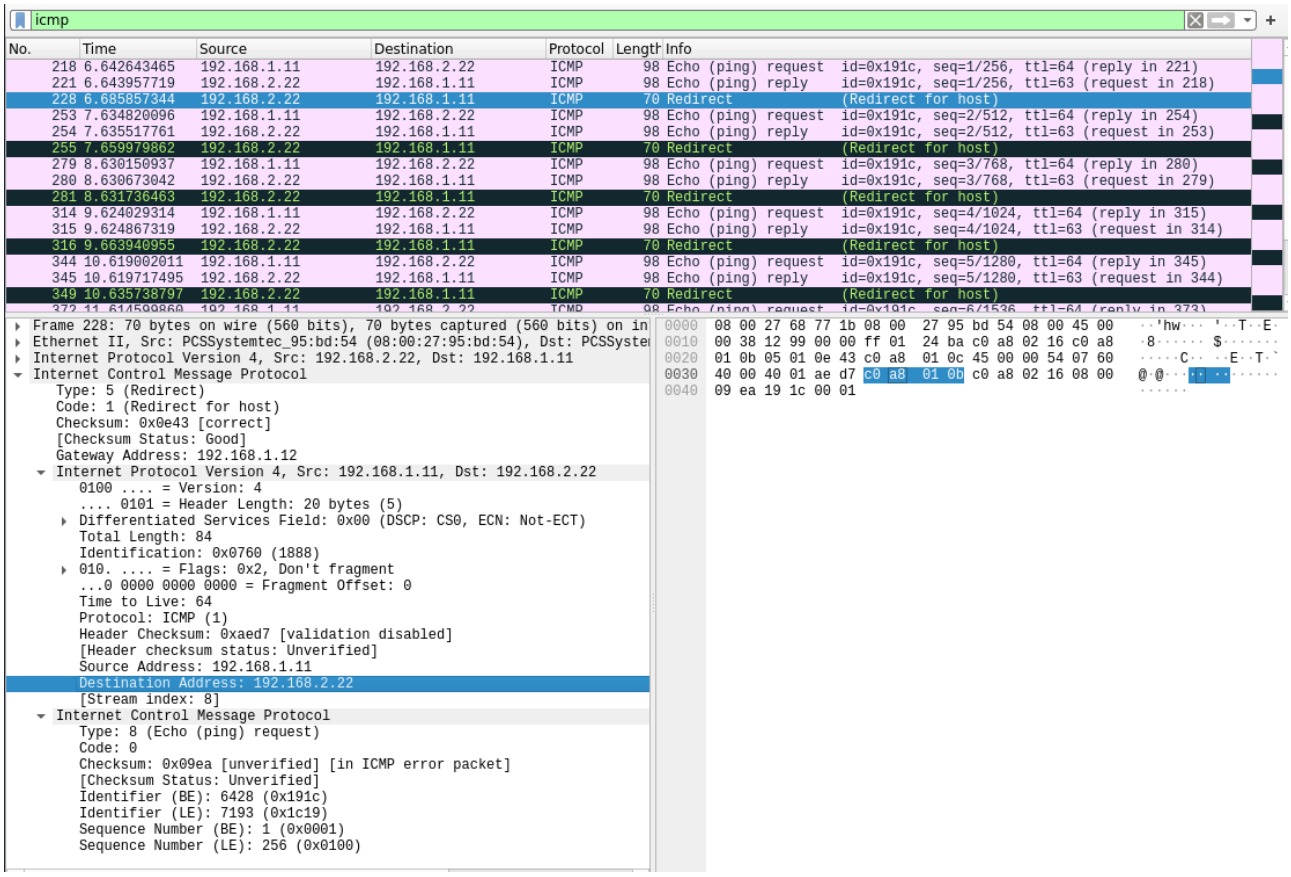


Рис. 6. Анализ трафика в Wireshark
Fig.6. Traffic analysis in Wireshark

Из рис. 6 можно заметить, что тип отправляемого сообщения является 5 или Redirect-сообщение (указывает отправителю на существование более эффективного маршрута для передачи данных).

Заключение

На основе полученных результатов можно сделать вывод что уязвимость протокола ICMP может быть использована для проведения кибератаки Man-in-the-middle, перехвата и изменения сетевого трафика, а также для создания угроз безопасности информации, которые могут привести к нарушению целостности и конфиденциальности данных в компьютерных сетях. Поэтому разработка и внедрение эффективных методов зашиты от таких атак является актуальной задачей для обеспечения устойчивости сетевых инфраструктур.

Список использованных источников

1. Ylli E., Fejzaj J. (2021) Man in the Middle: Attack and Protection. *RTA-CSIT*. 198-204
2. Arkin O. (2000). ICMP Usage in Scanning. *Black Hat Briefings*. 1–6.
3. Waichal S., Meshram B.B. (2013) Router Attacks-Detection And Defense Mechanisms. *International Journal of Scientific & Technology Research. IJSTR*. 2 (6), 1-6.
4. Feng X., Liyx Q., Sunz K., Yang Y., Xu K. (2023) Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. *IEEE Symposium on Security and Privacy (SP). IEEE*. 3162-3177.
5. Postel J. (1981). RFC0777: Internet Control Message Protocol. *RFC*. 1–6.

References

1. Ylli E., Fejzaj J. (2021) Man in the Middle: Attack and Protection. *RTA-CSIT*. 198-204
2. Arkin O. (2000). ICMP Usage in Scanning. *Black Hat Briefings*. 1–6.
3. Waichal S., Meshram B.B. (2013) Router Attacks-Detection And Defense Mechanisms. *International Journal of Scientific & Technology Research. IJSTR*. 2 (6), 1-6.
4. Feng X., Liyx Q., Sunz K., Yang Y., Xu K. (2023) Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. *IEEE Symposium on Security and Privacy (SP). IEEE*. 3162-3177.
5. Postel J. (1981). RFC0777: Internet Control Message Protocol. *RFC*. 1–6.

Сведения об авторе

Русецкая Т.Б., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», flowt10932@gmail.com.

Information about the author

Rusetskaya T., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", flowt10932@gmail.com.

УДК 377.031

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Е.Г. Ручаевская, В.В. Шаталова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», Минск, Беларусь

Аннотация. Безопасность любой информационной системы можно определить как свойство, которое заключается в способности информационной системы обеспечить полную конфиденциальность и целостность хранимой информации, т.е. защиту данных от несанкционированного доступа, например в целях ее раскрытия, изменения или разрушения. Обеспечение информационной безопасности в информационно-вычислительных системах сегодня очень актуально. Информационную безопасность можно выделить как одну из основных информационных проблем XXI века. На самом деле, проблемы хищения информации, искажения смысла информации и ее уничтожения часто приводят к последствиям, ведущим не только к банкротствам фирм, но даже возможным жертвам (не говоря о возможных военных конфликтах). Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. Поэтому правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем.
Ключевые слова: информационные системы; информационные технологии; информационная безопасность; защита данных; несанкционированный доступ; информация; хищение информации; информационные проблемы; целостность информации; защита информации.

INFORMATION PROTECTION IN INFORMATION COMPUTING SYSTEM

E.G. Ruchaevskaya, V.V. Shatalova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", Minsk, Belarus

Abstract. The security of any information system can be defined as a property that consists in the ability of an information system to ensure complete confidentiality and integrity of stored information, i.e. protection of data from unauthorized access, for example for the purpose of its disclosure, modification or destruction. Ensuring information security is very important today. Information security can be identified as one of the main information problems of the 21st century. In fact, problems of information theft, distortion of the meaning of information and its destruction often lead to consequences leading not only to the bankruptcy of companies, but even to possible victims (not to mention possible military conflicts). Information protection is a set of measures aimed at ensuring information security. Therefore, a methodologically correct approach to information security problems begins with identifying the subjects of information relations and the interests of these subjects associated with the use of information systems.
Keywords: information systems; information Technology; information security; data protection; unauthorized access; information; theft of information; information problems; integrity of information; information protection.

Введение

Проблемы обеспечения защиты информации являются одними из важнейших при построении надежной информационной системы на базе ПЭВМ. Эти проблемы охватывают как защиту от несанкционированного доступа к данным, так и физическую защиту данных и системных программ, особенно защиту от компьютерного вируса. Таким образом, в понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным (санкционированность).

Основная часть

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Эти действия являются базовыми для дальнейшего рассмотрения.

Придерживаясь принятой классификации будем разделять все источники угроз на внешние и внутренние.

Источниками внутренних угроз являются:

– Сотрудники организации;

– Программное обеспечение;

– Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;

– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;

– ошибки в работе программного обеспечения;

– отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

– компьютерные вирусы и вредоносные программы;

– организации и отдельные лица;

– стихийные бедствия.

Формами проявления внешних угроз являются:

– заражение компьютеров вирусами или вредоносными программами;

– несанкционированный доступ (НСД) к корпоративной информации;

– информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

– действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

– аварии, пожары, техногенные катастрофы.

Угрозы для информационных систем можно представить следующими группами:

– угроза раскрытия – имеющаяся возможность доступа к определенной информации лицу, не имеющему права знать данную информацию.

– угроза целостности – намеренное несанкционированное изменение данных, которые хранятся в вычислительной системе или передаются из одной системы в другую по каналам связи (модификация или удаление).

Средства, которыми может быть обеспечена информационная безопасность, в зависимости от способа реализации можно разбить на следующие группы методов:

– организационные методы предполагают конфигурирование, организацию и администрирование информационной системы. Прежде всего, это относится к сетевым информационным системам и их операционным системам, полномочиям системного администратора, набору инструкций, которые определяют порядок доступа и функционирования в сети пользователей;

– технологические методы, охватывающие технологии осуществления сетевого администрирования, мониторинга и аудита безопасности ресурсов данных, ведения журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

– аппаратные методы, которые должны реализовать физическую защиту информационной системы от возможного несанкционированного доступа, аппаратные средства идентификации внешних терминалов системы и пользователей и т.д.;

– программные методы относятся к самым распространенным методам защиты информации (программы идентификации пользователей, программы парольной защиты, программы проверки полномочий, брандмауэры, криптопротоколы и т.д.). Без применения программной составляющей фактически невыполнимы даже первые три группы методов. При этом нужно учитывать, что стоимость реализации сложных программных комплексов по защите информации может значительно превосходить по затратам аппаратные, технологические и тем более организационные решения.

Со стороны разработчиков и потребителей в настоящее время наибольшее внимание вызывают следующие тенденции защиты информации:

– защита от несанкционированного доступа информационных ресурсов компьютеров, работающих автономно и в сети. В первую очередь эта проблема определяется для серверов и пользователей Интернета. Эта функция может быть реализована многочисленными программными, а также программно-аппаратными и аппаратными средствами;

– защита различных информационных систем от компьютерных вирусов, имеющих возможность не только разрушить необходимую информацию, но даже повредить технические компоненты системы;

– защита секретной, конфиденциальной и личной информации от чтения посторонними лицами и целенаправленного ее искажения. Эта функция может обеспечиваться как средствами защиты от несанкционированного доступа, так и с помощью криптографических средств, традиционно выделяемых в отдельный класс.

Также активно развиваются средства защиты от утечки информации по силовым каналам, каналам электромагнитного излучения компьютера или монитора (для решения данной проблемы может применяется экранирование помещений, использование генераторов шумовых излучений), средства защиты от электронных «жучков», устанавливаемых непосредственно в комплектующие компьютера и т. д.

Защита информации от несанкционированного доступа. Защита от несанкционированного доступа к информационным ресурсам компьютера представляется комплексной проблемой, которая предполагает решение следующих задач:

– присвоение пользователю, файлам, компьютерным программам и каналам связи идентификаторов – уникальных имен и кодов;

– установление подлинности при обращениях к вычислительной системе и информации, по сути, проверка соответствия лица или устройства, сообщившего идентификатор (такая идентификация пользователей, программ, терминалов при доступе к системе зачастую выполняется посредством проверки паролей или обращением в службу, которая отвечает за сертификацию пользователей).

Информационная безопасность включает меры по защите процессов создания данных, их ввода, обработки и вывода. Главная цель состоит в том, чтобы защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, когда информация создается, модифицируется, когда к ней обеспечивается доступ и когда она распространяется.

Информационная безопасность гарантирует достижение следующих целей:

– конфиденциальность критической информации;

– целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);

– доступность информации в случае необходимости;

– учет всех процессов, связанных с информацией.

Угроза безопасности компьютерной системы – это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Уязвимость компьютерной системы – это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нежелательные события.

Атака на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака – это реализация угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система защиты должна адекватно реагировать на любое из них.

Угроза раскрытия заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова «раскрытие» используются термины «кража» или «утечка».

Заключение

В заключении можно отметить, что защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу и государству.

Список использованных источников

1. Абразовский Ю.Д., Ручаевская Е.Г. (2024) Безопасность информационных технологий. *60 Научно-практическая конференция аспирантов, магистрантов и студентов БГУИР. Научная конференция учащихся филиала БГУИР «Минский радиотехнический колледж»,* 17–18.

References

1. Abrazovski J.D., Ruchaevskaya E.G. (2024) Safety information technologies. *60 Scientific practical conference-практическая конференция of postgraduates, masters and students BSUIR. Scientific students conference branch «Minsk Radio Engineering College»,* 17–18.

Сведения об авторах

Ручаевская Е.Г., канд. пед. наук, доц., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», elenruch@gmail.com.
Шаталова В.В., канд. техн. наук, доц., директор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», shatalova@bsuir.by.

Information about the authors

Ruchaevskaya E. Cand. Sci. Ped., Associate Professor, teacher, educational institution «Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", elenruch@gmal.com.
Shatalova V., Cand. Sci. Tech., Associate Professor, director, Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch «Minsk Radio Engineering College», Shatalova@bsuir.by.

УДК 004.021

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ И АЛГОРИТМЫ КОНСЕНСУСА ПРИ КВАНТОВОМ ШИФРОВАНИИ

А.В. Сидоренко, И.А. Приходько
Белорусский государственный университет, Минск, Республика

Аннотация. В работе приведены основные аспекты использования квантовых вычислений и блокчейна для обеспечения надежности и безопасности блокчейн сетей. Рассматриваются основные параметры протокола квантового распределения ключа и создания консенсуса в блокчейне. Представлены основные особенности, состав и характеристики разработанной реализации компьютерной программы прототипа блокчейн, полученные при использовании пакета QISKit.
Ключевые слова: квантовое шифрование; квантовый блокчейн; алгоритмы консенсуса; компьютерная программа

QUANTUM KEY DISTRIBUTION AND ALGORITHMS OF CONSENSUS FOR QUANTUM INFORMATION CODING

A.V. Sidorenko, I. A. Prihodko
Belarusian State University, Minsk, Belarus

Abstract. The main aspects of using quantum computation and blockchain for security, reliability and safety of blockchain networks. are presented. The based parameters of Quantum Distribution Keys, protocol of consensus are created for blockchain. The main features, structure and properties of created computer protocol of prototype blockchain are received by using QUISKit software package
Keywords: quantum encoding; quantum blockchain; algorithms of consensus; computer program

Введение

Интенсивное развитие новых технологий квантовых вычислений и блокчейна способствуют созданию более стойких криптографических методов при обеспечении

устойчивых к квантовым атакам алгоритмов шифрования. В данной работе исследованы возможности использования квантовых принципов при проектировании различных архитектур в технологии блокчейн

Рассматриваются вопросы квантового распределения ключей и алгоритмов консенсуса, которые обеспечивают надежность и безопасность блокчейн сетей.

Для обеспечения дополнительного уровня безопасности и уникальности блокчейна рассмотрена интеграция квантовой запутанности и алгоритмов консенсуса.

Целью работы является программная реализация архитектуры блокчейна с интегрированием квантового распределения ключа и алгоритма консенсуса Delegated Proof – of - Stake (DPoS).

Квантовое распределение ключей алгоритмы консенсуса

В основе квантовой криптографии лежит метод квантового распределения ключа (QKD). Применение принципа квантовой запутанности позволяет осуществить через оптический канал обмен информацией в кубитах при генерации скрытого ключа, устойчивого к атакам «прослушивание». Такая атака может производиться злоумышленниками в открытых каналах связи на электронные устройства, компьютеры и смартфоны. Квантовое распределение ключа использует комбинацию квантового канала и не секретность классического канала и позволяет надлежащим образом аутентифицировать распределение секретного ключа между двумя участниками. Фундаментальный принцип квантового распределения ключа основан на возмущении вызванного актом измерений квантовой системы, что позволяет немедленно обнаружить любой случай несанкционированного перехвата ключей.

Для квантового распределения ключей в настоящее время используется ряд протоколов: BB-84, B-92, E-91 и SARG-04, каждый из которых имеет отдельные преимущества и ограничения. Протокол E-91, выбранный нами для реализации компьютерной программы, основан на квантовой запутанности между двумя участниками. Доверенным источником генерируется запутанная пара частиц, квантовое состояние которых характеризуется состояниями Белла, после чего одна частица отправляется по квантовому каналу передающей стороне, другая – приемной стороне. Передающая сторона производит измерение проекции спинов полученных частиц на одно, случайно выбранное направление $\{0, \pi/8, \pi/4\}$, а приемная – на одно из $\{-\pi/8, 0, \pi/8\}$. Эти направления выбраны автором протокола для исполнения неравенств Белла. После чего по классическому каналу связи передающая и приемная стороны обмениваются базисами, в которых проводили измерения состояний частиц. Результаты измерений проекций спинов частиц на разные направления, используются для вычисления корреляционного значения. Если оно значительно отличается от $(-2\sqrt{2})$, то это значит, что запутанность состояний была нарушена либо шумами в квантовом канале, либо фактом прослушивания канала.

Блокчейн, в отличие от обычной базы данных, администрируемой централизованно, представляет собой одноранговую децентрализованную сеть, с которой может взаимодействовать любой участник. Классический блокчейн представляет из себя последовательную цепочку блоков данных. Блоки записываются один за другим, и, в зависимости от того, каким образом они записываются в цепочку, блокчейн обладает теми или иными определенными базовыми свойствами. Для того, чтобы система работала и, учитывала, что узлы блокчейна не зависят друг от друга, используются алгоритмы консенсуса блокчейна.

Алгоритмы консенсуса представляют собой совокупность принципов и правил, благодаря которым все участвующие в сети узлы автоматически приходят к консенсусу

о текущем состоянии сети. Это позволяет гарантировать безопасность сети, то есть достоверность всех хранящихся в ней данных. К наиболее распространенным алгоритмам консенсуса относятся: Proof – of - Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), YAC (Yet Another Consensus).

Алгоритм консенсуса Delegated Proof of Stake (DPoS, делегирование полномочий одному участнику), выбранный нами для использования в компьютерной программе, представляет собой разновидность алгоритма PoS. В алгоритме консенсуса DPoS право валидаторов одобрять транзакции декларируется им узлами, владеющими ресурсами сети, при этом они голосуют за того или иного валидатора. Любой участник сети, обладающий определенным объемом ресурсов, может стать валидатором, но также в любой момент голоса за этого валидатора могут быть отозваны в пользу другого. Риск при использовании этого алгоритма консенсуса представляет низкая активность участников, не исключен также сговор делегатов.

Программная реализация

Программная реализация разработанной авторами компьютерной программы проводилась с использованием симулятора квантовых вычислений и на квантовых устройствах компании IBM с применением QISKit (Quantum Information Software Kit), представляющих собой набор средств разработки с открытым исходным кодом для работы с квантовыми устройствами облачной платформы IBM Q [1]. В данной разработке также применена облачная платформа (IBM Quantum Platform), которая дает возможность работы на квантовом компьютере.

Реализация протокола Е-91 производилась компьютерным моделированием на симуляторе квантовых вычислений и квантовых устройствах с использованием QISKit.

В реализации структуры блокчейна был использован язык программирования Phyton. Определяющая структуру программы платформа "Flask" позволяет при помощи HTTP- запросов взаимодействовать с блокчейном в сети, регистрируя новые связанные узлы сети, тем самым делая его полноценной децентрализованной системой. Запустив исходный код программы, мы запускаем сервер. С помощью GET-запроса "http://localhost:5000/mine"формируется единый узел в нашем блокчейне.

Заключение

Разработана компьютерная реализация прототипа блокчейна с использованием языка программирования Python. Архитектура поддерживает генерацию и использование квантовых ключей для шифрования транзакций, а также включает классические механизмы консенсуса, такие как DPoS. Компьютерная программа квантового распределения ключа Е-91, моделирующая выполнение и тестирование этого протокола, выполнена на симуляторе квантовых вычислений, встроенном в пакете QISKit. и входит в состав разработанной программы.

Список использованных источников

1. IBM Quantum Platform [Электронный ресурс]. Режим доступа; IBM Quantum Platform. Дата доступа; 24.12.2024.

References

1. IBM Quantum Platform[Электронный ресурс]. Режим доступа; IBM Quantum Platform. Дата доступа; 24.12.2024.

Сведения об авторах

Сидоренко А.В., д.-р техн. наук, проф., профессор кафедры физики и аэрокосмических технологий, Белорусский государственный университет**,** e-mail: sidorenkoA@yandex.by.
Приходько И.А. студент факультета радиофизики и компьютерных технологий, Белорусский государственный университет.

Information about the authors

Sidorenko A., Dr. Sci. (Tech.), Professor, Professor of Department of Radiophysics and Computer Technologies, Belarusian State University, sidorenkoA@yandex.by.
Prihodko I. A. Dr. student of Department of Radiophysics and Computer Technologies, Belarusian State University.

УДК 539.143.4

НЕЛИНЕЙНЫЙ ТОКОПЕРЕНОС В НАНОСТРУКТУРЕ ФЕРРОМАГНЕТИК / ШИРОКОЗОННЫЙ ПОЛУПРОВОДНИК / ФЕРРОМАГНЕТИК

Т.Н. Сидорова, А.Л. Данилюк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Аннотация. В данной работе разработана модель токопереноса в туннельных наноструктурах ферромагнетик/ широкозонный полупроводник/ ферромагнетик с использованием двухзонной модели Франца-Кейна и метода фазовых функций. Рассчитаны вольт-амперная характеристика и туннельное магнитосопротивление (ТМС) такой наноструктуры с учетом возникновения дополнительного канала токопереноса через валентную зону широкозонного полупроводника. Показано, что если уровень Ферми E_F лежит ниже середины запрещенной зоны широкозонного полупроводника, в зависимости туннельного тока от внешнего смещения возникают участки отрицательного дифференциального сопротивления (ОДС). Установлено, что ТМС основного канала монотонно спадает, а ТМС дополнительного канала осциллирует с ростом внешнего смещения, коррелируя с ВАХ. Наличие эффекта ОДС в рассматриваемых наноструктурах позволит существенно увеличить значение ТМС, что важно для практических применений.
Ключевые слова: ферромагнетик, широкозонный полупроводник, спин-зависимый токоперенос, вольт-амперная характеристика, туннельное магнитосопротивление, двухзонная модель, метод фазовых функций, валентная зона, ширина запрещенной зоны, отрицательное дифференциальное сопротивление

NONLINEAR TRANSPORT IN THE FERROMAGNETIC/ WIDE-GAP SEMICONDUCTOR/ FERROMAGNETIC NANOSTRUCTURE

T.N. Sidorova, A.L. Danilyuk
Belorussian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

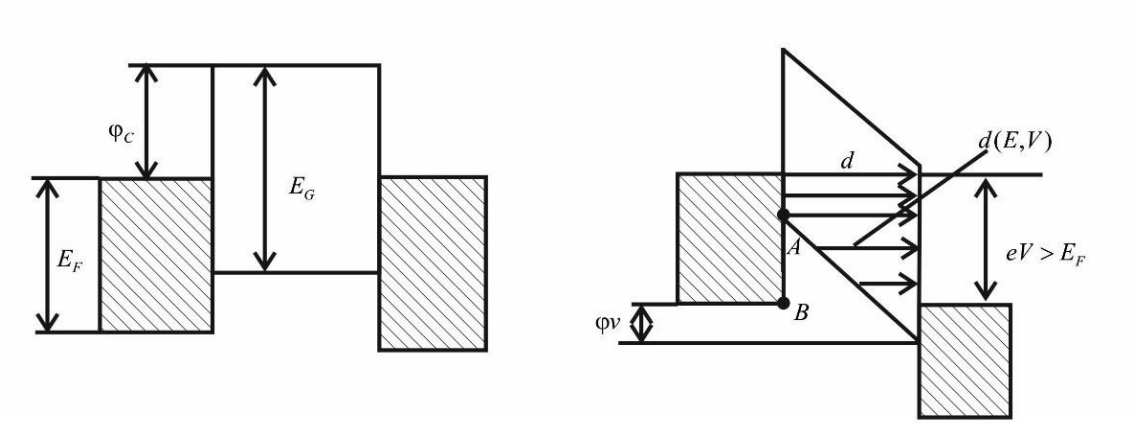
Abstract. Model of the transport in the tunneling nanostructures ferromagnetic/ wide-gap semiconductor / ferromagnetic based on two-band Franz-Kein Model and phase function method was developed. Current-Voltage characteristics and tunneling magnetoresistance (TMR) considering the additional transport channel through the valence band of the wide-gap semiconductor were calculated. Shown, if Fermi level E_F is lower than the middle of the band gap of the wide-band semiconductor, depending on the external bias and tunneling current regions of the negative differential resistance (NDR) appear. It is found out, TMR of the main channel goes down monotonously, at the same time TMR of the additional channel oscillates with the external bias growth, correlating with the Current-Voltage characteristics. Availability of the NDR leads to the TMR increasing, which is important for the practical application
Keywords: ferromagnetic, wide-gap semiconductor, spin-dependent transport, current-voltage characteristic, tunnel magnetoresistance, two-band model, phase function model, valence band, band-gap thickness, negative differential resistance.

Введение

В настоящее время интенсивно исследуются механизмы токопереноса в наноструктурах ферромагнетик/ широкозонный полупроводник / ферромагнетик (ФМ/ШЗП/ФМ) для создания устройств обработки информации, в том числе с использованием спина. Раннее расчет туннельного магнитосопротивления (ТМС) в таких структурах проводился только в рамках однозонной модели.

Модель

В данной работе разработана модель токопереноса в туннельных наноструктурах ферромагнетик/ широкозонный полупроводник / ферромагнетик с использованием двузонной модели [1] и метода фазовых функций [2]. В связи с тем, что валентная зона может давать существенный вклад в токоперенос (наличие дополнительного канала токопереноса), рассмотрим двухзонную модель. Особенностью данной модели является учет валентной зоны в полупроводниковом слое. Туннельный барьер представляет собой не потенциальную ступеньку, а запрещенную полосу энергий, верхней границей которой является дно зоны проводимости E_C, а нижней – потолок валентной зоны E_V.



a *b*

Рис. 1. Потенциальная диаграмма структуры ФМ/ШЗП/ФМ в отсутствии внешнего смещения (*a*) и при его наличии (*b*)

Fig. 1. Potential structure diagram of the structure ferromagnetic/Wide-gap semiconductor/ ferromagnetic without external bias (*a*) and with external bias (*b*)

Внутри этой полосы волновой вектор электрона является мнимой величиной, которая в соответствии с законом Франца-Кейна определяется соотношением [1]

$$k_Z^2 = \frac{2m_i}{h^2}\frac{(E-Ec)(E-E_V)}{E_G} - k_{\|}^2 . \qquad (1)$$

Здесь k_z – перпендикулярная, а $k_{\|}$ – параллельная барьеру составляющие волнового вектора электрона, E – полная энергия электрона, m_i – его эффективная масса, E_G – ширина запрещенной зоны полупроводника.

Величину тока определяем с учетом поперечной составляющей энергии туннелирующего электрона на основе транспортного уравнения [1]:

$$I(V) = \frac{4\pi m_i e}{h^3}\int_0^{\infty} dE(f_L(E) - f_R(E)) \int_0^{(m/m_i)E} dE_{II} T(E, E_{II}, V) , \qquad (2)$$

где E_{II} – компонента электронной энергии E, параллельная плоскости туннельного барьера, m – эффективная масса электрона в электроде (ФМ), а $f_L(E)$ и $f_R(E)$ – функции распределения Ферми- Дирака эмиттера и коллектора, $T(E, E_{II}, V)$ – коэффициент туннельного прохождения.

Для нахождения коэффициента туннельного прохождения нами разработана модель на основе метода фазовых функций [2,3]. Модель учитывает параметры барьера, потенциал сил изображения, позволяет включать потенциальный рельеф границ раздела и в объеме полупроводника. Коэффициент туннельного прохождения через барьер описывается уравнением:

$$T_\sigma = \exp\left[\frac{1}{k_\sigma}\int_a^b U_{eff}(z)\left[b_\sigma(z)\cos(2k_\sigma z) - a_\sigma(z)\sin(2k_\sigma z)\right]dz\right], \quad (3)$$

где эффективный потенциал $U_{eff}=(2m_i/\hbar^2)(U_0+k^2_{\|} - qV(z)-q\varphi(z)\pm V_{sc}(z))$, k_σ – волновой вектор, σ – индекс спиновой компоненты, $\hbar$ – постоянная Планка, U_0 – максимальная величина потенциального барьера для электронов проводимости, φ(z) – потенциал сил изображения; $V_{sc}(z)$ – потенциал рассеяния, учитывающий неоднородность потенциального рельефа, $V(z)$ – электростатический потенциал, q – элементарный заряд.

Результаты

Была рассчитана вольт-амперная характеристика (ВАХ) наноструктуры ФМ/ШЗП/ФМ с учетом возникновения дополнительного канала токопереноса через валентную зону широкозонного полупроводника.

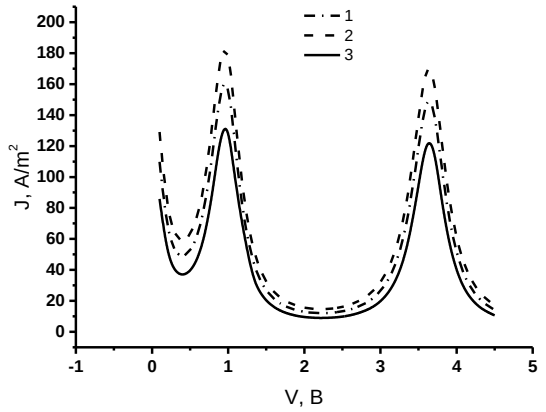


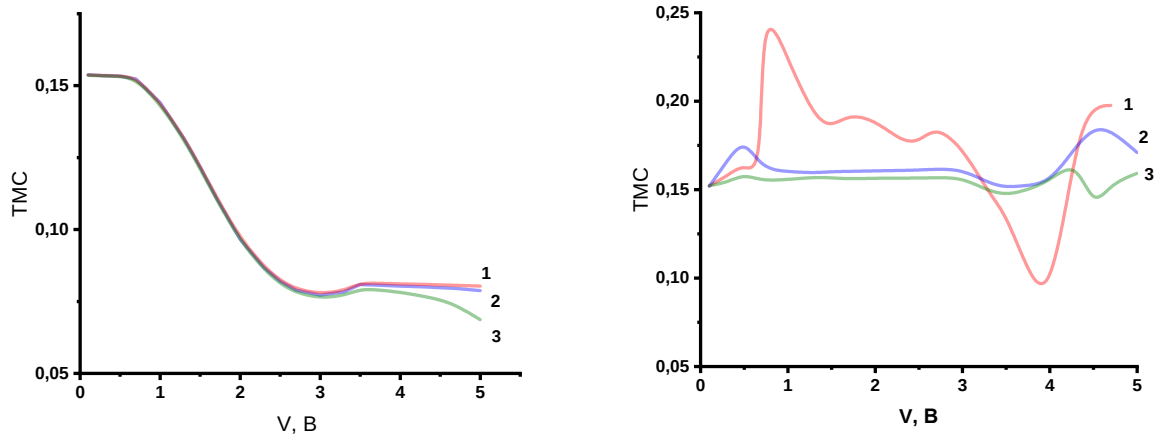
Рис. 2. Вольт-амперная характеристика в зависимости от значения ширины запрещенной зоны полупроводника, где 1 – E_G=8 эВ, 2 – E_G =8,5 эВ, 3 – E_G =7,5 эВ
Fig. 2. Current-Voltage characteristics depending from the band gap thickness, where 1 – E_G=8 eV, 2 – E_G =8,5 eV, 3 – Eσ=7,5 eV

При увеличении значения ширины запрещенной зоны полупроводника с 7,5 эВ до 8,5 эВ (рис. 2) значения плотности тока в пиках меняются с 125 А/м^2 до 180 А/м^2 и с 120 А/м^2 до 175 А/м^2. Поведение ВАХ при этом не меняется. Максимальные пики приходятся на значения 1,0 В и 3,9 В соответственно. При изменении толщины полупроводника значения экстремумов ВАХ не меняются, однако поведение ВАХ притерпевает определенные изменение. При увеличении толщины с 0,5 нм до 2 нм пик смещается в сторону меньшего напряжения. Например, при толщине 0,5 нм пик приходиться на 0,5 В, однако при d = 2 нм пик становится уже.

В вольт-амперных характеристиках наблюдаются области отрицательного дифференциального сопротивления (ОДС). Все кривые имеют резко выраженный максимум, после которого туннельный ток уменьшается. Первый пик можно связать с изменением эффективной толщины ШП, рис. 1б, а второй – с положением уровня Ферми. Если уровень Ферми E_F исследуемой структуры лежит ниже середины запрещенной зоны ШП ($qV > E_F$), то в зависимости туннельного тока от напряжения смещения возникает ОДС.

Таким образом, появление ОДС в вольт-амперной характеристике есть своеобразное проявление зонного эффекта, связанного с изменением положения уровня Ферми эмиттера относительно середины запрещенной зоны ЩП, а также уменьшением эффективной толщины $d(E,V)$ ШП, рис.1, *b*.

Было также рассчитано туннельное магнитосопротивление (ТМС) наноструктуры ФМ/ШЗП/ФМ учитывая возникновение дополнительного канала токопереноса через валентную зону широкозонного полупроводника. ТМС основного канала нелинейно изменяется с 0,15 до 0,03 с ростом внешнего смещения и почти не зависит от толщины до V= 2,5 В (рис. 3, *a*). При V>2,5 В, ТМС расщепляется в зависимости от толщины: наибольшее значение наблюдается при d=2.0 нм, а наименьшее при d = 1,5 нм. Наблюдается локальный минимум (V = 3,0 В) и локальный максимум (V = 3,5–3,6 В). Эти экстремумы коррелируют с экстремумами ВАХ, рис.2. ТМС дополнительного канала с ростом внешнего смещения осциллирует при d=2,0 нм, а при d=1,5 и 2,5 нм практически не изменяется в области 1–3 В (рис. 3, *b*).



a *b*

Рис. 3. Туннельное магнитосопротивление в зависимости от толщины широкозонного полупроводника в случае, когда E_F расположен выше середины запрещенной зоны, где 1 – d = 2 нм, 2 – d=2,5 нм, 3 – d=1,5 нм : *a* – ТМС основного канала, *b* – ТМС дополнительного канала

Fig. 3. Tunneling magnetoresistance depending from the wide band semiconductor thickness when E_F is higher the middle of the band gap , where 1 – d = 2.0 nm, 2 – d = 2.5 nm, 3 – d = 1.5 nm : *a* – TMR of the main channel, *b* – TMR of the additional channel

Для средней толщины в 2,0 нм наблюдается 2 экстремума на графике ТМС дополнительного канала при напряжении около 1 В (ТМС=0,25) и вблизи 4,0 В (ТМС = 0,1). Эти экстремумы могут быть обьяснены взаимозависимостью между наибольшим и наименьшим значением на ВАХ в области ОДС именно при этой толщине. Наличие эффекта ОДС в рассматриваемых наноструктурах позволит существенно увеличить значение ТМС, что важно для практических применений.

Заключение

Согласно проведенным расчетам, ВАХ и туннельное магнитосопротивление наноструктуры ФМ/ШЗП/ФМ являются существенно нелинейными. Такое поведение обусловливается смещением осцилляций коэффициентов туннельного прохождения в область энергии Ферми и уменьшением эффективной толщины ШЗП при росте внешнего смещения. При росте внешнего смещения осцилляции ВАХ И ТМС претерпевают фазовые и амплитудные изменения, обусловленные изменением, как высоты, так и толщины потенциального барьера. Для ШЗП с толщиной равной 1,5 нм и 2,5 нм ТМС для дополнительного канала практически не изменяется. Для толщины 2 нм наблюдается 2 экстремума в зависимости ТМС для дополнительного канала при напряжении смещения около 1 В (ТМС=0,25) и 4 В (ТМС =0,1). Эти экстремумы могут быть объяснены наличием корреляции ТМС с ВАХ.

Список использованных источников

1. K.H. Gundlach, Theory of metal-insulator-metal tunneling for a simple two-band model. J. Appl. Phys. Vol. 44, Iss. 11, P.5005-5010 (1973).
2. Babikov V.V (1976) Phase-function method in quantum mechanics, Moscow, Nauka (in Russian).
3. T.N. Sidorova, Alexander L. Danilyuk (2014), Negative differential resistance in ferromagnet/wide-gap semiconductor/ferromagnet nanostructure, Materials Physics and Mechanics, vol. 20, Iss.2, P.106-110

References

1. K.H. Gundlach, Theory of metal-insulator-metal tunneling for a simple two-band model. J. Appl. Phys. Vol. 44, Iss. 11, P.5005-5010 (1973).
2. Babikov V.V (1976) Phase-function method in quantum mechanics, Moscow, Nauka (in Russian).
3. T.N. Sidorova, Alexander L. Danilyuk (2014), Negative differential resistance in ferromagnet/wide-gap semiconductor/ferromagnet nanostructure, Materials Physics and Mechanics, vol. 20, Iss.2, P.106-110

Сведения об авторах

Сидорова Т.Н., младший научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», sharsu_antea@bk.ru.
Данилюк А.Л., кандидат физико-математических наук, доцент, ведущий научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danilyuk@bsuir.by.

Information about the authors

Sidorova T.N., junior researcher at the Center for Nanoelectronics and New Materials of R&D Department of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", sharsu_antea@bk.ru.
Danilyuk A.L., PhD in Physics and Mathematics, Associate Professor, Leading Researcher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", danilyuk@bsuir.by.

УДК 004.62

ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

К.А. Скалозуб, С.Н. Нестеренков, Е.В. Бегляк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются основные технические аспекты защиты данных в облачных вычислениях. Описаны ключевые угрозы безопасности, такие как утечки данных, атаки на инфраструктуру и компрометация учетных записей, которые могут привести к серьезным последствиям для организаций и пользователей. Анализируются современные технологии защиты,

включая шифрование, многофакторную аутентификацию, модели контроля доступа и технологии защиты данных во время передачи и хранения. Подчеркивается важность интеграции средств защиты в облачные системы для обеспечения их надежности, повышения уровня безопасности и соответствия современным стандартам. Внедрение эффективных методов защиты данных является необходимым условием для минимизации рисков и обеспечения доверия пользователей к облачным сервисам и приложениям, что актуально в условиях быстрого роста объемов данных и увеличения киберугроз.
Ключевые слова: облачные вычисления; защита данных; кибербезопасность; шифрование; аутентификация; контроль доступа; утечки данных; атаки на инфраструктуру; компрометация учетных записей; технологии защиты.

TECHNICAL ASPECTS OF DATA PROTECTION IN CLOUD COMPUTING

K.A. Skalozub, S.N. Nesterenkov, E.V. Begliak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the main technical aspects of data protection in cloud computing. It describes key security threats, such as data leaks, infrastructure attacks, and account compromises, which can lead to serious consequences for organizations and users. Modern protection technologies are analyzed, including encryption, multi-factor authentication, access control models, and data protection technologies during transmission and storage. The importance of integrating protective measures into cloud systems is emphasized to ensure their reliability, enhance security levels, and comply with modern standards. Implementing effective data protection methods is essential for minimizing risks and ensuring user trust in cloud services and applications, which is particularly relevant in the context of rapid data growth and increasing cyber threats.
Keywords: cloud computing; data protection; cybersecurity; encryption; authentication; access control; data leaks; infrastructure attacks; account compromise; protection technologies.

Введение

С развитием облачных вычислений увеличивается объем обрабатываемых и хранящихся данных. Это создает новые вызовы для обеспечения безопасности, так как данные, находящиеся в облаке, могут быть уязвимы для различных угроз. Защита данных становится приоритетной задачей как для поставщиков облачных услуг, так и для их клиентов. В данной статье рассматриваются ключевые угрозы безопасности и современные технологии защиты данных в облачных вычислениях, а также значимость интеграции средств защиты для обеспечения надежности и доверия к облачным сервисам.

Угрозы безопасности

Облачные вычисления подвержены ряду угроз, среди которых:

1. Утечки данных. Данные могут быть случайно или намеренно раскрыты третьим лицам, что приводит к финансовым потерям и потере репутации. Утечки могут происходить из-за недостатков в системе безопасности, человеческого фактора или недобросовестных действий сотрудников.

2. Атаки на инфраструктуру. Хакеры могут целенаправленно атаковать облачные сервисы, используя уязвимости в системах безопасности. Это может включать DDoS-атаки, направленные на перегрузку серверов или атаки на программное обеспечение, использующее уязвимости.

3. Компрометация учетных записей. Неавторизованный доступ к учетным записям может привести к манипуляциям с данными и их утечке. Использование слабых паролей и отсутствие многофакторной аутентификации значительно увеличивают риски.

4. Недостаточная безопасность облачной инфраструктуры. Многие организации полагаются на облачных провайдеров для обеспечения безопасности, однако недостаточная защита на уровне инфраструктуры может привести к серьезным последствиям. Это включает в себя отсутствие шифрования данных и недостаточные меры по управлению доступом.

5. Неправильная конфигурация облачных ресурсов. Ошибки в настройках облачных сервисов могут привести к уязвимостям. Например, неправильно настроенные разрешения могут позволить доступ к данным неавторизованным пользователям.

Технологии защиты данных

Для борьбы с угрозами применяются различные технологии и методы защиты. Шифрование данных, как в процессе передачи, так и в состоянии покоя, является основным методом защиты. Оно защищает данные от несанкционированного доступа, даже если они будут перехвачены. Современные методы шифрования, такие как AES (Advanced Encryption Standard), обеспечивают высокий уровень безопасности и могут использоваться для защиты как файлов, так и сетевых соединений.

Использование многофакторной аутентификации (MFA) значительно повышает уровень безопасности. MFA требует от пользователей предоставления нескольких форм идентификации, что затрудняет доступ злоумышленников. Например, сочетание пароля и одноразового кода, отправленного на мобильный телефон, делает учетные записи более защищенными.

Эффективные модели контроля доступа позволяют ограничить доступ к данным только авторизованным пользователям. Это может быть реализовано через ролевое управление доступом (RBAC) или атрибутное управление доступом (ABAC). Использование таких моделей помогает применять принцип наименьших привилегий, что снижает риски утечек данных.

Системы виртуальных частных сетей (VPN) и протоколы защищенной передачи данных, такие как SSL/TLS, помогают защитить данные во время их передачи через интернет. Эти технологии обеспечивают шифрование и аутентификацию, что позволяет защитить данные от перехвата и несанкционированного доступа.

Регулярный мониторинг и аудит безопасности помогают выявлять и устранять уязвимости. Использование систем обнаружения вторжений (IDS) и систем управления информацией и событиями безопасности (SIEM) позволяет отслеживать подозрительную активность и реагировать на инциденты в реальном времени.

Заключение

Защита данных в облачных вычислениях является сложной, но необходимой задачей, требующей внимания со стороны всех участников процесса. Внедрение современных технологий защиты данных, таких как шифрование, многофакторная аутентификация и модели контроля доступа, поможет минимизировать риски и повысить уровень доверия пользователей к облачным сервисам. В условиях быстрого роста объемов данных и увеличения киберугроз эффективная защита данных становится ключевым элементом успешного функционирования облачных решений. Организации должны быть готовы адаптироваться к изменяющимся угрозам и постоянно улучшать свои стратегии защиты данных.

Список использованных источников

1. Самокиш А.В. (2017) Облачные технологии. *Экономика и социум*. 1–4.
2. Никульчев Е.В., Лукьянчиков О.И., Ильин Д.Ю. (2019) *Облачные технологии*. Москва, Издательство «РТУ МИРЭА».
3. Иванов П.В. (2025) *Менеджмент: методы принятия управленческих решений*. Москва, Издательство «Юрайт».
4. Исаев Е.А., Думский Д.В., Самодуров В.А., Корнилов В.В. (2015) Обеспечение информационной безопасности облачных вычислений. *Математическая биология и биоинформатика.* 571–577.
5. Сафонов В.А. (2024) Исследование уязвимостей и методов защиты данных в облачных информационных хранилищах. *Актуальные исследования*. 1–5.

References

1. Samokish A.V. (2017) Cloud technologies. 1–4 (in Russian).
2. Nikilchev E.V., Lukyanchikov O.I., Iluin D.Yu. (2019) *Cloud technologies.* Moscow, RTU MIREA Publishing House (in Russian).
3. Ivanov P.V. (2025) *Management: methods of making management decisions*. Moscow, Yurait Publishing House (in Russian).
4. Isaev E.A., Dumsky D.V., Samodurov V.A., Kornilov V.V. (2015) Ensuring information security of cloud computing. *Mathematical biology and bioinformatics*. 571–577 (in Russian).
5. Safonov V.A. (2024) Study of vulnerabilities and methods of data protection in cloud information storages. *Current researches*. 1–5 (in Russian).

Сведения об авторах

Скалозуб К.А., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», seniaskalozub6@gmail.com.
Нестеренков С.Н., канд. техн. наук, доцент кафедры программного обеспечения информационных технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.nesterenkov@bsuir.by.
Бегляк Е.В., магистрант, ассистент кафедры вычислительных методов и программирования, инженер-программист 1 категории отдела сетевых технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», katarina@bsuir.by.

Information about the authors

Skalazub K., Student of the Department of Electronic Computing Machines, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kseniaskalozub6@gmail.com.
Nesterenkov S., Cand. Sc. (Tech.), Associate Professor of the Department of Information Technology Software, Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.nesterenkov@bsuir.by.
Begliak E.V., Master's student, Assistant at the Department of Computational Methods and Programming, 1st category Software Engineer of the Network Technologies Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", katarina@bsuir.by.

УДК 004.934.1

АЛГОРИТМ ПОСТРОЕНИЯ ИНТЕРФЕЙСА ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ДЕФЕКТОВ СЛОВ

В.А. Столер, К.А. Гурин, С.В. Арешко
Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь

Аннотация. Предложен алгоритм построения интерфейса программы для распознавания дефектов слов при их произношении, используемой в устройствах звукового управления электронными устройствами, например в системах информационной безопасности. Рассмотрены способы оптимизации программы и пути повышения точности распознавания речи.
Ключевые слова: обработка звука; дефекты произношения слов; интерфейс программы; алгоритмы обработки.

ALGORITHM FOR CONSTRUCTING A PROGRAM INTERFACE FOR RECOGNITION OF WORD DEFECTS

V.A. Stoler, K.A. Gurin, S.V. Areshko
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. An algorithm for constructing a user interface for a program for recognizing word defects during their pronunciation, used in sound control devices for electronic devices, such as in information security systems. Methods for program optimization and ways to improve speech recognition accuracy are considered.
Keywords: sound processing; pronunciation defects; program interface; processing algorithms.

Введение

Известно множество различных программ распознавания речи, в том числе и автоматическая обработка звука, однако большинство из них являются коммерческими программами. Поскольку коммерческие распознаватели речи доступны для определенных приложений, таких как произношение или транскрипция, то многие проблемы автоматического распознавания речи (ASR) при дефектах речи, в шумной среде, низкое качество записи, еще предстоит решить [1].

Основная часть

В данной статье предложен алгоритм построения программы для распознавания ключевых слов, используемых при голосовом управлении, содержащие дефекты произносимой речи. В терминах цифровой обработки сигналов процесс шумоочистки представляет собой преобразование входного сигнала, содержащего как полезный сигнал – речь, так и аддитивный сигнал-помеха – шум, в выходной сигнал, содержащий только речь. Поскольку создание систем, в точности удовлетворяющих данному условию, является довольно сложной задачей, проблему очистки сигнала от шума приходиться решать следующим образом [2].

Во-первых, необходимо задать погрешность для шума, оставшегося после обработки. Определяем локальные максимумы графика. Интервал M_i, на котором график выходит за пределы заданного значения $\Delta_ш$, имеет локальный максимум и ограничен локальными минимумами, является буквой в слове (рис. 1).

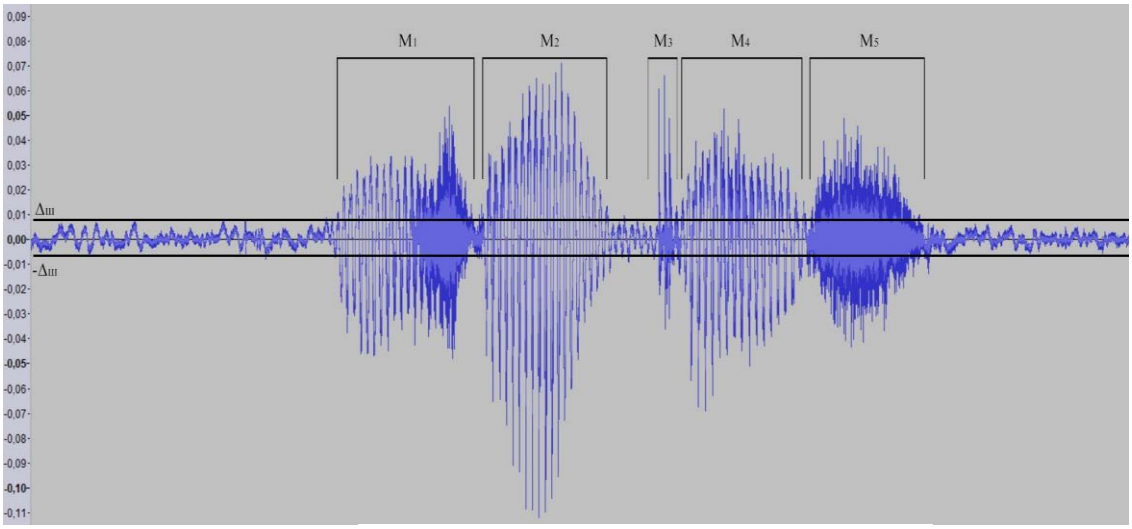


Рис. 1. Выбор интервалов M_i на графике записанной речи
Fig. 1. Selecting *Mi* intervals on the recorded speech graph

Во-вторых, сопоставляем эталонный график и график записанной речи. Выберем количество точек N для сравнения на заданном интервале M_i и зададим погрешность для точек, в пределах сравниваемых интервалов графиков, $\Delta_т$. При этом эталонными считаются графики слов, записанные на профессиональном оборудовании, и содержащие минимальное количество шумов. Данные условия необходимы для минимизации числа ошибок при сравнении слов.

При равенстве точек $[x_j; y_j]$ графика записанной речи точкам $[x_j; y_k]$ эталонного графика с учетом выбранной погрешности $\Delta_т$ можно говорить о равенстве произнесенных букв. Из равенства всех интервалов M_i сравниваемых звуковых сигналов следует равенство произнесенных слов. В результате, обобщенный алгоритм программы для распознавания ключевых слов в записанной речи можно представить следующим образом (рис. 2).

Для оптимизации алгоритма необходимо нормализовать входной сигнал, т. е. задать верхнюю границу значения y. Если разница между минимальным (максимальным) значением y первого графика и минимальным (максимальным) значением y второго графика больше заданной погрешности точки Δт, можно говорить о неравенстве символов, т.е. о неравенстве слов [3].

Для корректного определения M_i необходимо учесть, что значение y локального максимума символа много больше заданного значения погрешности шума $\Delta_ш$. Изменение значений погрешности шума $\Delta_ш$ и погрешности точки $\Delta_т$ позволяет задать необходимую точность сравнения.

При разработке алгоритма учитывались следующие возможные ситуации: количество символов M в записанном слове больше, чем у эталонного; интервал M в записанном слове вмещает в себя большее количество точек N, чем эталон. Бóльшее число символов M в записанном слове может означать не только более длинное слово, но и дефект произношения (например, «Пприве́т»). Для обработки данной ситуации необходимо предусмотреть проверку, в которой у записанного слова будут попарно сравниваться соседние интервалы M_i и M_{i+1}. Если соседние интервалы равны между собой, значит M_i необходимо исключить из сравнения.

Кроме того, необходимо обратить внимание на такую ситуацию, при которой длина интервала M_i в записанном слове больше длины соответствующего интервала M_i в эталонном слове, т.е. количество вмещаемых интервалом точек N различно. Такое различие может возникнуть не только при неравенстве символов, но и при более

длинном произношении буквы (например, «Маамаа»). При систематическом повторении значений y в пределах рассматриваемого интервала, можно говорить о более длинном произношении символа и исключить часть интервала из сравнения для уравнивания значений N.

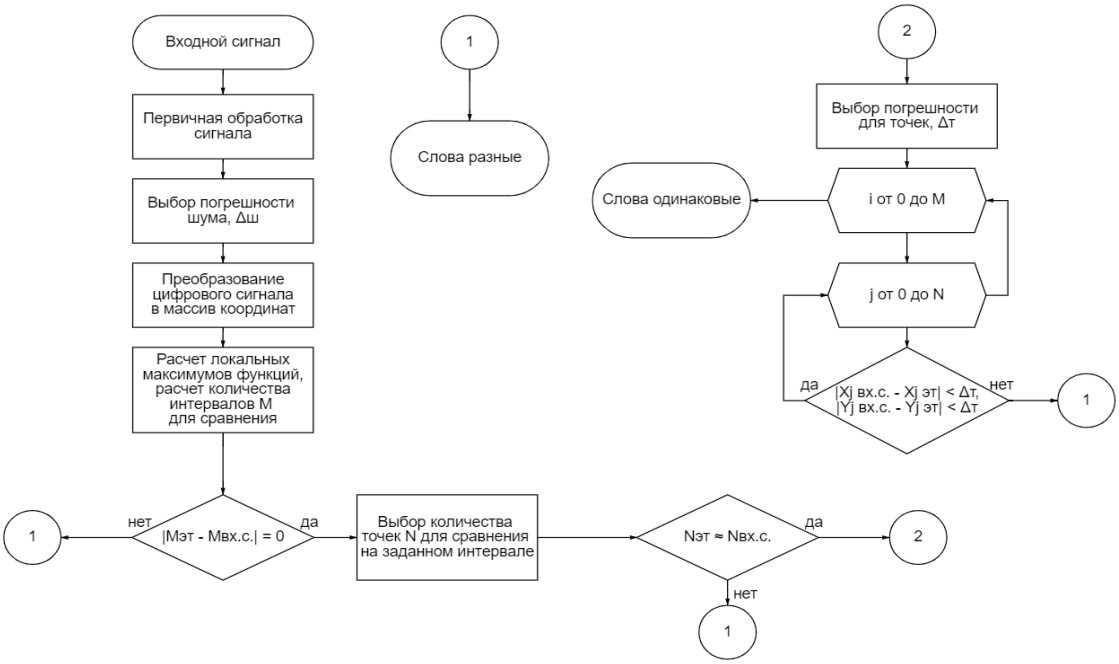


Рис. 2. Алгоритм программы для распознавания ключевых слов
Fig. 2. Algorithm of the program for recognizing keywords

Заключение

В результате исследований был выполнен анализ основных способов взаимодействия пользователя с интерфейсами, используемых в программах распознавания речи. Предложен алгоритм обработки звука, учитывающий дефекты произношения слов, для построения компьютерной программы распознавания речи, используемой в различных программах и системах, например, при звуковом управлении электронными устройствами. Рассмотрены способы оптимизации программы и повышения точности распознавания речи.

Список использованных источников / References

1. Springer Handbook of Speech Processing / Jacob Benesty, M. Mohan Sondhi, Yiteng Arden Huang. – Springer-Verlag Berlin Heidelberg, 2008. – 1161 p.

2. Vishnyakov I.E., Masyagin M.M., Odintsov O.A., Sliusar V.V. Methods and algorithms for real time voice noise cleaning. Proc. Univ. Electronics, 2021, vol. 26, no. 2, pp. 184–196.

3. Jayashree Padmanabhan, Melvin Jose, Johnson Premkumar. Machine Learning in Automatic Speech Recognition: A Survey. Proc. IETE Technical Review, 2015, vol. 32, no. 5, pp. 240–251.

Сведения об авторах

Столер В.А., канд. техн. наук, доц., профессор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stoler@bsuir.by.
Гурин К.А., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Арешко С.В., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Stoler V.A., Ph.D. (Eng.), Assoc. Prof., Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", stoler@bsuir.by.
Gurin K.A., Master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics".
Areshko S.V., Master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics".

УДК 004.056.53

ИМПУЛЬСНО-РЕФЛЕКТОРНЫЙ МЕТОД ОБНАРУЖЕНИЯ ЗАКЛАДНЫХ РАДИОУСТРОЙСТВ

И.С. Сурвило, С.Н. Петров
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Рассматрены современные подходы к обнаружению закладных устройств, используемых для негласного получения информации. Описаны различные методы, основанные на регистрации физических явлений, таких как электромагнитные излучения, тепловые отклонения и гармонические искажения, каждый из которых имеет свои сильные и слабые стороны. Особое внимание уделено импульсно-рефлекторному методу, который выделяется своей универсальностью. Этот метод позволяет обнаруживать как активные, так и пассивные устройства за счет анализа отраженных сигналов и использования резонансных явлений, минимизируя при этом помехи для других систем. Несмотря на определенные ограничения, импульсно-рефлекторный метод рассматривается как перспективное решение для повышения точности и надежности обнаружения закладных устройств в условиях постоянно развивающихся технологий.
Ключевые слова: защита конфиденциальных данных; закладные устройства; обнаружение закладных устройств; электромагнитные излучения; резонансные характеристики; импульсно-рефлекторный метод; пассивные устройства; тепловые отклонения; гармонические искажения; системы защиты информации.

IMPULSE-REFLECTIVE METHOD FOR DETECTING HIDDEN RADIODEVICE

I.S. Survilo, S.N. Petrov
Educational Institution "Belarusian State University of Informatics and Radioelectronics" Minsk, Belarus

Abstract. Modern approaches to detecting embedded devices used for unauthorized access to information were discusses. Various methods based on the registration of physical phenomena such as electromagnetic radiation, thermal deviations and harmonic distortions are described, each of which has its own strengths and weaknesses. Special attention is paid to the pulse-reflex method, which stands out for its versatility. This method makes it possible to detect both active and passive devices by analyzing reflected signals and using resonant phenomena, while minimizing interference to other systems. Despite certain limitations, the pulse-reflex method is considered as a promising solution for improving the accuracy and reliability of detecting embedded devices in conditions of constantly developing technologies.
Keywords: protection of confidential data; covert radio device; detection of covert radio device; electromagnetic radiation; resonant characteristics; impulse reflex method; passive devices; thermal deviations; harmonic distortion; information protection systems.

Введение

В современном мире, где информационные технологии чрезвычайно развиты, защита конфиденциальных данных становится одной из ключевых задач. Утечка информации может привести к серьезным последствиям, включая финансовые потери, репутационный ущерб и даже угрозу национальной безопасности. Одним из наиболее скрытных и опасных способов несанкционированного доступа к информации является использование закладных устройств. Эти устройства, часто миниатюрные и малозаметные, способны перехватывать, записывать и передавать данные на расстоянии, оставаясь незамеченными в течение длительного времени. Закладные устройства могут быть интегрированы в различные объекты инфраструктуры, включая офисные помещения, транспортные средства или бытовую технику. Их обнаружение представляет собой сложную техническую задачу, поскольку такие устройства часто работают в широком диапазоне частот, используют сложные методы модуляции сигналов и могут быть активированы только в определенных условиях. В связи с этим, разработка эффективных методов обнаружения закладных устройств является актуальной задачей в сфере обеспечения безопасности [1].

Основная часть

В условиях постоянного совершенствования элементной базы и структуры закладных устройств, методы их обнаружения также постоянно развиваются. Однако существующие подходы обладают определенными ограничениями и не могут считаться универсальными, что усложняет задачу обнаружения закладных устройств. Данные подходы обладают рядом особенностей, которые важно учитывать.

Линейный метод основывается на регистрации электромагнитных излучений, создаваемых активными электронными компонентами закладных устройств. Основная идея метода заключается в том, что многие электронные устройства, даже в режиме ожидания, могут излучать слабые сигналы в радиочастотном диапазоне, что позволяет их обнаружить с помощью специализированного оборудования. Линейный метод широко используется для поиска активных закладных устройств, работающих на различных радиочастотах. Однако данный метод имеет ряд ограничений. Прежде всего, метод эффективен только для устройств, находящихся в активном режиме и излучающих радиосигналы во время поиска. Если закладное устройство находится в пассивном режиме или использует сложные механизмы маскировки своих сигналов, линейный метод может оказаться недостаточно эффективным. Кроме того, данный метод требует точной настройки оборудования на конкретный диапазон частот, что может усложнить процесс поиска.

Нелинейный метод основан на обнаружении гармонических искажений, возникающих в электронных компонентах закладных устройств под воздействием мощного электромагнитного поля. При облучении таких устройств радиоволнами высокой мощности, полупроводниковые элементы начинают генерировать гармоники на кратных частотах. Именно эти гармоники и фиксируются оборудованием нелинейного радиолокатора, позволяя с высокой точностью обнаружить наличие электронных компонентов. Основное преимущество нелинейного метода заключается в возможности обнаружения закладных устройств, которые находятся в режиме ожидания и не излучают сигналы. Однако метод также имеет свои недостатки. Например, нелинейные радиолокаторы требуют значительной мощности излучения, что может создавать помехи для других электронных систем, находящихся в зоне

действия. Кроме того, работа в микроволновом диапазоне может оказать вредное воздействие на оператора при длительном использовании.

Тепловой метод обнаружения основан на фиксировании тепловых отклонений, возникающих в окружающей среде вследствие работы электронных компонентов закладных устройств. Любое электронное устройство при работе выделяет тепло, и это можно использовать для его обнаружения. Специальные тепловизоры способны фиксировать малейшие изменения температуры в окружающей среде, позволяя выявить активные закладные устройства по тепловым следам их работы. Однако тепловой метод также имеет свои ограничения. Во-первых, он может быть эффективен только в отношении устройств, которые выделяют достаточное количество тепла для регистрации. Во-вторых, тепловой метод требует использования высокочувствительных приборов, что увеличивает стоимость оборудования и сложность его эксплуатации.

Помимо перечисленных методов, существуют и другие подходы, такие как оптические, магнитные и рентгеновские, каждый из которых имеет свои области применения и ограничения. Однако ни один из этих методов не может гарантировать полного обнаружения всех типов закладных устройств, особенно с учетом их постоянного совершенствования и усложнения. Одним перспективных направлений является импульсно-рефлекторный метод, который сочетает в себе преимущества различных подходов и минимизирует их недостатки.

Импульсно-рефлекторный метод основывается на улавливании и анализе отраженных сигналов, возникающих в результате облучения исследуемой области зондирующими импульсами. Этот метод позволяет выявлять активные и пассивные элементы радиоустройств, такие как антенные системы и фильтрующие элементы, благодаря их резонансным характеристикам. Основная идея импульсно-рефлекторного метода заключается в следующем: с помощью специального локатора исследуемое пространство облучается зондирующими импульсами в диапазоне частот, соответствующем возможным рабочим частотам закладных радиоустройств. Эти устройства, как правило, функционируют на фиксированной частоте или в узком диапазоне частот, что делает их уязвимыми для методов, основанных на резонансных явлениях. Антенные системы закладных устройств обычно имеют высокую добротность – параметр, характеризующий способность контура эффективно накапливать и отдавать энергию при резонансе. Когда устройство с высокодобротным контуром облучается зондирующим сигналом с частотой, равной резонансной частоте контура, амплитуда наведенных в контуре токов резко возрастает. Это приводит к значительному увеличению мощности отраженного сигнала, принимаемого локатором [2].

Данный метод особенно эффективен при работе с закладными устройствами, чьи антенные системы работают в узком диапазоне частот и обладают выраженными резонансными характеристиками. В случае облучения устройств зондирующим сигналом на резонансной частоте происходит значительное усиление отклика, что позволяет надежно обнаруживать закладные устройства на фоне естественного электромагнитного шума и других помех.

Таким образом импульсно-рефлекторный метод обладает рядом ключевых преимуществ, которые делают его более эффективным и универсальным по сравнению с традиционными методами обнаружения закладных устройств:

– высокая чувствительность к резонансным элементам: антенные системы и другие высокодобротные компоненты закладных устройств создают четко выраженные резонансные отклики, которые легко обнаруживаются с помощью данного

метода. Это особенно важно при работе с устройствами, скрытыми в конструкциях или оборудовании;

– обнаружение устройств, работающих в пассивном режиме: в отличие от методов, требующих активного излучения от закладного устройства, импульсно-рефлекторный метод позволяет выявлять даже пассивные элементы, такие как антенные системы, которые не излучают сигналы, но откликаются на зондирующее воздействие;

– независимость результата от излучаемой мощности закладных устройств;

– низкая средняя мощность зондирующих сигналов позволяет минимизировать воздействие на окружающие системы связи и другое радиоэлектронное оборудование.

Несмотря на значительные преимущества, импульсно-рефлекторный метод не лишен недостатков. Одним из них является зависимость от наличия резонансных контуров в закладных устройствах. Если устройство использует нерезонансные схемы или имеет специальную экранировку, сигнал может быть ослаблен до такой степени, что его обнаружение станет затруднительным.

Реализация устройства, работающего на импульсно-рефлекторном методе, требует учета ряда особенностей, которые обеспечивают его эффективность и надежность. Центральным элементом системы является генератор, который создает короткие импульсы с заданной частотой и мощностью. В качестве зондирующего сигнала целесообразно использовать короткие импульсы с определенным периодом повторения [3]. Короткие импульсы позволяют достичь высокой пиковой мощности при относительно низкой средней мощности, что минимизирует энергопотребление. Кроме того, короткие импульсы обеспечивают высокую временную разрешающую способность.

Передающая антенна излучает зондирующие импульсы в окружающее пространство. Ее конструкция и характеристики должны обеспечивать эффективное распространение сигнала в заданном диапазоне частот. Антенна должна быть направленной, чтобы минимизировать рассеивание энергии и увеличить дальность действия системы. Приемная антенна должна обладать высокой чувствительностью, чтобы улавливать слабые отраженные сигналы, включая вторичное излучение от закладных устройств.

Полученные сигналы обрабатываются с использованием оптимальных алгоритмов. Это позволяет выделить характерные признаки отраженных сигналов, такие как резонансные частоты и амплитудные всплески, которые свидетельствуют о наличии закладного устройства.

Таким образом импульсно-рефлекторный метод предоставляет значительные возможности для улучшения систем обнаружения закладных устройств. Его использование позволяет объединить передовые технологии обработки сигналов и подходы к их передаче, создавая потенциал для повышения точности, дальности и надежности обнаружения, что делает данный метод перспективным для дальнейшего развития и применения в системах защиты информации.

Заключение

Существующие подходы к обнаружению закладных устройств имеют свои особенности и не всегда обеспечивают универсальное решение. Импульсно-рефлекторный метод, основанный на анализе отраженных сигналов и использовании резонансных явлений, предлагает более гибкий и универсальный подход. Он позволяет обнаруживать как активные, так и пассивные устройства, не создавая значительных помех для других систем. Однако его эффективность зависит от наличия резонансных

контуров в закладных устройствах, что в некоторых случаях может снизить его применимость.

Список использованных источников

1. Куприянов А. И., Петренко П. Б., Сычев М. П. (2010) *Теоретические основы радиоэлектронной разведки: учебное пособие*. Москва, МГТУ им. Баумана.

2. Буневич М. А., Майоров А. И., Врублевский И. А. (2022) Применение SDR-приемопередатчиков в системах для поиска закладных радиоустройств. *Цифровая трансформация*. 28 (4), 62-71.

3. Ворошень А. В., Ворошень В. И. (2015) Функциональные особенности резонансно-рефлектометрического локатора для обнаружения радиозакладных устройств. *Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации»*. С 13-14.

References

1. Kupriyanov A. I., Petrenko P. B., Sychev M. P. (2010) *Theoretical Foundations of Electronic Intelligence: Textbook*. Moscow, Bauman Moscow State Technical University (in Russian).

2. Bunevich M. A., Mayorov A. I., Vrublevsky I. A. (2022) The Use of SDR Transceivers in Systems for Searching Covert Radiodevices. *Digital Transformation*. 28 (4), 62–71 (in Russian).

3. Voroshen A. V., Voroshen V. I. (2015) Functional Features of Resonance-Reflectometric Locator for Detection of Radio Bugs. *Proceedings of the XIII Belarusian-Russian Scientific and Technical Conference "Technical Means of Information Protection"*. P 13–14 (in Russian).

Сведения об авторах

Сурвило И.С., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ilya_survilo@mail.ru.
Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.

Information about the authors

Survilo I.S., Master's student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ilya_survilo@mail.ru.
Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by.

УДК 004.056:336.71(076)

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СЕМАНТИЧЕСКИХ ИЗМЕНЕНИЙ ОБЕЗЛИЧЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

А.М. Тимофеев[1], К.Р. Восковцева[2], Я.А. Клиндухов[2]
[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь
[2]Учреждение образования «Национальный детский технопарк», Минск, Беларусь

Аннотация. Предложены принципы реализации метода изменения состава или семантики, заключающиеся в использовании наборов различных доверительных вычислительных баз (ДВБ). Такие принципы соответствуют требованиям законодательства Республики Беларусь в сфере защиты информации и могут быть использованы при проектировании, создании и эксплуатации (модернизации) современных информационных систем, посредством которых осуществляется автоматизированная обработка биометрических, генетических либо специальных персональных данных. Выполнены исследования влияния семантических изменений обезличенных персональных данных на их информационную безопасность, и получена зависимость вероятностей появления обезличенных символов персональных данных от их номеров, содержащихся в ДВБ. Установлено, что с ростом количества ДВБ и с увеличением количества исходных и соответствующих им обезличенных персональных данных, содержащихся в каждой такой ДВБ, отклонение вероятности появления исходных

персональных данных от вероятности появления обезличенных персональных данных проявляется в бóльшей мере.
Ключевые слова: информационные системы; персональные данные; защита информации; деобезличивание персональных данных; методы обезличивания персональных данных; метод изменения состава или семантики.

STUDY OF THE IMPACT OF SEMANTIC CHANGES OF DEPERSONALIZED PERSONAL DATA ON THEIR INFORMATION SECURITY

[1]A. Timofeev, [2]K. Voskovtseva, [2]Y. Klindukhov
[1]Education Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus
[2]Education Institution "National Children's Technopark", Minsk, Belarus

Abstract. The principles of implementing the method of changing the composition or semantics are proposed. These principles consist in using sets of different trusted computing bases (TCB). This approach complies with the legislation of the Republic of Belarus in the field of information security. The implementation of the method of changing the composition or semantics can be used in the design, creation and operation (modernization) of modern information systems that are used for automated processing of biometric, genetic or special personal data. The influence of semantic changes in depersonalized personal data on their information security has been studied. The dependence of the probabilities of occurrence of depersonalized symbols of personal data on their numbers contained in the TCB has been obtained. It has been established that with an increase in the number of TCBs and with an increase in the number of original and corresponding depersonalized personal data contained in each such TCB, the deviation of the probability of occurrence of the original personal data from the probability of occurrence of depersonalized personal data manifests itself to a greater extent.
Keywords: information systems; personal data; information security; depersonalization of personal data; methods of depersonalization of personal data; method of changing the composition or semantics.

Введение

В настоящее время одной из наиболее важной задач, решаемых при построении информационных систем типовых классов, является обеспечение их информационной безопасности [1–3]. При этом важно учитывать наличие в таких системах любых персональных данных, кроме общедоступных.

Персональными данными называют любую информацию, относящуюся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Под общедоступными персональными данными будем понимать персональные данные, распространенные либо самим субъектом персональных данных, либо с его согласия или распространенные в соответствии с требованиями законодательных актов Республики Беларусь.

В соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации для обеспечения информационной безопасности персональных данных выполняют их обезличивание с использованием методов, определенных в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. №259 «Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66». Процедура обезличивания персональных данных подразумевает действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Субъект персональных данных – это физическое лицо, в отношении которого осуществляется обработка персональных данных

Одним из таких методов является метод изменения состава или семантики, сущность которого заключается в том, что выполняют обобщение, изменение или удаление части сведений, позволяющих идентифицировать субъекта персональных данных. При этом полученные обезличенные персональные данные и правила их изменения необходимо хранить раздельно.

Отметим, что в случае обобщения или удаления части исходных персональных данных при реализации процедуры их обезличивания не выполняется свойство полноты обезличенных персональных данных. Это не позволит выполнить деобезличивание персональных данных без использования соответствующих таблиц. Применение указанных таблиц создает уязвимость информационных систем, что является недостатком метода изменения состава или семантики. От этого недостатка свободные методы [4], которые предусматривают дополнительно изменение семантики обезличенных персональных данных по отношению к семантике исходных персональных данных. Однако указанная замена сохраняет статистику естественного языка, что может быть использовано нарушителем для доступа к исходным персональным данным и реализовано на основе методов частотного анализа [5]. В связи с этим целью данной работы являлась реализация семантических изменений исходных персональных данных для решения задач их обезличивания, при которых статистические распределения вероятностей появления отдельных обезличенных символов не соответствуют статистическим распределениям вероятностей появления символов исходных персональных данных.

Объектом исследования являлся метод изменения состава, применяемый для обезличивания персональных данных. Этот метод выбран в качестве объекта исследования, поскольку он является одним из обязательных методов обезличивания персональных данных для организаций и предприятий, в которых осуществляется обработка биометрических, генетических либо специальных персональных данных с использованием типовых информационных систем в соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации.

Предметом исследования являлось применение набора доверительных вычислительных баз для реализации обезличивания персональных данных на основе метода изменения состава или семантики, при котором статистические распределения вероятностей появления отдельных обезличенных символов не соответствуют статистическим распределениям вероятностей появления символов исходных персональных данных.

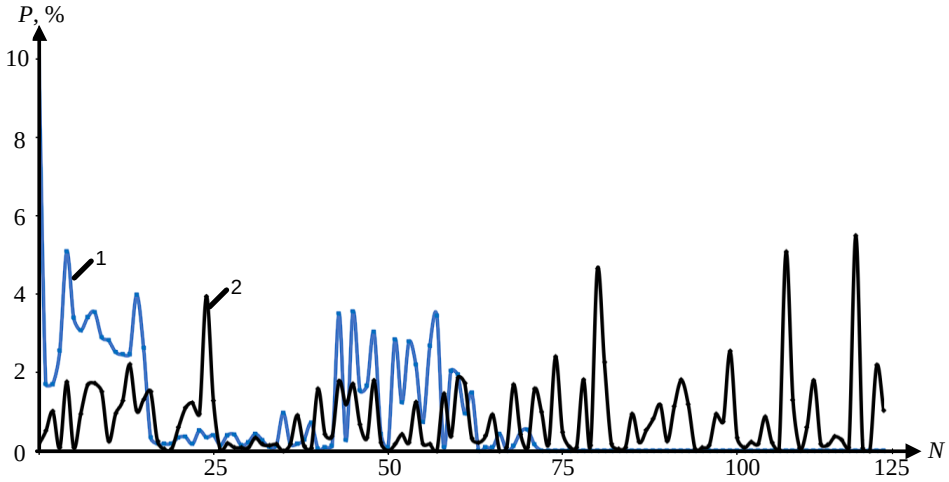
Обезличивание персональных данных с использованием блочной замены и набора различных ДВБ

В рамках данной работы предложена реализация метода изменения состава или семантики, которая заключается в следующем. Персональные данные, подлежащие обезличиванию, вначале разбивают на блоки длинной n символов каждый. В случае если общее число символов не кратно n, то последний блок дополняют символами пробела. Затем формируют n-ое количество доверительных вычислительных баз, которые представляют собой перестановочные таблицы, являются ключевыми элементами информационных систем и хранятся защищенным образом отдельно от исходных и обезличенных персональных данных. После этого первый символ первого блока исходных персональных данных заменяют на обезличенный символ из первой ДВБ, второй символ – из второй ДВБ и т.д. Последний символ первого блока исходных персональных данных заменяют на обезличенный символ из n-ой ДВБ. Второй

и последующий блоки исходных персональных данных обезличивают аналогичным образом с использованием ДВБ 1 ÷ *n* соответственно.

Отметим, что целесообразно устанавливать общее количество записей, содержащихся в каждой ДВБ, исходя из требований информационной безопасности, которые определяют собственники информационных систем либо до начала проектирования информационных систем, либо на этапе их эксплуатации (модернизации).

Выполнены исследования влияния семантических изменений обезличенных персональных данных на их информационную безопасность, и получена зависимость вероятностей появления обезличенных символов персональных данных от их номеров, содержащихся в ДВБ, которая представлена на рисунке.



Зависимость вероятности появления обезличенных
символов персональных данных от их номера из ДВБ.
Реализация метода состава или семантики с использованием:
1 – простой замены на базе одной ДВБ; 2 – сложной замены на базе двух ДВБ

Важно отметить, что представленные на рис. результаты получены с использованием двух ДВБ, каждая из которых имеет 780 записей исходных и соответствующих им символов обезличенных персональных данных.

Из приведенных результатов видно, что вероятности появления символов исходных персональных данных в случае использования сложной замены на базе двух ДВБ не соответствуют вероятностям появления обезличенных символов, что наблюдалось при использовании простой замены на базе одной ДВБ. Это позволяет повысить уровень информационной безопасности персональных данных с использованием их обезличивания на основе метода изменения состава или семантики при выполнении сложной замены на базе набора ДВБ за счет того, что частотный анализ обезличенных символов усложняется, в сравнении с частотным анализом символов, обезличенных на базе одной ДВБ.

Выполненная оценка показала, что с ростом количества ДВБ и с увеличением количества исходных и соответствующих им обезличенных персональных данных, содержащихся в каждой такой ДВБ, отклонение вероятности появления исходных персональных данных от вероятности появления обезличенных персональных данных проявляется в бóльшей мере.

Предложенные в данной работе принципы обезличивания персональных данных соответствуют требованиям законодательства Республики Беларусь в сфере защиты информации, реализованы на базе программной платформы Windows Forms на языке программирования высокого уровня C#12 (.NET Framework 4.8) и выполнены в виде

исследовательского проекта учреждения образования «Национальный детский технопарк». Для проведения исследований использовалась специально сгенерированная база исходных персональных данных, полученная с помощью генератора псевдослучайных данных, который выполнен программно (любые совпадения с персональными данными реальных физических лиц случайны; авторы работы и издательство не несут ответственности и не предоставляют гарантий в связи с публикацией в настоящей статье любой информации, относящейся к реальному физическому лицу). Так, например, запись исходных персональных данных №5034 «Сидоров Александр Андреевич» после реализации обезличивания с использованием предложенных в настоящей работе принципов имеет вид «ɛœãн′ϑÚPɼĠøÐøUÚã′Ĥ<Ú ħ′aœŪaɛ».

Важно отметить, что представленные в данной работе принципы обезличивания персональных данных не требуют больших вычислительных ресурсов от современных аппаратно-программных комплексов и характеризуются высоким уровнем информационной безопасности, достаточным для решения практических задач по обезличиванию персональных данных.

Заключение

Предложены принципы реализации метода изменения состава или семантики, позволяющие повысить уровень информационной безопасности информационных систем, в которых обрабатываются персональные данные, за счет использования наборов различных доверительных вычислительных баз. Эти принципы соответствуют требованиям законодательства Республики Беларусь в сфере защиты информации и могут быть использованы при проектировании, создании и эксплуатации (модернизации) современных информационных систем, в частности, для информационных систем типовых классов.

Применение наборов различных доверительных вычислительных баз для решения задач обезличивания персональных данных на основе метода изменения состава или семантики позволило сохранить вычислительную сложность указанного метода и при этом повысить уровень информационной безопасности обезличенных персональных данных за счет усложнения процедуры частотного анализа, который может быть применен возможным нарушителем информационной безопасности.

Список использованных источников

1. Ворона, В. А. (2023) *Биометрическая идентификация личности.* Москва, Горячая линия-Телеком.
2. Коллинз, М. (2020) *Защита сетей. Подход на основе анализа данных.* Москва, ДМК Пресс.
3. Остапенко, Г. А. (2020) *Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия.* Москва, Горячая линия-Телеком.
4. Солдатова В. И. (2020) Защита персональных данных в условиях применения цифровых технологий. *Lex russica*. (2), 33–43.
5. Арьков, В. Ю. (2023) *Частотный анализ числовых и текстовых данных*. Екатеринбург, Издательские решения.

References

1. Vorona V. A. (2023) *Biometric Identification of Personality*. Moscow, Goryachaya Liniya-Telecom (in Russian).
2. Collins M. (2020) *A Data-Based Approach*. Moscow, DMK Press (in Russian).
3. Ostapenko G. A. (2020) *Information Operations and Attacks in Socio-Technical Systems: Organizational and Legal Aspects of Counteraction*. Moscow, DMK Press (in Russian).

4. Soldatova V. I. (2020) Protection of Personal Data in the Context of Digital Technologies. *Lex russica*. (2), 33–43 (in Russian).
5. Arkov V. Yu. (2023) *Frequency Analysis of Numerical and Text Data*. Ekaterinburg, Publishing Solutions (in Russian).

Сведения об авторах

Тимофеев А.М., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», tamvks@mail.ru.
Восковцева К.Р., учащаяся, учреждение образования «Национальный детский технопарк», kristiza2009@gmail.com.
Клиндухов Я. А., учащийся, учреждение образования «Национальный детский технопарк», klinyarik1@gmail.com.

Information about the authors

Timofeev A., Cand. Sci. (Tech.), Assosiate Professor, Associate Professor of the Department of Information Protection, Educational Institution "Belarusian State University of Informatics and Radioelectronics", tamvks@mail.ru.
Voskovtseva K., Student, Educational Institution "National Children's Technopark", kristiza2009@gmail.com.
Klindukhov Y., Student, Educational Institution "National Children's Technopark", klinyarik1@gmail.com.

УДК 004.056:336.71(076)

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ВВЕДЕНИЯ ИДЕНТИФИКАТОРОВ

А.М. Тимофеев[1], М.А. Тавгень[2], А.С. Янковец[2]
[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь
[2]Учреждение образования «Национальный детский технопарк», Минск, Беларусь

Аннотация. Применительно к информационным системам, в которых осуществляется автоматизированная обработка персональных данных с обеспечением информационной безопасности персональных данных за счет реализации методов их обезличивания, разработаны структурные схемы блоков обезличивания и деобезличивания персональных данных. Предложенные в работе схемы построены на базе симметричного блочного алгоритма ГОСТ 28147-89, являющегося одним из обязательных алгоритмов криптографического преобразования данных в соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации. Особенности построения и функционирования разработанных схем характеризуются применением криптографических и криптоподобных операций, не требующих знания таблиц соответствия при выполнении процедуры деобезличивания персональных данных, что упрощает реализацию системы защиты информации, по сравнению с существующими схемами.
Ключевые слова: информационные системы; персональные данные; защита информации; обезличивание персональных данных; методы обезличивания персональных данных; метод введения идентификаторов.

DEPERSONALIZATION OF PERSONAL DATA BASED ON THE METHOD OF INTRODUCING IDENTIFIERS

[1]A. Timofeev, [2]M. Tavgen, [2]A Yankovets
[1]Education Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus
[2] Education Institution "National Children's Technopark", Minsk, Belarus

Abstract. Structural diagrams of personal data depersonalization and depersonalization blocks have been developed. They can be used in information systems that perform automated processing of personal data while ensuring their information security based on depersonalization methods. The circuits are based on the symmetric block algorithms of GOST 28147-89. This standard is one of the mandatory algorithms for cryptographic data transformation in accordance with the requirements of the legislation of the Republic of Belarus in the field of information security. The basic principles of construction and operation of the developed diagrams are

described. They are characterized by the use of cryptographic and crypto-like operations that do not require knowledge of correspondence tables when performing the procedure of depersonalization of personal data. This simplifies the implementation of the information security system, compared to existing diagrams.
Keywords: information systems; personal data; information protection; depersonalization of personal data; methods of depersonalization of personal data; method of introducing identifiers.

Введение

Весьма важной задачей в сфере защиты информации является обеспечение информационной безопасности персональных данных, к которым относят любую информацию об идентифицированном физическом лице или физическом лице, которое может быть идентифицировано [1–3].

Под физическим лицом, которое может быть идентифицировано, понимают физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

В соответствии с требованиями законодательства Республики Беларусь определены методы обезличивания персональных данных, которые предусматривают выполнение таких действий по отношению к персональным данным, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных – физическому лицу, в отношении которого осуществляется обработка персональных данных.

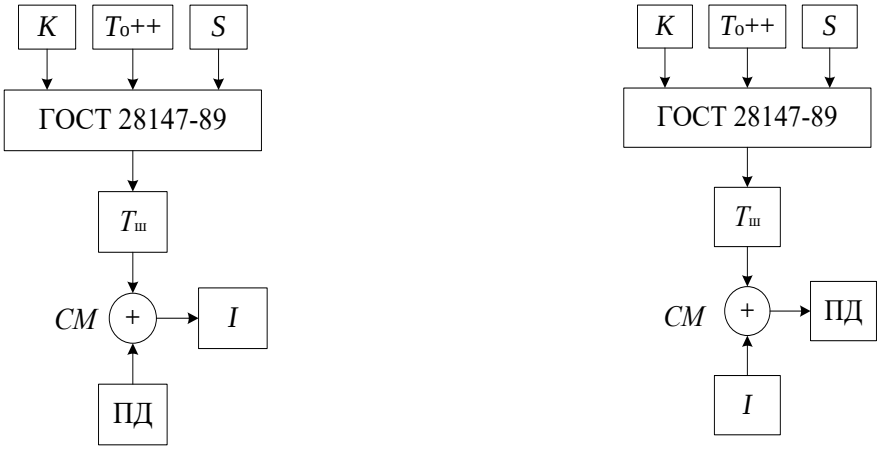
Одним из методов обезличивания персональных данных является метод введения идентификаторов, сущность которого заключается в замене персональных данных или части персональных данных, позволяющих идентифицировать субъекта персональных данных, их идентификаторами и создании таблицы соответствия с последующим раздельным хранением идентификаторов и таблиц. Однако известные реализации процедур обезличивания персональных данных на основе метода введения идентификаторов не позволяют выполнить деобезличивание персональных данных без знания указанных выше таблиц [1–3]. Это усложняет существующие реализации, поскольку таблицы соответствия являются ключевыми компонентами информационных систем и должны сохраняться в секрете. В связи с этим целью данной работы являлось разработать структурные схемы, позволяющие обезличивать и деобезличивать персональные данные на базе метода введения идентификаторов, которые упрощают известные схемы за счет выполнения процедуры деобезличивания персональных данных без знания таблиц соответствия.

Объектом исследования являлся стандарт ГОСТ 28147-89 – блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками. ГОСТ 28147-89 выбран в качестве объекта исследования, поскольку является одним из обязательных стандартов для предприятий и организаций, осуществляющих криптографическую защиту информации в соответствии с требованиями законодательства Республики Беларусь.

Предметом исследования являлось использование ГОСТ 28147-89 в режиме гаммирования для решения задач обезличивания и деобезличивания персональных данных на базе метода введения идентификаторов.

Структурные схемы блоков обезличивания и обезличивания персональных данных

На рисунке приведены структурные схемы блоков обезличивания и обезличивания персональных данных.



a *b*

Структурные схемы блоков обезличивания (a) и деобезличивания (b) персональных данных
Block diagrams of the depersonalization (a) and depersonalization (b) blocks of personal data

Схема блока обезличивания персональных данных функционирует следующим образом (см. часть *a* рисунка). Персональные данные ПД, закодированные на базе кодировочной таблицы UTF-16, разбивают на блоки длиной 64 бита. Затем первый блок ПД длиной 64 бита подают на первый вход сумматора СМ, на второй вход которого поступает первый блок $T_{ш}$ длиной 64 бита, выработанный в соответствии с требованиями, определяемыми ГОСТ 28147-89 в режиме гаммирования с использованием секретного криптографического ключа *K*, блоков открытого текста T_o и синхропосылки *S*. Результат с выхода сумматор СМ образует первый блок идентификатора. Процедуру выработки др. блоков идентификаторов выполняют аналогичным образом, за исключением того, что для каждого последующего идентификатора предыдущий блок T_o инкрементируют. Полученные таким образом блоки идентификаторов конкатенируют в общую последовательность, являющуюся выработанным идентификатором.

Отметим, что в качестве блочного шифра может быть использован любой другой алгоритм блочного типа, например, AES, СТБ 34.101.31-2020 и пр. При этом принципы, изложенные выше, останутся неизменными. Аналогичным образом кодировочная таблица UTF-16, применяемая в разработанной схеме, может быть заменена на любую другую кодировочную таблицу, обеспечивающую однозначный перевод символов персональных данных в двоичный код. Важно отметить, что алгоритм блочного типа и кодировочная таблица должны быть выбраны однотипными для блоков обезличивания и деобезличивания персональных данных.

Схема блока деобезличивания персональных данных (см. часть *b* рисунка) функционирует схожим образом, как и схема обезличивания персональных данных, за исключением следующего. В схеме деобезличивания персональных данных на первый вход сумматора СМ подают блоки идентификаторов, а на выходе СМ получают двоичную последовательность, которая с помощью кодировочной таблицы UTF-16

преобразуется в блоки персональных данных ПД. Это позволяет, реализовав один пакет программного обеспечения для обезличивания персональных данных, использовать этот же пакет программного обеспечения для деобезличивания персональных данных. Причем при выполнении обезличивания персональных данных входной информацией будут является непосредственно персональные данные, а при деобезличивании – идентификаторы, что упрощает реализацию системы защиты информации.

Важно отметить, что схема деобезличивания персональных данных, предложенная в настоящей работе, не требует использования и обязательного хранения таблиц соответствия, что выгодно отличает данную схему, по сравнению с существующими.

Заключение

При реализации метода введения идентификаторов чрезвычайно важно определить алгоритмы, отдельные параметры алгоритмов и используемые математические вычисления, которые позволят не только преобразовывать персональные данные к виду идентификаторов (обезличивать их), но и вычислительно выполнить обратную процедуру, т.е. на основе идентификаторов рассчитывать персональные данные.

Предложены структурные схемы блоков обезличивания и деобезличивания персональных данных, построенные на базе симметричного блочного шифра ГОСТ 28147-89 в режиме гаммирования. Схема деобезличивания персональных данных не требует хранения и использования таблиц соответствия при осуществлении процедуры деобезличивания, что упрощает ее реализацию, по сравнению с существующими.

Список использованных источников

1. Ворона, В. А. (2023) *Биометрическая идентификация личности.* Москва, Горячая линия-Телеком.
2. Коллинз, М. (2020) *Защита сетей. Подход на основе анализа данных.* Москва, ДМК Пресс.
3. Остапенко, Г. А. (2020) *Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия.* Москва, Горячая линия-Телеком.

References

1. Vorona V. A. (2023) *Biometric Identification of Personality*. Moscow, Goryachaya Liniya-Telecom (in Russian).
2. Collins M. (2020) *A Data-Based Approach*. Moscow, DMK Press (in Russian).
3. Ostapenko G. A. (2020) *Information Operations and Attacks in Socio-Technical Systems: Organizational and Legal Aspects of Counteraction*. Moscow, DMK Press (in Russian).

Сведения об авторах

Тимофеев А.М., канд. техн. наук, доц.,
доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»,
tamvks@mail.ru.
Тавгень М.А, учащийся, учреждение образования «Национальный детский технопарк»,
makdisp2@gmail.com
Янковец А.С., учащийся, учреждение образования «Национальный детский технопарк»,
tomraid3301@gmail.com

Information about the authors

Timofeev A., Cand. Sci. (Tech.), Assosiate Professor, Associate Professor of the Department of Information Protection, Educational Institution "Belarusian State University of Informatics and Radioelectronics",
tamvks@mail.ru.
Tavgen M., Student, Educational Institution "National Children's Technopark",
makdisp2@gmail.com.
Yankovets A., Student, Educational Institution "National Children's Technopark",
tomraid3301@gmail.com.

УДК 621.391.82: 621.3.049.77

АНАЛИЗ ЭЛЕКТРОМАГНИТНОЙ ВОСПРИИМЧИВОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ И ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Н.А.Титович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Проведены экспериментальные исследования и расчеты влияния ВЧ и СВЧ электромагнитных помех на характеристики и параметры p-n-перехода и биполярного транзистора (БТ). Разработанные точные модели воздействия электромагнитных помех на простейшие полупроводниковые приборы (ПП) позволяют значительно снизить затраты по оценке восприимчивости более сложных интегральных схем (ИС) и электронных устройств.
Ключевые слова: полупроводниковые приборы, интегральные схемы; ВЧ и СВЧ помехи; электромагнитная восприимчивость.

ANALYSIS OF ELECTROMAGNETIC SUSCEPTIBILITY OF SEMICONDUCTOR DEVICES AND INTEGRATED MICROCIRCUITS

N. Titovich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Experimental studies and calculations of the influence of high-frequency and microwave electromagnetic interference on the characteristics and parameters of the p-n junction and bipolar transistor (BT) were conducted. The developed accurate models of the impact of electromagnetic interference on the simplest semiconductor devices (SD) allow to significantly reduce the costs of assessing the susceptibility of more complex integrated circuits (IC) and electronic devices.
Keywords: semiconductor devices, integrated circuits; high-frequency and microwave interference; electromagnetic susceptibility.

Введение

Современные подходы к проектированию радиоэлектронной аппаратуры, работающей в сложной помеховой обстановке, предполагают рассмотрение вопросов электромагнитной совместимости (ЭМС) уже на стадии выбора элементной базы. Микросхемы являются сердцем практически любой электронной системы. Благодаря небольшим размерам соединения между элементами ИС малы и поэтому не могут функционировать в качестве эффективных антенн. Поэтому уровни излучаемых ими помех, а также уровни наводок на эти соединения существенно меньше, чем от помех, присутствующих на значительно более длинных проводниках печатных плат, на которых размещены ИС. Основными источниками ЭМП, которые воздействуют на ИС, являются шины питания и заземления, незащищенные сигнальные проводники. Нелинейность активных элементов ИС может привести к детектированию мешающих ВЧ и СВЧ помех. Продукты детектирования могут вызвать как искажение полезных сигналов, так и сдвиги постоянного напряжения и тока в чувствительных узлах ИС, что может вывести ее из правильного режима работы. На практике аналоговые ИС более восприимчивы к электромагнитным воздействиям, чем цифровые, так как они, как правило, не работают с заранее установленными уровнями сигналов, которые предполагают пороговую устойчивость к помехам [1].

К настоящему времени разработаны критерии, методики и специализированная аппаратура для исследования восприимчивости полупроводниковых ПП и ИС к воздействию ВЧ и СВЧ электромагнитных помех (ЭМП). Они позволяют выявить общие тенденции поведения различных элементов при воздействии радиопомех,

накопить определенную справочную информацию. Однако для более детального исследования восприимчивости более сложных ИС проведение натурных экспериментов все более сдерживается их громоздкостью, высокой стоимостью. Именно поэтому уже с 80-х годов исследователи все больше используют расчетный метод [2, 3]. Разработка точных моделей реакции простейших элементов на воздействие ЭМП позволяет в дальнейшем перейти к моделированию сложных схем и получить достоверные результаты, прибегая к натурным экспериментам только для подтверждения полученных в ходе расчетов выводов.

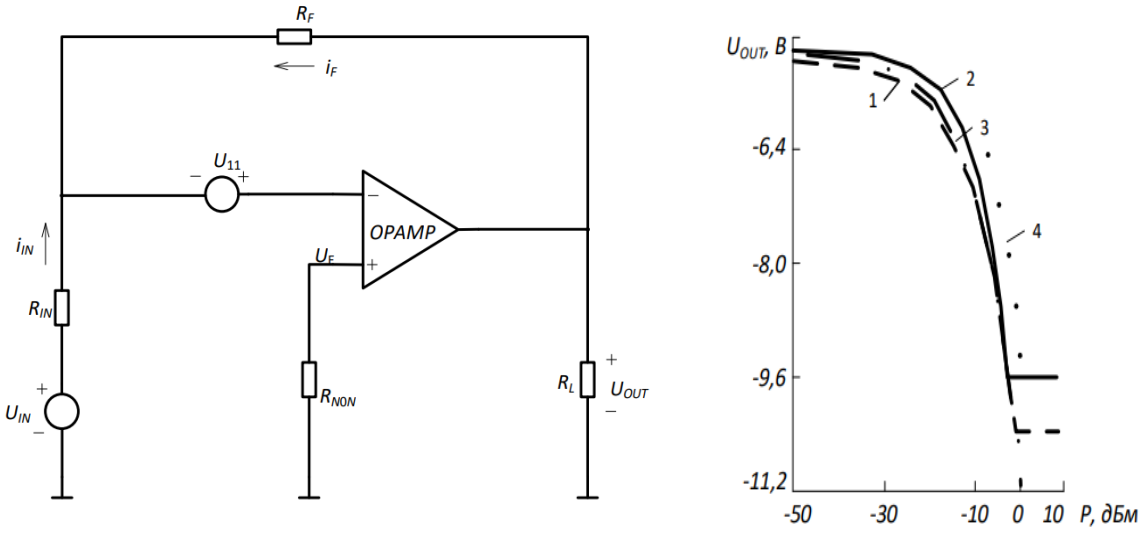
Основная часть

При анализе влияния внеполосных ВЧ и СВЧ ЭМП на работу ИС можно выделить два основных подхода. В основу первого подхода положено использование программы SPICE, предназначенной для описания электрических цепей, расчета во временной и частотной областях и для анализа переходных процессов. Моделирование сложных интегральных схем связано с обработкой больших объемов данных и значительными затратами машинного времени, что вызвано большим количеством элементов схемы. Несмотря на то, что результаты приведенных расчетов достаточно хорошо совпадают с данными экспериментальных исследований, главная трудность такого схемотехнического моделирования микросхем – секретность, т.е. отсутствие в свободном доступе принципиальных электрических схем ИС, тем более с физическими параметрами пассивных и активных элементов. Полной информацией обладают только разработчики ИС [2, 4].

Второй подход предполагает детальное описание входных/выходных цепей ИС и представление внутренней структуры микросхемы, как черный ящик. Упрощенная модель ОУ для анализа воздействия радиопомехи на инверсный вход, представленная на рис.1а, требует минимальных вычислительных затрат [3]. Учет влияния ЭМП на входные цепи усилителя осуществляется введением в цепь прямого или инверсного входа ОУ генератора напряжения смещения U_{11} (рис.1а), который обусловлен детектированием ВЧ помехи в *p-n*-переходах. Величина напряжения генератора зависит от поглощаемой мощности ЭМП P_{RF} и для малых значений амплитуд помехового сигнала составляет $U_{11} = KP_{RF}$, где K – постоянная, зависящая от частоты ЭМП и положения рабочей точки ОУ по постоянному току.

На рис.1б представлены результаты расчетов с помощью макро- , полной и упрощенной моделей, а также экспериментальные зависимости выходного напряжения ОУ от уровня мощности ВЧ помехи с частотой 220 МГц, воздействующей на инверсный вход [2].

Анализ полученных результатов показывает, что точность моделирования с помощью упрощенной модели во многом зависит от точности описания влияния помех на входные, выходные цепи или шины питания и заземления ИС. При этом не требуется полная информация о физических параметрах всех пассивных и активных элементов, как в полной и макромоделях. Достаточно детально учесть параметры элементов расположенных по периферии кристалла ИС, на которые воздействия ЭМП наиболее вероятны.

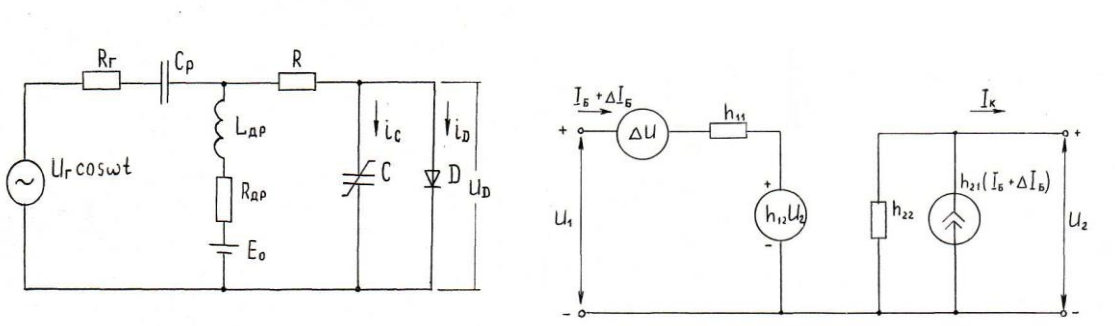


a *b*

Рис. 1. Упрощенная модель ОУ μA741 для анализа восприимчивости при подаче ЭМП на инверсный вход (*a*) и результаты (*b*) экспериментов (4) и расчетов с помощью макро- (1), полной (2) и упрощенной (3) моделей

Fig. 1. Simplified model of the MCA741 op-AMP for the analysis of susceptibility when EMF is applied to the reverse input (*a*) and the results (*b*) of experiments (4) and calculations using macro (1), full (2) and simplified (3) models.

Проведенные исследования показали, что при оценке восприимчивости отдельных ПП и логических элементов (ЛЭ) целесообразно применять метод прямого введения мощности ВЧ и СВЧ помехи в цепь исследуемого элемента [1, 3]. Результаты эксперимента позволяют учесть все особенности влияния ЭМП на ПП и простейшие ИС и отразить это в расчетных моделях. Используя для построения моделей сложных ИС библиотеку простых моделей, можно прибегать к проведению эксперимента только на стадии испытаний законченного блока или устройства, что позволяет значительно сократить затраты времени и средств.



a *b*

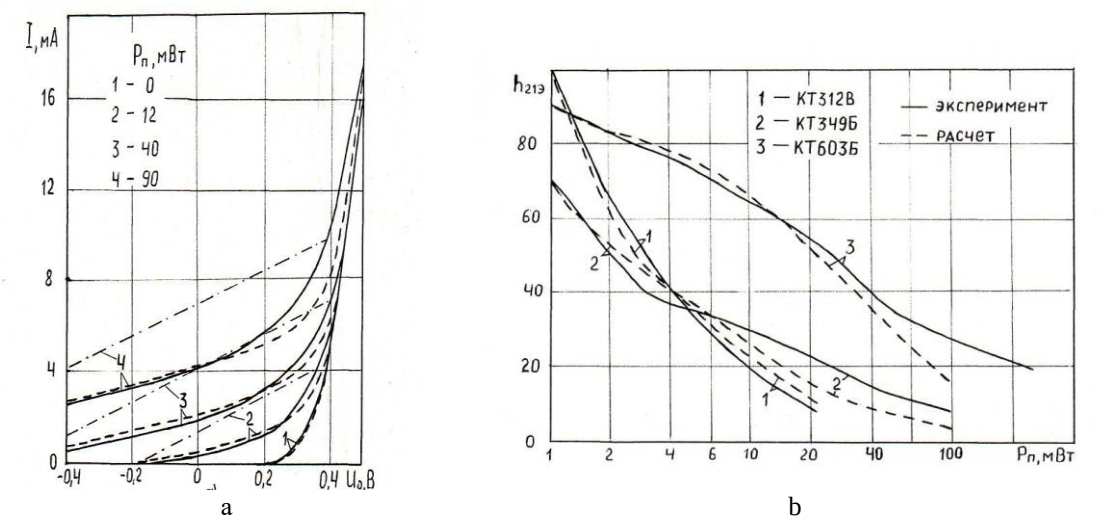
Рис. 2. Эквивалентные схемы *p-n* перехода (а) и биполярного транзистора в схеме с общим эмиттером (*b*), учитывающие воздействие ВЧ помехи

Fig. 2. Equivalent circuits of a p-n junction (*a*) and a bipolar transistor in a circuit with a common emitter (*b*), taking into account the effects of RF interference

Известны несколько моделей, учитывающих воздействие радиопомех на характеристики и параметы *p-n* переходов и транзисторов [2, 4]. Важным условием для их дальнейшего использования при оценке восприимчивости ИС является хорошая корелляция с результатами эксперимента и относительная простота при определении эквивалентных параметров. На рис.2 представлены эквивалентные схемы *p-n*-перехода (а) и биполярного транзистора (б), на которые действует ВЧ помеха, превышающая граничные рабочие частоты ПП. В данном случае $U_Г$ напряжение гармонического помехового сигнала, $R_Г$ – выходное сопротивление генератора помехи, E_0 - напряжение источника смещающего напряжения, $L_{ДР}$ и $R_{ДР}$ – индуктивность и сопротивление ВЧ-дросселя, препятствующего проникновению ВЧ-помех в цепь источника смещения, R и C – последовательное сопротивление и эквивалентная параллельная емкость перехода. При рассмотрении данной модели важно учитывать не только нелинейность *p-n*-перехода, но и нелинейность его диффузионной емкости [2].

На рис. 3, *a* изображены снятые экспериментально и расчитанные с помощью модели (рис. 2, *a*), вольт-амперные характеристики *p-n*-перехода при воздействии ВЧ помех различной мощности.

При расчетах закон изменения емкости перехода представлялся как линейной (штрих-пунктирнае линии), так и экспоненциальной (штриховые) функцией. Из рис. 3, *a* видно, что линеаризация ВАХ, описанная в [3], не позволяет достичь высокой точности, учет же нелинейности емкости дает результаты значительно более близкие к данным эксперимента (сплошные линии). По результатам расчетов (рис. 3, *a*) не сложно определить величины изменения напряжения рабочей точки ΔU и приращения тока ΔI за счет детектирования огибающей ВЧ помехи относительно ВАХ при $P_п$ =0.



a b

Рис. 3. Экспериментальные и расчетные изменения характеристик p-n перехода (*a*) и коэффициента передачи по току биполярных транзисторов (*b*) от уровня поглощенной действием ЭМП с частотой 400 МГц

Fig. 3. Experimental and calculated changes in the characteristics of the p-n junction (*a*) and the current transfer coefficient of bipolar transistors (*b*) from the level of absorption by the action of EMF with a frequency of 400 MHz

В эквивалентную схему биполярного транзистора (БТ) (рис.2б), представленную в системе *h*-параметров, введены дополнительный источник напряжения ΔU и увеличение выходноготока на величину ΔI, обусловленные детектированием огибающей радиопомехи на эмиттерном переходе транзистора, которые можно

определить по изменению ВАХ *p-n*-перехода. При оценке восприимчивости транзисторов изменения ВАХ сравнивать неудобно. Поэтому для БТ в качестве обобщенного критерия удобнее всего выбрать степень снижения коэффициента передачи по току $h_{21э}$, которую можно рассчитать с помощью выражения:

$$h_{21э} = h_{21э0}/(1 + qP_п((R_б A_э/(2\pi f_п C_п))^{1/2}/(2kTP_э I_{бн}(R_б+(1+h_{21э0})R_э)), \quad (1)$$

где $h_{21э0}$ – значение коэффициента передачи при $P_п = 0$; $R_э$ и $R_б$ – сопротивления эмиттера и базы БТ; $I_{бн}$ – ток базы в режиме насыщения; $P_п$, $f_п$ – мощность и частота воздействующей ЭМП; $P_э$ – периметр эмиттера; $A_э$ – площадь перехода Э-Б; $C_п$ – емкость перехода Э-Б; kT/q =0,026 В.

На рис. 3, *b* представлены рассчитанные и экспериментальные зависимости изменения $h_{21э}$ от уровня воздействующих помех [4]. Результаты расчетов и экспериментов для нескольких типов БТ достаточно хорошо совпадают. Это позволяет использовать предложенную модель *p-n*-перехода (рис.2а) для определения величины дополнительного напряжения смещения U_{11} в схеме ОУ (рис. 1, *а*). Установлено, что менее восприимчивыми являются БТ с большим периметром эмиттера $P_э$, т. е. имеющие встречно-штыревую конструкцию эмиттерного перехода. Более восприимчивы к воздействию радиопомех чувствительные схемы ОУ, маломощные БТ, быстродействующие ИС. Восприимчивость ПП и ИС снижается с увеличением частоты воздействующих помех.

Заключение

Измерения и расчеты влияния ВЧ и СВЧ помех на различные типы диодов, транзисторов и ИС [2, 4] показали, что описанные выше модели достаточно достоверно отражают влияние радиопомех на ВАХ *p-n*-переходов и транзисторов. Это позволяет снизить затраты на проведение натурных испытаний восприимчивости более сложных электронных устройств. Точные модели реакции простейших элементов на воздействие ЭМП позволяют использовать их при моделировании сложных схем.

Список использованных источников

1. Redouté J.-M., Steyaert M. (2010) *EMC of Analog Integrated Circuits, Analog Circuits and Signal Processing.* Springer Science+Business Media B.V. – 248 p.

2. Титович Н.А. Моделирование воздействия радиопомех на логические элементы (2005). *6-й международный симпозиум по электромагнитной совместимости и электромагнитной экологии: материалы симпозиума. 21-24 июня 2005 г.* – Санкт-Петербург. – С. 220–223.

3. Бригидин А.М., Титович Н.А., Кириллов В.М., Юсов Ю.П., Листопад Н.И., Ясюля Г.И. (1992). Влияние электромагнитных помех на работоспособность полупроводниковых приборов и нитегральных схем (обзор). *Электронная техника. Управление качеством.* Вып. 1 (148). С. 3–13.

4. Титович Н.А., Ползунов В.В. (2015) Исследование восприимчивости полупроводниковых приборов к воздействию электромагнитных помех // *Журнал «Доклады БГУИР»*, №1, с.114-118.

References

1. Redouté J.-M., Steyaert M. (2010) *EMC of Analog Integrated Circuits, Analog Circuits and Signal Processing.* Springer Science+Business Media B.V. – 248 p.

2. Titovich N. Modeling the impact of radio interference on logical elements (2005). *6th International Symposium on Electromagnetic Compatibility and Electromagnetic Ecology: Symposium Proceedings. June 21-24, 2005* – St. Petersburg, – P.220-223.

3. Brigidin A., Titovich N., Kirillov V., Yusov Yu., Listopad N., Yasyulya G. (1992). Influence of electromagnetic interference on the performance of semiconductor devices and integral circuits (review). *Electronic engineering. Quality management.* Iss. 1 (148). P. 3–13.

4. Titovich N., Polzunov V. (2015) Study of susceptibility of semiconductor devices to electromagnetic interference // *Journal "Reports of BSUIR",* No. 1, pp. 114-118.

Сведения об авторе

Титович Н.А., канд.техн.наук, доцент, доцент кафедры ИРТ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nikolai.titovich@gmail.com.

Information about the author

Titovich N., PhD, Associate Professor, Associate Professor of the IRT Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nikolai.titovich@gmail.com.

УДК 004.56

СКАНЕР УЯЗВИМОСТИ СЕТИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

М.И. Тихонович
Государственное предприятие «НИИ ТЗИ», Минск, Беларусь

Аннотация. Чтобы выявить уязвимость сети есть множество устройств и подходов. Одним из них является сканер уязвимости сети. Грамотно его используя, специалисты по информационной безопасности могут значительно усилить сетевую безопасность организации. Рассмотрены вопросы, связанные с анализом существующих механизмов поиска уязвимостей. Актуальность данной темы обосновывается возрастающим числом кибератак и инцидентов по утечке данных, которые представляют серьезную угрозу для конфиденциальности и целостности информации. С развитием средств автоматизации проектирования и разработки операционных систем, программного обеспечения и повышения уровня развития технологий злоумышленники все чаще находят «дыры» в корпоративной сети, которые в последствии могут быть использованы для несанкционированного доступа, изменения данных или нарушения нормальной работы локально вычислительной сети организации.
Ключевые слова: сканер; сканер уязвимости; угроза; анализ уязвимостей; корпоративная сеть; уязвимость; оптимизация; сеть; сетевая безопасность; ИТ-инфраструктура.

NETWORK VULNERABILITY SCANNER AS A MEAN OF ENSURING DATA PROTECTION

M.I. Tikhonovich
State Enterprise "NII TZI", Minsk, Belarus

Abstract. To identify network vulnerability there are many devices and approaches. One of them is a network vulnerability scanner. Properly using it, information security specialists can significantly strengthen the network security of the organization. The questions related to the analysis of existing vulnerability scanning mechanisms are considered. The relevance of this topic is justified by the increasing number of cyberattacks and data leakage incidents, which pose a serious threat to the confidentiality and integrity of information. With the development of automation design and development of operating systems, software and increasing the level of technology, attackers are increasingly finding "holes" in the corporate network, which can then be used for unauthorized access, data modification or disruption of the normal operation of the local area network of the organization.
Keywords: scanner; vulnerability scanner; threat; vulnerability analysis; corporate network; vulnerability; optimization; network; network security; IT infrastructure.

Введение

Сканеры уязвимостей – это программные инструменты, предназначенные для поиска слабых мест в информационной инфраструктуре. Они позволяют обнаруживать уязвимости в сетевых ресурсах, операционных системах, приложениях и веб-сервисах, что крайне важно для обеспечения кибербезопасности. Современные сканеры способны анализировать как внутренние, так и внешние угрозы, предоставляя отчеты с детальными рекомендациями по устранению обнаруженных проблем.

Главная задача сканеров уязвимостей – предотвращение потенциальных атак. Они помогают выявить слабые места до того, как злоумышленники смогут их использовать. Использование этих инструментов позволяет поддерживать высокий уровень информационной безопасности, защищая данные компании и пользователей от утечек и несанкционированного доступа. Сканеры автоматизируют процесс поиска уязвимостей, значительно сокращая время на проверку и улучшая точность.

Основная часть

Принцип работы сканеров – проверка используемых операционных систем, приложений, средств защиты информации, поиск «дыр», которыми могли бы воспользоваться хакеры, и предупреждение администратора о зонах риска системы.

Таким образом, сканеры уязвимостей направлены на решение следующих задач:

– идентификация и анализ уязвимостей;

– инвентаризация ресурсов;

– формирование отчетов.

Сканеры уязвимостей сети при своей работе используют два основных механизма: зондирование, сканирование. Зондирование – не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. При зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы». Этот метод более медленный, чем «сканирование», но почти всегда гораздо более точный, чем он. В терминах компании ISS данный метод получил название «подтверждение» (verification). Согласно компании, Cisco этот процесс использует информацию, полученную в процессе сканирования («логического вывода»), для детального анализа каждого сетевого устройства. Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например, подверженность атакам типа «отказ в обслуживании» («denial of service»).

Второй механизм – сканирование – более быстрый, но дает менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения ее наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. Они в дальнейшем сравниваются с таблицей правил определения сетевых устройств, операционных систем и возможных «дыр». После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимости. Этот метод является наиболее быстрым и простым для реализации. В терминах компании ISS данный метод получил название «логический вывод» (inference). Согласно компании, Cisco этот процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта. Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.

На практике указанные механизмы реализуются следующими несколькими методами: «Проверка заголовков» (banner check), «Активные зондирующие проверки» (active probing check), «Имитация атак» (exploit check).

Большинство современных сканеров безопасности сети работает по следующим шагам: сбор информации о сети, обнаружение потенциальных уязвимостей,

подтверждение выбранных уязвимостей, формирование отчетов, автоматическое устранение уязвимостей.

Виды сканирования: WhiteBox – Сканер запускается внутри исследуемой сети, BlackBox – Сканер запускается извне исследуемой сети, Сканер локальной сети – жизненно необходимое средство для компаний, чья деятельность напрямую связана с хранением и обработкой уникальных баз данных, конфиденциальной информации, ценных архивов. Без сомнения, сканеры сети необходимы организациям в сфере обороны и других служб – словом, везде, где нежелательна или даже опасна утечка накопленной информации, имеются базы персональных данных клиентов.

Список использованных источников

1. Крутофал Г. Е. О необходимости применения сканеров уязвимостей для обеспечения информационной безопасности / Г.Е. Крутофал – Текст: электронный // Евразийский научный журнал. – 2022. – №. 4. – URL: https://cyberleninka.ru/article/n/o-neobhodimosti-primeneniya-skanerovuyazvimostey-dlya-obespecheniya-informatsionnoy-bezopasnosti/viewer (дата обращения: 28.02.2025).

2. Долгин А. А. Разработка сканера уязвимостей компьютерных систем на основе защищенных версий ОС Windows / А. А. Долгин, П. Б. Хорев // Труды международной научно-технической конференции «Информационные средства и технологии. – 2005. – URL: https://networkjournal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=7&pa=14&ar=6 (дата обращения: 25.02.2025).

3. Сирсен, Р., Хаббард, Д.У. Как оценить риски в кибербезопасности. Лучшие инструменты и практики / Ричард Сирсен, Дуглас У. Хаббард. – М. : «Бомбора», 2023 – 464 с.

References

1. Krutofal G. E. On the need to use vulnerability scanners to ensure information security / G.E. Krutofal – Text: electronic // Eurasian Scientific Journal. - 2022. - №. 4. - URL: https://cyberleninka.ru/article/n/o-neobhodimosti-primeneniya-skanerovuyazvimostey-dlya-obespecheniya-informatsionnoy-bezopasnosti/viewer (date of reference: 28.02.2025).

2. Dolgin, A. A. A. Development of a vulnerability scanner of computer systems based on protected versions of Windows OS / A. A. Dolgin, P. B. Khorev // Proceedings of the international scientific and technical conference "Information means and technologies. - 2005. - URL: https://networkjournal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=7&pa=14&ar=6 (date of reference: 25.02.2025).

3. Sirsen, R., Hubbard, D.W. How to assess risks in cybersecurity. Best tools and practices / Richard Sirsen, Douglas W. Hubbard. - Moscow : "Bombora", 2023 - 464 p.

Сведения об авторе

Тихонович М.И., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», инженер сектора систем защиты информации Государственного предприятия «НИИ ТЗИ», mtikh@niitzi.by.

Information about the author

Tikhonovich M.I., Master's Student, Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", engineer of the information protection systems sector of the State Enterprise "NII TZI", mtikh@niitzi.by.

УДК 004.56: 537.531

СТРУКТУРА АППАРАТНЫХ СРЕДСТВ ДЛЯ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ С ДИСПЛЕЕВ

И.А. Третьяков, Я.И. Рушечников, А.С. Куликова, В.В. Данилов
Донецкий государственный университет, г. Донецк, Российская Федерация

Аннотация. В настоящей работе показано, что восстановить информацию от некоторых средств вычислительной техники, в частности дисплеев, можно с помощью общедоступных радиоэлектронных средств.
Ключевые слова: электромагнитная совместимость; электромагнитное излучение; наводки электрических сигналов; восстановление информации.

THE STRUCTURE OF HARDWARE FOR RECOVERING INFORMATION FROM DISPLAYS

I.A. Tretiakov, IA.I. Rushechnikov, A.S. Kulikova, V.V. Danilov
Donetsk State University, Donetsk, Russian Federation

Abstract. This paper shows that it is possible to recover information from some computer equipment, in particular displays, using publicly available electronic means.
Keywords: electromagnetic compatibility; electromagnetic radiation; electrical signal interference; information recovery.

Введение

Проблема безопасности излучений и наводок в средствах электронной вычислительной технике известна со времен ее появления [1, 2]. Известно, что информацию, обрабатываемую средствами вычислительной техники, можно восстановить путем анализа электромагнитных излучений и наводок, используя соответствующий ее прием и декодирование [3]. Применение в средствах вычислительной техники импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре из лучений будут компоненты с частотами вплоть до СВЧ.

Основная часть

Для восстановления информации с дисплеев анализ лишь уровня электромагнитного излучения недостаточен, нужно знать еще его структуру. Для дисплеев она соответствует структуре телевизионного сигнала, поэтому в качестве инструмента измерений может использоваться ТВ-приемник. Целью измерений является установление расстояния, на котором информация с экрана дисплея уже не будет воспроизводиться приемником. Для проведения измерений использовалась структура аппаратных средств с диапазоном рабочих частот, более широким в сравнении с обычным ТВ-приемником и повышенной чувствительностью (рис. 1): 1 – исследуемый дисплей; 2 – дипольная антенна; 3 – магнитная рамочная антенна (15...25 кГц); 4 – измерительный приемник; 5 – смеситель; 6 – телевизионный приемник; 7 – формирователь синхросигналов; 8 – сигналы синхронизации (по волоконно-оптической линии); 9 – измеренное расстояние, 10 – сигнал гетеродина.

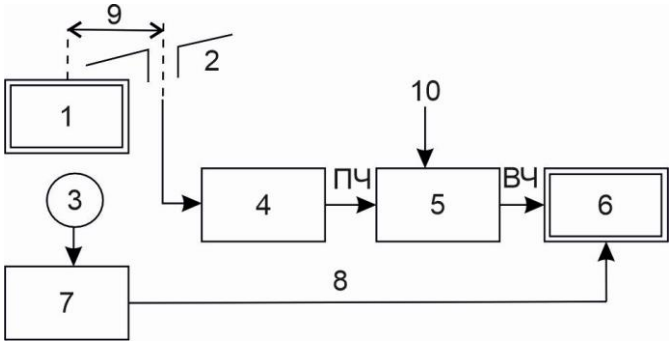


Рис. 1. Структура аппаратных средств измерений
Fig. 1. The structure of measurement hardware

Исследуемый дисплей располагается на высоте 1 м над заземленным металлическим листом, находящимся на полу измерительной площадки. Сигнал от калиброванной антенны подается на вход приемника для измерения в диапазоне 30... 1000 МГц. Сигнал ПЧ измерительного приемника перестройкой частоты преобразуется во входной сигнал ТВ-приемника. Два приемника позволяют не только восстанавливать, но и проводить измерения напряженности электрического поля и сравнивать ее значение с качеством восстановления.

Эксперимент показал, что для качественного восстановления текста на экране телевизионного приемника полоса измерительного приемника должна составлять не менее 4 МГц. При полосе 1 МГц текст становится трудночитаемым, но распознается как текст. Если полоса меньше 1 МГц, изображение на экране приемника с трудом распознается как текст.

В отличие от ситуации реального извлечения информации из излучения при измерениях имеющийся в наличии дисплей позволяет измерять синхросигналы. Строчный синхросигнал получают непосредственно от дисплея, как правило, за счет магнитного поля строчного трансформатора. С помощью магнитной антенны и последующего фильтра выделяется синусоида с частотой 15...20 кГц, которая имеет значительную фазовую нестабильность. Для устранения нестабильности требуется фазовая автоподстройка с большой постоянной времени. Схема формирования импульсов превращает синусоиду в синхроимпульсы строк, последние делением частоты повторения в раз превращаются в синхроимпульсы кадров. Синхроимпульсы поступают на приемник по волоконно-оптическому кабелю для предотвращения их влияния на поле излучения дисплея.

Заключение

Измерения показали, что несмотря на то, что все исследуемые дисплеи удовлетворяют нормам на электромагнитные помехи, с расстояния 50 м можно было получить хорошее изображение информации с экрана дисплея на экране приемника, если дисплей имел пластмассовый корпус. Если корпус металлический, то это расстояние уменьшалось до 10 м. В измерениях использовалась дипольная антенна, замена которой в следующих экспериментах на направленную антенну (трехэлементная, типа «волновой канал»), дает выигрыш порядка 10 дБ. В этом случае указанные расстояния составляют более 300 м, для дисплея в пластмассовом корпусе, 150 м для дисплея в металлическом корпусе.

Список использованных источников

1. Лыньков Л. М., Борботько Т. В., Казека А. А. (2008) Защита от побочного электромагнитного излучения персонального компьютера. *Доклады Белорусского государственного университета информатики и радиоэлектроники*. 5(35), 29-34. EDN YUIMVU.

2. Хорев А. А. (2020) Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютер. *Доклады Томского государственного университета систем управления и радиоэлектроники*. № 2(32), 207-213. EDN SEBGWX.

3. Рушечников Я. И., Яновский А. В., Жинкина А. С., Данилов В. В. (2019) Электромагнитные излучения элементов электронной вычислительной техники. *Вестник Донецкого национального университета. Серия Г: Технические науки*. (2), 25-35. EDN TXLBMK.

References

1. Lynkov L. M., Borbotko T. V., Kazeka A. A. (2008) Zashchita ot pobochnogo elektro-magnitnogo izlucheniia personalnogo kompiutera. *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioelektroniki.* 5(35), 29-34 (in Russian).

2. KHorev A. A. (2020) Otsenka vozmozhnosti obnaruzheniia pobochnykh elektromagnitnykh izluchenii videosistemy kompiuter. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki.* 2(32), 207-213 (in Russian).

3. Rushechnikov IA. I., IAnovskii A. V., ZHinkina A. S., Danilov V. V. (2019) Elektro-magnitnye izlucheniia elementov elektronnoi vychislitelnoi tekhniki. *Vestnik Donetskogo natsionalnogo universiteta. Seriia G: Tekhnicheskie nauki.* (2), 25-35 (in Russian).

Сведения об авторах

Третьяков И.А., канд. техн. наук, доц., доц. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, i.tretiakov@mail.ru.
Рушечников Я.И., ст. преп. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, ya.rushechnikov@donnu.ru.
Куликова А.С., мл. научн. сотр. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, nastya.zhinkina@mail.ru.
Данилов В.В., д-р техн. наук, проц., зав. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, ut5iv@mail.ru.

Information about the authors

Tretiakov I., Cand. Sci. (Tech.), Associate Professor, Associate Professor at Department of Radiophysics and Infocommunication Technologies, Donetsk State University, i.tretiakov@mail.ru.
Rushechnikov IA., Senior Lecturer at Department of Radiophysics and Infocommunication Technologies, Donetsk State University, ya.rushechnikov@donnu.ru.
Kulikova A., Junior Researcher at Department of Radiophysics and Infocommunication Technologies, Donetsk State University, nastya.zhinkina@mail.ru.
Danilov V., Dr. Sci. (Tech.), Professor, Head of the Department of Radiophysics and Infocommunication Technologies, Donetsk State University, ut5iv@mail.ru.

УДК 621.865.8

РАЗРАБОТКА АЛГОРИТМА ОБРАБОТКИ ДАННЫХ С УЛЬТРАЗВУКОВОГО ДАТЧИКА ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ПОЗИЦИОНИРОВАНИЯ МОБИЛЬНОГО РОБОТА

Ж.Р. Уалиев, А.И. Акжолова, Б.А. Талпакова, Д.М. Уйпалакова
Алматинский технологический университет, Алматы, Казахстан

Аннотация. В данной работе рассматриваются методы и алгоритмы обработки данных с ультразвуковых датчиков, используемые для точного позиционирования мобильных роботов. Анализируются существующие подходы, такие как фильтр Калмана [2], SLAM (Simultaneous Localization and Mapping) [3] и методы обнаружения препятствий [4]. Предлагается улучшенный алгоритм, сочетающий вероятностные методы, машинное обучение [5] и методы интеллектуальной фильтрации для повышения

точности навигации в сложных и динамических условиях. Также обсуждаются вопросы оптимизации вычислительных ресурсов и эффективности алгоритмов в реальных условиях эксплуатации.
Ключевые слова: алгоритм; обработка данных; ультразвуковой датчик; позиционирование; мобильный робот; Фильтр Калмана; SLAM (Simultaneous Localization and Mapping); машинное обучение; навигация; фильтрация; навигация.

DEVELOPMENT OF AN ALGORITHM FOR PROCESSING DATA FROM AN ULTRASONIC SENSOR TO IMPROVE THE POSITIONING ACCURACY OF A MOBILE ROBOT

Zh.R. Ualiev, A.I. Akzholova, B.A. Talpakova, D.M. Uypalakova
Almaty Technological University, Almaty, Kazakhstan

Abstract: This paper discusses methods and algorithms for processing data from ultrasonic sensors used for precise positioning of mobile robots. Existing approaches such as the Kalman filter [2], SLAM (Simultaneous Localization and Mapping) [3] and obstacle detection methods [4] are analyzed. An improved algorithm is proposed that combines probabilistic methods, machine learning [5] and intelligent filtering methods to improve navigation accuracy in complex and dynamic conditions. Optimization of computing resources and efficiency of algorithms in real-world operation conditions are also discussed.
Keywords: algorithm; data processing; ultrasonic sensor; positioning; mobile robot; Kalman filter; SLAM (Simultaneous Localization and Mapping); machine learning; navigation; filtering; navigation.

Мобильные роботы используются в различных областях, включая промышленность, медицину, логистику и автономные транспортные системы. Одним из ключевых аспектов их работы является точное позиционирование и навигация в пространстве. Ультразвуковые датчики являются популярными из-за их доступности и энергоэффективности, однако они подвержены ошибкам измерений из-за интерференции, шума и многолучевых отражений.

В последние годы наблюдается развитие комбинированных подходов, включающих использование нескольких типов датчиков (лидаров, инфракрасных сенсоров и IMU) для компенсации недостатков ультразвуковых измерений. В данной статье анализируются существующие методы навигации и предлагается новая методика обработки данных, сочетающая машинное обучение и адаптивные фильтры.

Современные мобильные роботы находят широкое применение в таких областях, как промышленность, сельское хозяйство, медицина, логистика, автономные транспортные системы и поисково-спасательные операции [1]. Важнейшим аспектом их эффективного функционирования является точное позиционирование и навигация в пространстве, что особенно актуально в условиях сложных и динамически изменяющихся сред. Развитие технологий датчиков и алгоритмов обработки информации позволило значительно повысить уровень автономности мобильных платформ. Однако ультразвуковые датчики, широко используемые для измерения расстояний до объектов, подвержены ряду ограничений, включая шумы, многолучевые отражения и интерференцию [2].

Обзор существующих методов:

Фильтр Калмана (Kalman Filter, KF) [3] – применяется для прогнозирования и коррекции данных о местоположении робота. Вариант EKF (Extended Kalman Filter) используется в нелинейных системах, а UKF (Unscented Kalman Filter) – для более точного представления вероятностного распределения.

Фильтр частиц (Particle Filter, PF) [4] – вероятностный метод, позволяющий более точно определять местоположение в условиях неопределенности. Используется в системах, где требуется учет большого количества переменных.

SLAM [5] – метод одновременной локализации и построения карты, использующий сочетание датчиков (ультразвуковые, лидары, IMU и камеры) для формирования точной модели окружающей среды.

Методы обнаружения препятствий [6] – включают обработку данных ультразвуковых датчиков, камер и лидаров, что позволяет более точно определять объекты и оценивать их положение в реальном времени.

Методы машинного обучения [7] – используются для предсказания ошибок измерения, компенсации шумов и улучшения точности восприятия окружающей среды.

Интеграция SLAM и многосенсорных систем

В исследовании [8] рассматривается разработка алгоритма построения карты для мобильного робота на основе данных, поступающих от инфракрасных и ультразвуковых датчиков. Метод SLAM в данной работе комбинируется с фильтрами Калмана и частиц, что позволяет повысить точность позиционирования в условиях ограниченной сенсорной информации. Данный подход особенно эффективен при работе в неизвестных средах, где стандартные методы не дают достаточной точности.

Предложенный алгоритм

Предлагается комбинированный алгоритм, включающий:

– использование усовершенствованного фильтра Калмана [3] для первичной обработки данных с ультразвуковых датчиков, включая адаптивное обновление ошибок измерения;

– применение фильтра частиц [4] для повышения точности позиционирования в сложных условиях, где присутствует высокая степень неопределенности;

– интеграцию SLAM [5] для одновременной локализации и построения карты, что позволяет работать в неизвестных средах;

– использование машинного обучения [7] для предсказания ошибок измерения и их компенсации, а также обнаружения и классификации препятствий;

– внедрение методов интеллектуальной фильтрации данных с использованием нейронных сетей для устранения шумов и многолучевых отражений.

Были проведены симуляционные и практические эксперименты, в которых оценивалась точность позиционирования мобильного робота в различных средах, включая закрытые помещения, сложные промышленные территории и открытые пространства. Результаты показали:

– Снижение средней ошибки позиционирования на 30-40% по сравнению с традиционными методами [4].

– Улучшенную устойчивость к шумам и помехам, возникающим в сложных средах [6].

– Повышенную адаптивность алгоритма к изменяющимся условиям.

Дополнительно были протестированы сценарии работы алгоритма в реальном времени. Использование нейросетей позволило увеличить скорость обработки данных на 15 %, а применение оптимизированных методов фильтрации уменьшило вычислительные затраты на 20% [7].

Применение комбинированного подхода, объединяющего фильтр Калмана [3], фильтр частиц [4], SLAM [5], машинное обучение [7] и интеллектуальную фильтрацию данных, позволяет значительно повысить точность позиционирования мобильного робота. Дальнейшие исследования могут быть направлены на адаптацию алгоритма к динамическим средам, интеграцию дополнительных сенсоров (например, лидаров и камер) и использование глубинного обучения для еще более точного анализа окружающей среды. Кроме того, перспективным направлением является разработка

алгоритмов адаптивной фильтрации, способных эффективно работать в условиях ограниченных вычислительных ресурсов.

Список использованных источников / References

1. Thrun, S., Burgard, W., & Fox, D. (2005). Probabilistic Robotics. MIT Press.
2. Kalman, R. E. (1960). A New Approach to Linear Filtering and Prediction Problems. Journal of Basic Engineering, 82(1), 35-45.
3. Montemerlo, M., Thrun, S., Koller, D., & Wegbreit, B. (2002). FastSLAM: A factored solution to the simultaneous localization and mapping problem. AAAI/IAAI.
4. Grisetti, G., Stachniss, C., & Burgard, W. (2007). Improved Techniques for Grid Mapping with Rao-Blackwellized Particle Filters. IEEE Transactions on Robotics, 23(1), 34-46.
5. Smith, R. C., Self, M., & Cheeseman, P. (1990). Estimating Uncertain Spatial Relationships in Robotics. Autonomous Robot Vehicles, Springer, 167-193.
6. CyberLeninka. Обработка сигналов в системах ультразвуковой локации объектов для закрытых помещений.
7. ArXiv. Online Learning of Wheel Odometry Correction for Mobile Robots with Attention-based Neural Network.
8. Nauchkor. Разработка алгоритма построения карты для мобильного робота на основе данных, поступающих от инфракрасных и ультразвуковых датчиков.
9. Keldysh Institute of Applied Mathematics. Method for Position and Orientation Estimation of Mobile Robot Using Median Filtering.
10. Recent Advances in Deep Learning for Robotic Navigation. ArXiv, 2022.

УДК 621.794.61

ФОРМИРОВАНИЕ И МАГНИТНЫЕ СВОЙСТВА УЛЬТРАДЛИННЫХ НАНОНИТЕЙ НИКЕЛЯ В МЕМБРАНЕ ИЗ ПОРИСТОГО АНОДНОГО ОКСИДА АЛЮМИНИЯ

А.И. Воробьева, Е.А. Уткина
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Высококачественные компактные массивы нанонитей Ni с высоким аспектным отношением (до 700) были получены методом электрохимического осаждения на постоянном токе в мембраны из пористого анодного оксида алюминия. Микроскопические и рентгеноструктурные результаты показали, что нанонити являются однородными, с гладкими стенками и в значительной степени монокристаллическими, ориентированными вдоль 220 направления роста. Магнитные свойства образцов заметно зависят от длины НН, а также от коэффициента упаковки (объемной доли НН в шаблоне). Влияние магнитостатического взаимодействия между длинными нанонитями (аспектное отношение > 500) в образцах с коэффициентом упаковки ≥ 37 % приводит к состоянию перемагничивания, при котором реализуется модель поведения НН по типу "скручивание".
Ключевые слова: Массивы нанонитей; электрохимическое осаждение; оксид алюминия; магнитиная анизотрапия; коэффициент упаковки; аспектное отношение.

FABRICATION AND MAGNETIC PROPERTIES OF THE ULTRA-LONG NICKEL NANOWIRES IN ALUMINA MEMBRANE

A.I. Vorobjova, E.A. Outkina
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. High quality and compact arrays of Ni nanowires with a high aspect ratio (up to 700) were obtained by DC electrochemical deposition into porous anodic alumina membranes. Microscopic and X-ray diffraction results showed that Ni nanowires are homogeneous, with smooth walls and mostly single-crystalline materials with 220-oriented growth direction. The magnetic properties of the samples more depend on the length of the nanowires, as well as on the packing factor (the volume fraction of the nanowires in the membrane). The effect of magnetostatic interaction between ultra-long nanowires (with an aspect ratio of > 500) in samples with a

packing factor of ≥ 37 % leads to a reversal magnetization state, in which a "curling type" model of nanowire behavior is realized.
Keywords: Nanowire arrays; electrochemical deposition; alumina; magnetic anisotropy; packing factor; aspect ratio.

Введение

Разработка микро- и наноразмерных систем, создание композитных наноструктур требуют изучения физико-химических свойств материалов в нанообъемах. Другая сложнейшая задача сегодняшнего дня – разработка надежных методов изготовления наноматериалов и наноструктур. Наиболее перспективные методы основаны на темплатном синтезе и принципах самоорганизации, поскольку они простые и недорогие [1]. Основное внимание исследователей сосредоточено на электрохимическом синтезе нанонитей (НН) и наноструктур на их основе с использованием нанопористых материалов в качестве матрицы.

Самые востребованные для синтеза НН нанопористые материалы, используемые в качестве темплат – это трековые полимеры, двухблочные сополимеры с гексагонально упорядоченными порами и нанопористые оксиды алюминия [2, 3]. Но среди этих материалов только пористый анодный оксид алюминия (ПАОА) устойчив к высоким температурам, не растворим в органических растворителях и его геометрические параметры можно легко регулировать, изменяя условия получения [4, 5].

На механизмы взаимодействия магнитного поля с образцами из квазирегулярных магнитных наноразмерных элементов (наноточек, наностолбиков, нанонитей (нанопроводов)) существенную роль играют коллективные моды квазипериодической структуры ферромагнетика. В ряде работ было показано, что магнитные свойства (коэрцитивность и квадратичность) длинных НН заметно зависят не только от диаметра, но и от длины НН, а также от коэффициента упаковки *P*, (packing factor) объемной доли НН в шаблоне (в ПАОА) [6].

Цель данной работы является разработка простого максимально приближенного к промышленному производству метода изготовления пространственно-упорядоченных массивов НН никеля разной длины с использованием ПАОА; исследование влияния геометрических параметров матрицы и собственно НН на магнитные параметры массива НН в ПАОА.

Методика проведения эксперимента

В данной работе мы использовали мембраны собственного изготовления в специально разработанной установке толстослойного анодирования. В качестве исходного материала использовалась Al фольга (99,995 %) толщиной ~100 мкм, из которой механической резкой формировались подложки размером 60×48 мм. Мембраны ПАОА (МПАОА) толщиной 55, 65, 75 мкм изготавливали методом двухстадийного анодирования фольги в потенциостатическом режиме при напряжении (40 ± 2) В. Тонкий контактный слой металла (Ti) толщиной 450±50 нм осаждали электронно-лучевым распылением, используя установку 01NE-7-004 («Оратория-9»). Более подробно процесс изготовления свободной ПАОА мембраны описан в наших предыдущих работах [7].

Для изготовления массивов НН Ni в МПАОА использовали режим гальваностатического осаждения на постоянном токе. Все эксперименты проводили при комнатной температуре (22±2 °С) при постоянной плотности тока (от 1,0 до 4,0 мА/см^2) и различной продолжительности осаждения в двухэлектродной ячейке. В качестве вспомогательного электрода использовали графитовую пластину. Использовали

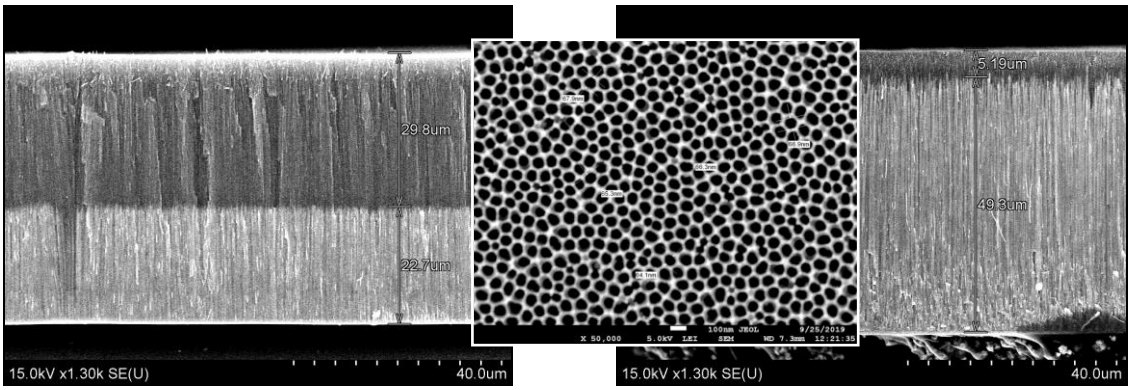
типовой электролит для осаждения тонких пленок никеля следующего состава (в г/л): $NiSO_4 \times 6H_2O$ (140) + $NiCl_2 \times 6H_2O$ (30) + H_3BO_3 (25) + Na_2SO_4 (60).

Топографию поверхности и поперечных сколов образцов исследовали с помощью сканирующей электронной микроскопии (СЭМ – Philips XL 30 S FEG и атомно-силовой микроскопии (АСМ – Nanotop NT-206 («Микротестмашины», Беларусь). Исследования фазового состава экспериментальных образцов проводили методом рентгенодифракционного анализа (XRD – X-ray diffraction) с использованием рентгенофазового дифрактометра ДРОН-2, Cu Kα излучение с длиной волны λ = 0,154056 нм.

Измерения удельной намагниченности образцов (магнитные измерения) при 300 К и 4,2 К проводили магнитометром вибрационного типа (VSM) 7400-S в магнитном поле до 2Т. Магнитные свойства образцов измеряли при направлении поля перпендикулярно и параллельно поверхности образцов. Точность установки поля ±10Г, температуры $\pm 10^{-2}$К.

Результаты и их обсуждение

Для оптимизации параметров процесса осаждения Ni были изготовлены массивы компактных НН Ni с разным аспектным отношением в МПАОА толщины при разных плотностях тока. На рис. 1 показаны СЭМ изображения сколов экспериментальных образцов: НН Ni в порах МРАА толщиной 55 мкм с диаметром пор (70±5) нм.



a *b*

Рис. 1. СЭМ изображения НН Ni в порах ПАОА мембраны толщиной 55 мкм: *a* – НН Ni длиной 23 мкм; *b* – НН Ni длиной 50 мкм. На вставке – СЭМ изображение поверхности мембраны до осаждения НН с обозначениями диаметра пор оксида

Fig. 1. SEM images of Ni NNs in the pores of a 55 μm thick PAO membrane: *a* – Ni NNs 23 μm long; *b* – Ni NNs 50 μm long. The inset shows a SEM image of the membrane surface before NN deposition with the oxide pore diameters indicated.

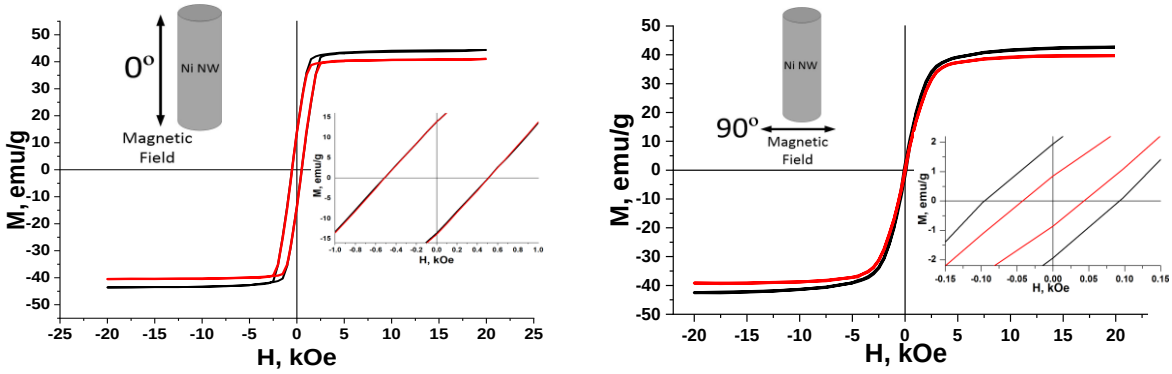
Полученные результаты и данные сканирующей электронной микроскопии (рис. 1) показывают, что качество НН (гладкость, однородность по толщине, непрерывность) зависят от параметров процесса осаждения (плотности тока и времени осаждения, то есть от скорости осаждения), и от совершенства (качества) матрицы. Равномерность процесса осаждения, в первую очередь, зависит от скорости заполнения пор металлом и, частично, от толщины матрицы в данном диапазоне (45–75) мкм.

Результаты рентгеноскопии показали, что преимущественным направлением роста НН Ni в оксиде является направление (220), узкий пик при $2\theta = 75{,}90^{o}$. Это свидетельствует о высокой кристалличности и взаимной (взаимосвязанной) ориентированности кристаллитов вдоль преимущественного направления роста (ось Z

– вертикально вдоль поры). Наличие других слабых пиков при 2θ = 43,82° (200) и при 2θ = 51,27° (111) свидетельствует о присутствии небольшого количества кристаллитов с другим направлением роста. Фазы Ni с ориентациями (111), (200), (220) типичны для электрохимически осажденных пленок Ni.

Магнитные свойства образцов измеряли при 300 К и 4,2 К магнитометром вибрационного типа (VSM) 7400-S в магнитном поле до 2Т при направлении поля перпендикулярно и параллельно поверхности образцов. Точность установки поля ±10Г, температуры $\pm 10^{-2}$К. Результаты приведены на рис. 2.

Из рис. 2 видно, что квадратичность и расширение петель гистерезиса больше, когда приложенное поле параллельно оси нанонитей. В этом случае домены магнетика располагаются вдоль оси нанонитей. Это способствует свободному вращению магнитных доменов вдоль магнитного поля и вызывает расширение и усиление квадратичности формы петель гистерезиса.



a *b*

Рис. 2. Петли гистерезиса для НН Ni при 300 К (красные линии) и 4,2 К (черные линии): *a* – приложенное поле параллельно оси НН; *b* – приложенное поле перпендикулярно оси (на вставках – увеличенные фрагменты намагниченности вблизи нулевого магнитного поля)
Fig. 2. Hysteresis loops for Ni HH at 300 K (red lines) and 4.2 K (black lines): *a* – applied field parallel to the HH axis; *b* – applied field perpendicular to the axis (insets – enlarged fragments of magnetization near zero magnetic field)

Полученные гистерезисные петли показывают, что НН Ni имеют характерное для ферромагнетиков поведение намагничивания из-за осевой анизотропии формы (одноосной анизотропии формы, uniaxial shape anisotropy). Результатом осевой анизотропии формы НН является наличие двух стабильных ориентаций магнитного момента, а именно, в параллельном или антипараллельном направлении к оси НН [8].

Таким образом НН Ni в МПАОА характеризуются преобладающей магнитной ориентацией вдоль оси, то есть типичной для ферромагнетиков типа никеля и железа осевой анизотропией формы.

Подробная информация о магнитных параметрах нанонитей Ni в МРАОА по сравнению с поликристаллическим массивным Ni (тонкие пленки никеля) и аналогичными образцами типа НН Ni в МПАОА из других работ представлена в таблице ($n = L_{NW}/ d_{NW}$).

Сравнение коэрцитивности (*Hc*) и квадратичности петли гистерезиса *Mr/Ms* для НН Ni в МПАОА с различным аспектным отношением при температурах 4,2 и 300К

Type and № of sample	Aspect ratio	*T*, K	H_c, ∥ Oe	H_c, ⊥ Oe	M_r/M_s, ∥	M_r/M_s, ⊥
I (№1)	170	4.2	770	207	0.65	0.07
		300	723	182	0.66	0.08
I (№2)	320	4.2	798	222	0.48	0.07
		300	756	208	0.51	0.07
I (№3)	350	4.2	775	174	0.66	0.06
		300	727	138	0.65	0.06
II (№4)	430	4.2	603	94	0.41	0.04
		300	593	44	0.40	0.03
II (№5)	570	4.2	574	73	0.42	0.03
		300	596	40	0.44	0.02
II (№6)	700	4.2	515	95	0.35	0.05
		300	513	43	0.34	0.02
[9] Ni NWs in Al_2O_3 template		300	580	162	0.49	0.066
[10] Ni NWs in Al_2O_3 template	200	300	624	-	0.30	-
[11] Bulk Ni		300	100	-	0.49	-

Заключение

В изготовленных наноструктурах длина нанонитей определяет степень магнитостатического взаимодействия между ними, которое оказывает влияние на коэрцитивность и квадратичность плотно упакованных массивов НН, качество которых зависит от условий изготовления матрицы МРАОА и НН.

Полученные наноструктуры могут быть использованы при изготовлении магнитных запоминающих устройств, нового поколения магниточувствительных транзисторов, энергоаккумулирующих систем, а также элементной базы современных средств защиты информации.

Список использованных источников / References

1. Mátéfi-Tempfli S., Mátéfi-Tempfli M., Vlad A., Antohe V., Piraux L. (2009) Nanowires and nanostructures fabrication using template methods: a step forward to real devices combining electrochemical synthesis with lithographic techniques. *J. Mater. Sci.: Mater. Electron.* 20(1), S249-S254.].

2. Fleischer R.P., Price P.B., Walker R.M. (1975) *Nuclear tracks in solids: principles and applications*. University of California Press: Berkeley, CA.

3. Kaniukov E. Yu., Shumskaya A.E., Kozlovskiy A.L., Zdorovets M.V., Trukhanov A.V., Zubar T.I., et al. (2021) Structure and magnetic properties of FeCo nanotubes obtained in pores of ion track templates. *Nano-Struct. Nano-Objects*. 26, 1000691.

4. Srivastav A.K. (2021) On the temperature dependent magnetization in dual-phase Co nanowires confinedly electrodeposited inside nanoporous alumina membrane. *J. Cryst. Growth*. 562, 126084.

5. Xu Q.; Meng G.; Han F. (2018) Porous AAO template-assisted rational synthesis of largescale 1D hybrid and hierarchically branched nanoarchitectures. *Prog. Mater. Sci*. 95, 243–285.

6. Qin L.; Zhaon J.; Guo Q.; Yan Z.; Mu F.; Chen P.; et al. (2013) Effect of length on magnetic properties of Ni 300 nm wide nanowires. *Physica E Low Dimens. Syst. Nanostruct*. 50, 17.

7. Vorobjova A.I.; Shimanovich D.L., Outkina E.A., Khodin A. A. (2018) Highly ordered through-holes porous alumina membranes for nanowires fabrication. *Appl. Phys. A*. 1, 124-132.

8. Ohgai T. (2012). *Magnetoresistance of nanowires electrodeposited into anodized aluminum oxide nanochannels. nanowires - Recent Advances.* Xihong Peng, IntechOpen.

9. Thongmee S., Pang H.L., Ding J., Lin J.Y. (2009) Fabrication and magnetic properties of metallic nanowires via AAO templates. *J. Magn. Magn. Mater*. 321, 2712-2716.

10. Escrig J., Lavın R., Palma J.L., Denardin J.C., Altbir D., Cortés A., et al. (2008) Geometry dependence of coercivity in Ni nanowire arrays. *Nanotechnol*. 19, 075713-075719.

11. Hwang J.H., Dravid V.P., Teng M.H., Host J.J., Elliott B.R., Johnson D.L., et al. (1997) Magnetic properties of graphitically encapsulated nickel nanocrystals. *J. Mater. Res*. 12, 1076–1082.

Сведения об авторах

Уткина У.А., канд. техн. наук, доц., ведущий научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», outkina@bsuir.by.
Воробьева А.И., канд. техн. наук, доц., ведущий научный сотрудник, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vorobjova@bsuir.by.

Information about the authors

Outkina E.A., Ph.D, Leading Researcher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", outkina@bsuir.by.
Vorobjova A.I., Ph.D, Leading Researcher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", vorobjova@bsuir.by.

УДК 378

ПОВЫШЕНИЕ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ НА ПРИМЕРЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «ТЕОРИЯ ЭЛЕКТРИЧЕСКОЙ СВЯЗИ»

Т.М. Фильченкова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье автор представил результаты проведенного опроса об организации лекций по учебной дисциплине «Теория электрической связи». Произведена оценка удовлетворенности студентов материалами, размещенными в системе электронного обучения. Данное исследование позволило преподавателю скорректировать проведение лекций с учетом пожеланий студентов. Рассмотрены факторы, влияющие на повышение качества подготовки специалистов в области защиты информации по специальности «Информационная безопасность».
Ключевые слова: качество образования; лекция; опрос; преподаватель; система электронного обучения; студенты; студентоцентрированное образование; учебная дисциплина; учреждение высшего образования; экзамен.

IMPROVING THE QUALITY OF TRAINING SPECIALISTS IN THE FIELD OF INFORMATION SECURITY THROUGH THE USE OF AN E-LEARNING SYSTEM USING THE EXAMPLE OF THE DISCIPLINE "THEORY OF ELECTRICAL COMMUNICATION"

T.M. Filchenkova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In the article, the author presented the results of a survey conducted on the organization of lectures on the academic discipline «Theory of Electrical Communications». An assessment of student satisfaction with the materials posted in the e-learning system was made. This study allowed the teacher to adjust the conduct of lectures taking into account the wishes of students. Factors influencing the improvement of the quality of training specialists in the field of information security in the specialty «Information Security» are considered.
Keywords: quality of education; lecture; survey; teacher; e-learning system; students; student-centered education; academic discipline; higher education institution; exam.

Введение

В настоящее время актуальным для учреждений высшего образования становится развитие студентоцентрированного образования. При таком подходе главное место занимают результаты обучения и воспитания, которые демонстрируют успешность выпускников учреждений высшего образования. В конце 2024 года Премьер-министр Республики Беларусь Роман Головченко провел в Белорусском национальном техническом университете совещание, на котором был озвучен вопрос об острой необходимости пересмотреть политику подготовки кадров инженерного профиля в учреждениях высшего образования Республики Беларусь. В новой модели подготовки инженеров должны быть учтены следующие моменты: реагирование на спрос самостоятельного творчества у студентов, на активное использование дистанционных методов обучения в образовательном процессе.

Основная часть

Учебная дисциплина «Теория электрической связи» для студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» специальности «Информационная безопасность» преподается в 4-ом семестре (2 курс). На рис. 1 представлено схематично структура учебно-методической карты учебной дисциплины «Теория электрической связи». Форма текущей аттестации по данной учебной дисциплине – экзамен. Учебная дисциплина «Теория электрической связи» способствует формированию у студентов специальности «Информационная безопасность» профессиональных компетенций, развитию самостоятельности, ответственности и организованности.

Структура учебно-методической карты учебной дисциплины «Теория электрической связи»

Темы															
Раздел 1							Раздел 2								
1		**2**			**3**		**4**	**5**	**6**	**7**	**8**			**9**	
Лекции															
№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	№12	№13	№14	№15	№16
Лабораторные работы															
№1		№2			№3		№4	—	—	—	—			—	
Практические занятия															
№1		№2			—		№3	—	—	—	—			№4	

Рис. 1. Схематическое представление структуры учебно-методической карты учебной дисциплины «Теория электрической связи»
Fig. 1. Schematic representation of the structure of the educational and methodological map of the academic discipline «Theory of Electrical Communications»

Как видно из рис. 1 учебная дисциплина состоит из 2-ух разделов, 9 тем, 16 лекций, 4 лабораторные работы и 4 практических занятия. Темы 5–8 не охвачены лабораторными и практическими, по ним только читаются лекции №№9–14.

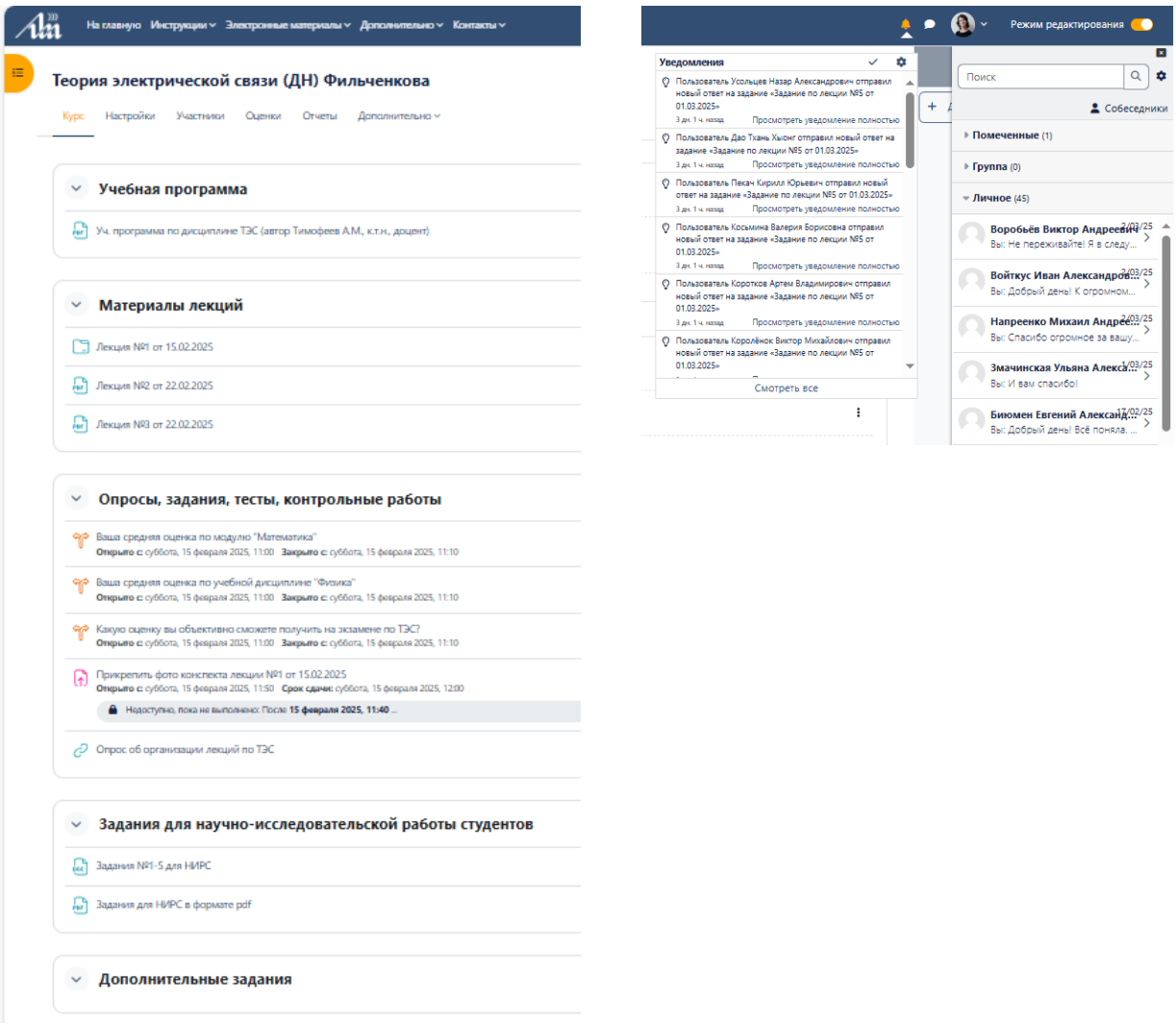
Студенты, как правило, во время семестра в образовательном процессе расставляют приоритеты готовиться к тому, что у них будут спрашивать и по чем

нужно будет отвечать устно или письменно. Таким образом, для качественного изучения студентами 2-го курса специальности «Информационная безопасность» учебной дисциплины «Теория электрической связи» на протяжении всего семестра преподаватель решил использовать возможности системы электронного обучения Moodle. На рис. 3 показан скриншот окна курса «Теория электрической связи».

С 15 февраля по 1 марта 2025 года было прочитано 5 лекций по двум темам учебной дисциплины «Теория электрической связи». Был проведен контроль знаний в конце 3-ей лекции в виде самостоятельной работы, а также организован опрос об организации лекций по учебной дисциплине «Теория электрической связи».

В ходе опросе студенты (45 из 68 студентов) оценили проведение лекционных занятий на 4,5 балла по 5-тибалльной системе.

На рис. 4 представлена гистограмма ответов студентов на вопрос «Вам нравится учебная дисциплина «Теория электрической связи»?». Интегральная оценка составила 8,53 балла по 10-балльной шкале.



a *b*

Рис. 3. Скриншот окна курса «Теория электрической связи»
в системе электронного обучения Moodle: *a* – структура курса; *b* – уведомления и чат
Fig. 3. Screenshot of the course window «Theory of Electrical Communications»
in the Moodle e-learning system: *a* – course structure; *b* - notifications and chat

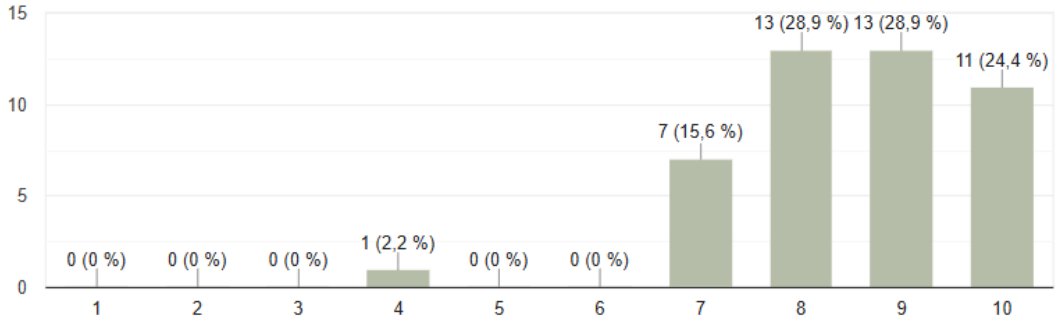


Рис. 4. Гистограмма ответов студентов на вопрос «Вам нравится учебная дисциплина «Теория электрической связи»?»
Fig. 4. Histogram of students' answers to the question "Do you like the academic discipline "Theory of Electrical Communications"?"

Студентам было предложено в опросе ответит на вопрос «Что вас не устраивает в проведении лекций?». В результате 69% респондентов ответили, что их все устраивает. Из наиболее интересных ответов на данный вопрос можно привести следующие:

– «Иногда не хватает времени полностью записать материал и из-за этого концентрируешься не на материале, а на том, чтобы все успеть написать, но добавление презентаций в СЭО упрощает эту задачу».

– «Немного неудобно перерисовывать графики, так как, параллельно с этим еще идет объяснение материала далее и фокус внимания немного смещается, не хватает еще письменного пояснения графика».

В ходе исследования студентам был задан вопрос «Вы довольны результатом самостоятельной работы, которую написали 22.02.2025?», результаты приведены на рис. 5.

Рис. 5. Диаграмма ответов студентов на вопрос «Вы довольны результатом самостоятельной работы, которую написали 22.02.2025?»
Fig. 5. Diagram of students' answers to the question "Are you satisfied with the result of the independent work that you wrote on 22.02.2025?"

Предоставление преподавателем материалов по учебной дисциплине «Теория электрической связи» в системе электронного обучения Moodle ***«Курс: Теория электрической связи (ДН) Фильченкова | СЭО»*** студенты оценили на 4,80 по 5-тибалльной шкале.

Студенты считают, что качество образования повышается при использовании такого формата проведения лекций и предоставлении материалов в системе электронного обучения Moodle. Гистограмма ответов на вопрос «Какую оценку

объективно вы сможете вы получить за экзамен по учебной дисциплине «Теория электрической связи»?»

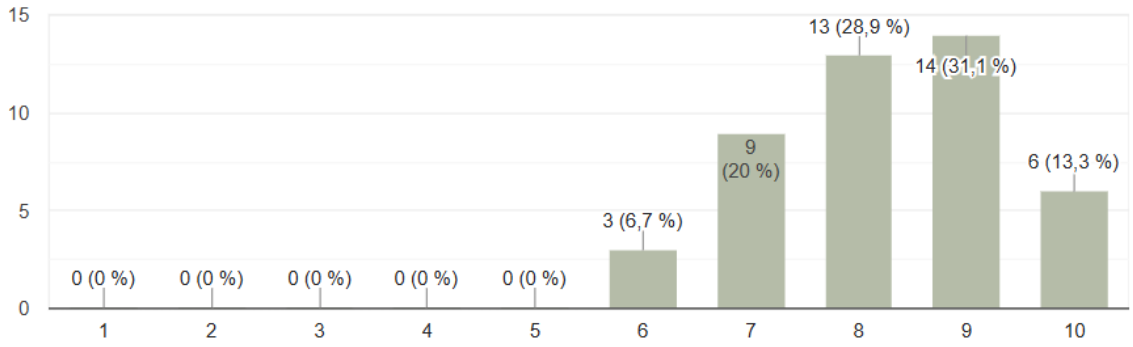


Рис. 6. Гистограмма ответов студентов на вопрос «Какую оценку объективно вы сможете вы получить за экзамен по учебной дисциплине «Теория электрической связи»?»
Fig. 6. Histogram of students' answers to the question "What grade can you objectively receive for the exam in the academic discipline "Theory of Electrical Communications"?"

В конце опроса у студентов спросили: «Может быть у вас есть идеи как преподавателю стоит организовать проведение лекций, чтобы это было качественно, эффективно и результативно для студентов, изучающих учебную дисциплину «Теория электрической связи»?». Студенты оставили по желанию такие ответы:

– «Я не знаю, но я впечатлена тем, как оценивают студентов в процессе обучения».

– «Приводить практические примеры».

– «Возможно, дать в СЭО материал для дополнительного самостоятельного изучения, который позволил бы ознакомиться с предметом немного глубже».

– «Мне нравится проведение таких самостоятельных, так как я действительно запоминаю лучше материал».

Заключение

Исследование показало, что участие студентов в организации образовательного процесса по учебной дисциплине «Теория электрической связи» повышает мотивацию учиться, совершенствовать преподавателю курс и проведение лекций. Таким образом, данный подход позволяет повышать качество образования по учебной дисциплине «Теория электрической связи».

Сведения об авторе

Фильченкова Т.М., старший преподаватель кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», t.filchenkova@bsuir.by.

Information about the author

Filchenkova T., Senior Lecturer, Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", t.filchenkova@bsuir.by.

УДК 004.056.5

О СПОСОБАХ СОВМЕСТНОГО ШИФРОВАНИЯ И АУТЕНТИФИКАЦИИ

В.М. Фомичев[1, 2, 3], Д.А. Бобровский[2], И.Э. Недомолкин[2]
[1]Российский технологический университет (РТУ МИРЭА), Москва, Россия
[2]ООО «Код Безопасности», Москва, Россия
[3]Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук, Москва, Россия

Аннотация. В докладе рассматривается разработка нового способа совместного шифрования и аутентификации данных – способа E-IB, который ориентирован на повышение вычислительной эффективности при сохранении высокого уровня безопасности. Этот способ объединяет функции шифрования и аутентификации, используя общий ключ и минимизируя вычислительные затраты по сравнению с традиционными подходами, что особенно важно для маломощных устройств, не поддерживающих AVX-инструкции. Для аутентификации используются промежуточные блоками процесса шифрования, что позволяет обеспечить безопасность с низкими затратами на вычисления и память. В докладе представлены экспериментальные результаты применения предложенного метода на примере шифра Магма, где показана его высокая производительность и преимущество по быстродействию по сравнению с известными режимами, такими как XTSMAC и MGM. Также обсуждаются возможности применения этого подхода в условиях ограниченных вычислительных ресурсов, например, в IoT-устройствах и других встраиваемых системах. Режим CBC-IB устойчив к атакам CPA при корректном использовании IV и защищен от атак на целостность шифртекста, однако для защиты от атак CCA требуются дополнительные меры.
Ключевые слова: AEAD; шифрование; аутентификация; промежуточные блоки; вычислительная эффективность; маломощные устройства; AVX; шифр Магма; производительность.

ON COMBINED ENCRYPTION AND AUTHENTICATION METHODS

V.M. Fomichev[1, 2, 3], D.A. Bobrovskiy[2], I.E. Nedomolkin[2]
[1]Moscow Technological University (MIREA), Moscow, Russia
[2]LLC "Code Security", Moscow, Russia
[3]Federal Research Center "Informatics and Management" of the Russian Academy of Sciences, Moscow, Russia

Abstract. This paper presents the development of a new combined encryption and authentication method, the E-IB method, which aims to improve computational efficiency while maintaining a high level of security. This method combines encryption and authentication functions, using a shared key and minimizing computational costs compared to traditional approaches, which is particularly important for low-power devices that do not support AVX instructions. The method integrates control of intermediate blocks during the encryption process, ensuring high security with low computational and memory overhead. Experimental results of applying the proposed method, based on the Magma cipher, are also presented, demonstrating its high performance and superior speed compared to well-known modes such as XTSMAC and MGM. The potential of applying this approach in environments with limited computational resources, such as IoT devices and other embedded systems, is also discussed. The CBC-IB mode is resistant to CPA attacks when the IV is used correctly and protected against ciphertext integrity attacks; however, additional measures are required to defend against CCA attacks.
Keywords: AEAD; encryption; authentication; intermediate blocks; computational efficiency; low-power devices; AVX; Magma cipher; performance.

Введение

При синтезе средств криптографической защиты информации актуальна разработка режимов шифрования класса AEAD – совместного шифрования и аутентификации данных. Целью AEAD-режимов является объединение шифрования и аутентификации при сохранении криптостойкости и эффективности использования

памяти, а также снижение вычислительной сложности по сравнению с их раздельным выполнением [1].

Известные режимы шифрования класса AEAD не всегда удовлетворяют требованиям по вычислительной сложности при совместном выполнении шифрования и аутентификации. В связи с этим актуальна разработка режима с достаточно высокими криптографическими свойствами и приемлемыми характеристиками сложности [2].

В связи с режимами класса AEAD в докладе представлен E-IB (E – encryption, IB - intermediate blocks) – способ совместного шифрования и аутентификации данных с использованием суммирования промежуточных блоков. Представлены данные для сравнения характеристик нового способа с характеристиками прототипов. Способ EIB особенно актуален для применения в маломощных устройствах, не поддерживающих инструкции AVX, где важно снизить вычислительные требования и эффективнее использовать ресурсы процессора. Этот подход позволяет реализовать эффективные механизмы защиты данных, минимизируя нагрузку на аппаратные ресурсы, что критично для таких устройств.

Способ E-IB шифрования и генерации кода аутентификации

Способ E-IB может быть реализован для различных режимов блочного шифрования с обратной связью по шифрованному тексту, например, для режимов CBC, CFB и других. Название конкретного режима получится, если заменить букву E на аббревиатуру конкретного режима блочного шифра, например, CBC-IB.

Обозначим V_n множество двоичных n-битовых векторов.

Опишем способ CBC-IB на примере $2r$-раундового блочного шифра Фейстеля с ключом $k \in V_n$ на основе режима шифрования CBC, $r > 1$. Для простоты изложения число раундов четное, однако это условие не нарушает общности рассуждений.

Запишем уравнения в режиме CBC с использованием функции шифрования E_k с ключом k и случайным и уникальным инициальным вектором $z \in V_{2m}$, присоединяемым к сообщению в открытом виде. Шифрование сообщения $x_1, \dots, x_t$, состоящего из $2m$-битовых блоков, задано уравнениями:

$$E_k(x_i \oplus y_{i-1}) = y_i, i = 1, \dots, t, \quad (1)$$

где $y_1, \dots, y_t$ – шифрованный текст, $y_i \in V_{2m}$, $y_0 = z \oplus E_k(z)$, $\oplus$ – XOR-суммирование.

Шифр Фейстеля построен на основе нелинейной рекурренты порядка 3 над множеством V_m. Обозначим U_k зависящую от ключа k нелинейную часть генерирующей функции рекурренты, и пусть для $b_i \in V_m$ выполнено

$$b_{j+1} = U_k(b_j) \oplus b_{j-1}, j \geq 1. \quad (2)$$

Тогда в соответствии с (2) шифрование есть вычисление для открытого текста $x = (b_0, b_1)$ шифрованного текста $y = (b_{2r+1}, b_{2r})$. Отметим, что шифртекст состоит из двух последних членов рекуррентной последовательности, взаимно переставленных по сравнению с естественным порядком. В шифрах Фейстеля такая перестановка необходима для инволютивности алгоритмов зашифрования и расшифрования.

При шифровании блока x_i на ключе k для начального блока $x_i \oplus y_{i-1} = (b_0^{(i)}, b_1^{(i)})$, $i = 1, \dots, t$, в соответствии с (2) вычисляем рекуррентную последовательность $\{b_2^{(i)}, b_3^{(i)}, \dots, b_{2r}^{(i)}, b_{2r+1}^{(i)}\}$ и получаем шифртекст

$y_1 = \left(b_{2r+1}^{(1)}, b_{2r}^{(1)}\right), \dots, y_t = \left(b_{2r+1}^{(t)}, b_{2r}^{(t)}\right)$. Попутно с шифрованием вычисляем промежуточные блоки $a_r^{(i)} = \left(b_r^{(i)}, b_{r+1}^{(i)}\right) \in V_{2m}$, $i = 1, \dots, t$, и код аутентификации $A_k(y_0, x_1, \dots, x_t)$:

$$A_k(y_0, x_1, \dots, x_t) = \left(\sum_{1 \le i \le t} a_r^{(i)}\right) \bmod 2^{2m}. \quad (3)$$

Шифрованное сообщение в режиме CBC-IB вкупе с кодом аутентификации есть последовательность $y_1, \dots, y_t, A_k(y_0, x_1, \dots, x_t)$.

Расшифрование и проверка аутентичности открытого текста

При расшифровании используем равенство, следующее из (2):

$$b_{j-1} = U_k(b_j) \oplus b_{j+1}, 1 \le j \le 2r. \quad (4)$$

В соответствии с (4) при расшифровании вычисляем блоки открытого текста $(b_0^{(i)}, b_1^{(i)})$ по блокам шифртекста $\left(b_{2r+1}^{(i)}, b_{2r}^{(i)}\right)$, попутно вычисляя промежуточные блоки $c_r^{(i)} = \left(b_r^{(i)}, b_{r+1}^{(i)}\right)$, $i = 1, \dots, t$, и суммируя их по $\bmod 2^{2m}$. Данные признаются аутентичными $\Leftrightarrow$

$$\left(\sum_{1 \le i \le t} c_r^{(i)}\right) \bmod 2^{2m} = A_k(y_0, x_1, \dots, x_t).$$

Анализ свойств способа CBC-IB

1. Ключ k общий (одинаковый) для функций шифрования и аутентификации.

2. Создание кода аутентификации и проверка аутентичности открытого текста не увеличивает значительно сложность вычислений по сравнению с алгоритмами зашифрования-расшифрования и не требует значительной дополнительной памяти.

3. Параметры r и m не должны быть малы. Блочный шифр после r раундов должен реализовать вполне перемешивающую нелинейную подстановку, т.е. каждая координатная функция подстановки после r раундов должна быть нелинейной и зависеть существенно от всех битов открытого текста и ключа. Во избежание случайного угадывания кода аутентификации достаточно взять $m \ge 32$.

4. «Подделка» нарушителем кода аутентификации и вектора y_0 требует знания ключа k вкупе с открытым текстом. Сложность определения ключа блочного шифра по открытому тексту, шифртексту и коду аутентификации должна быть столь же высокая, как и без знания кода.

Для анализа свойств безопасности AEAD-схем относительно угроз нарушения конфиденциальности и целостности в работе [3] были введены базовые определения безопасности. CBC-IB устойчив к простым атакам CPA, если IV генерируется случайным образом и используется корректно. Защита от CCA требует дополнительных механизмов для предотвращения манипуляций с шифртекстами и расшифрованиями. CBC-IB устойчив к атакам на целостность шифртекста.

Заключение

Результаты практической реализации способа аутентифицированного шифрования CBC-IB подтверждают целесообразность его применения в средствах

защиты информации.

Экспериментально получены показатели скорости работы различных режимов для шифра Магма, а также предложенного способа CBC-IB на основе шифра Магма. Эксперименты проводились на ЭВМ с процессором AMD Ryzen 5 5600G с постоянной тактовой частотой 4.0 ГГц. В таблице ниже для различных алгоритмов указаны число затраченных тактов процессора, скорость зашифрования и производительность относительно алгоритма Магма в режиме CBC, принятая за 100%.

Таблица 1. Сравнение производительности
Table 1. Performance comparison

Режим	Число тактов процессора	Скорость, MiB/s	Относительная производительность, %
Magma CBC	$59.5 * 10^6$	72.27	100
Magma CBC-IBS	$60 * 10^6$	71.67	99,2
XTSMAC	$64 * 10^6$	67.19	93,1
AK Magma MGM	$121 * 10^6$	35.54	49,2

Таблица показывает, что аутентифицированное шифрование CBC-IB фактически не уступает по быстродействию режиму CBC и превосходит известные режимы: на 6,1 % XTSMAC и более чем в 2 раза MGM. Достоинством CBC-IB является также техническая простота интеграции режима AEAD в среде, где применяется CBC: переход на CBC-IB упрощен по сравнению с XTSMAC или MGM.

Аналогичный эффект ожидается от аутентифицированного шифрования CFB-IB.

Список использованных источников / References

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2001). Handbook of Applied Cryptography. CRC Press

2. Kampanakis P., Campagna M., Crocket E. (2024) Practical Challenges with AES-GCM and the need for a new cipher. Practical Challenges with AES-GCM and the need for a new cipher. NIST PQC

3. Bellare, M., & Namprempre, C. (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. In Proceedings of the 3rd International Conference on Theory of Cryptography (TCC 2000).

Сведения об авторах

Фомичев В.М., д.ф.-м.н., проф., Российский технологический университет (РТУ МИРЭА), ООО «Код Безопасности», Федеральный исследовательский центр "Информатика и управление" Российской Академии Наук.
Бобровский Д.А., руководитель группы отдела криптографического анализа, ООО «Код Безопасности»
Недомолкин И.Э., младший системный аналитик отдела криптографического анализа, ООО «Код Безопасности.

Information about the authors

V.M. Fomichev, Dr. Sci., Prof., Russian Technological University (RTU MIREA), "Security Code" LLC, Federal Research Center "Informatics and Management" of the Russian Academy of Sciences.
D.A. Bobrovsky, Team Leader, Cryptographic Analysis Department, "Security Code" LLC.
I.E. Nedomolkin, Junior Systems Analyst, Cryptographic Analysis Department, "Security Code" LLC.

УДК 004.056

АНАЛИЗ УСТОЙЧИВОСТИ СОВРЕМЕННЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

А.М. Хамраев, А.Б. Суннатов
Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. В данной работе анализируются современные криптографические алгоритмы, включая симметричные и асимметричные системы шифрования, а также хеш-функции. Рассматриваются их преимущества, недостатки и уязвимости в контексте традиционных и современных атак. Особое внимание уделено угрозам со стороны квантовых вычислений и перспективам постквантовой криптографии. Работа завершается обсуждением актуальных вызовов и тенденций в области криптографической защиты данных.
Ключевые слова: AES; хэш-функции; постквантовые; криптосистема; суперсингулярные.

ANALYSIS OF THE RESILIENCE OF MODERN CRYPTOGRAPHIC ALGORITHMS

A.M. Hamrayev, A.B. Sunnatov
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. This paper analyzes modern cryptographic algorithms, including symmetric and asymmetric encryption systems, as well as hash functions. Their advantages, disadvantages, and vulnerabilities in the context of traditional and modern attacks are examined. Particular attention is paid to threats from quantum computing and the prospects of post-quantum cryptography. The paper concludes with a discussion of current challenges and trends in the field of cryptographic data protection.
Keywords: AES; hash functions; post-quantum; cryptosystem; supersingular.

Введение

Криптография является основой цифровой безопасности, защищая данные в финансовых системах, коммуникациях, облачных сервисах и других сферах. Однако эволюция атакующих технологий, таких как квантовые компьютеры, ставит под угрозу традиционные алгоритмы шифрования. Эта статья анализирует современные криптографические алгоритмы с точки зрения их устойчивости, обсуждает их слабые стороны и прогнозирует будущее развития этой области.

Современные криптографические алгоритмы: структура и особенности

Симметричные алгоритмы используют единый ключ для шифрования и дешифрования.

AES (Advanced Encryption Standard). Устойчив к большинству известных атак, поддерживает длину ключа 128, 192 и 256 бит. Уязвимости: атаки полного перебора остаются единственным реальным способом взлома, но требуют огромных вычислительных ресурсов.

ChaCha20. Обеспечивает высокую скорость шифрования, устойчив к криптоаналитическим атакам. Преимущества: энергоэффективность, что делает его подходящим для мобильных устройств.

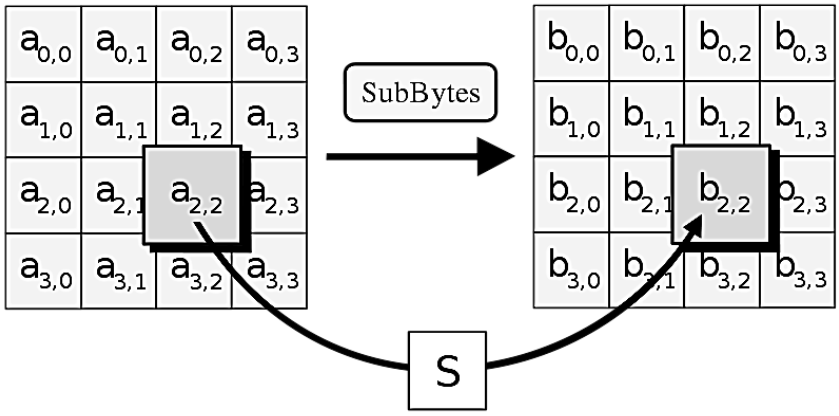


Рис. 1. SubBytes() трансформация при шифровании
Fig. 1. SubBytes() transformation during encryption

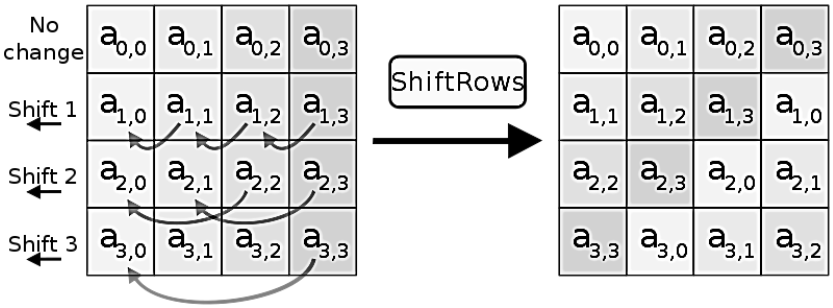


Рис. 2. ShiftRows() трансформация при шифровании
Fig. 2. ShiftRows() transformation during encryption

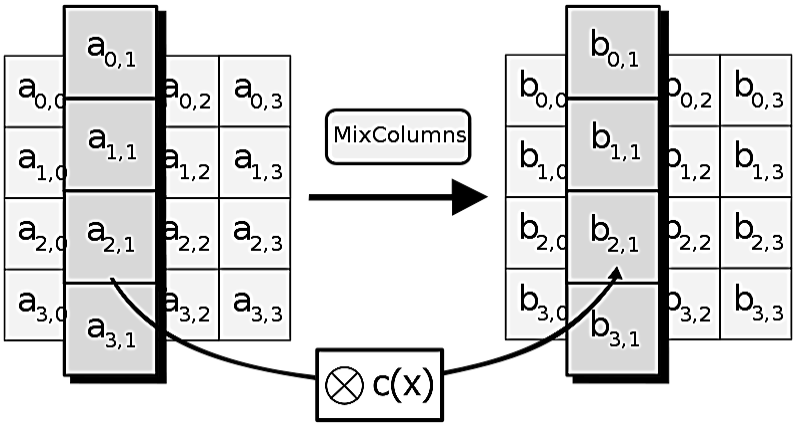


Рис. 3. MixColumns() трансформация при шифровании
Fig. 3. MixColumns() transformation during encryption

Асимметричные алгоритмы шифрования

Основаны на использовании пары ключей: публичного и приватного.

RSA. Основан на сложности факторизации больших чисел. Уязвимости: уязвим к квантовым атакам (алгоритм Шора).

Эллиптические кривые (ECC). Предлагают повышенную устойчивость при меньшем размере ключа по сравнению с RSA. Уязвимости: аналогично RSA, уязвимы к атакам квантовых компьютеров.

Хеш-функции. Используются для проверки целостности данных и создания цифровых подписей.

SHA-2 и SHA-3. Устойчивы к большинству современных атак, за исключением квантовых угроз. Уязвимости: квантовые атаки (например, атака Гровера) могут сократить сложность нахождения коллизий.

MD5 и SHA-1. Устарели из-за высокого риска коллизий.

Методы атак на криптографические алгоритмы следующие.

1. Атаки полного перебора. Основаны на переборе всех возможных ключей. Противодействие: увеличение длины ключа.

2. Криптоаналитические атаки. Линейный и дифференциальный анализ (применимы к симметричным алгоритмам).

3. Атаки на основе подобранных шифротекстов.

4. Атаки на основе квантовых вычислений: Алгоритм Шора: эффективен для решения задач факторизации и дискретного логарифма. Алгоритм Гровера: снижает сложность перебора ключей в два раза.

Угрозы квантовых вычислений

Квантовые компьютеры могут коренным образом изменить криптографический ландшафт. Для асимметричных алгоритмов угроза особенно велика:

– RSA и ECC становятся уязвимыми при наличии достаточно мощного квантового компьютера.

– Симметричные алгоритмы (например, AES) остаются более устойчивыми, но требуют увеличения длины ключа.

Постквантовые криптографические алгоритмы

Для защиты от квантовых атак разрабатываются постквантовые алгоритмы, основанные на задачах, устойчивых к квантовым вычислениям:

– Решеточные криптосистемы (Lattice-based):

– Основаны на сложных задачах, связанных с многомерными решетками. Примеры: NTRU, Kyber.

– Кодовые криптосистемы (Code-based):

– Основаны на декодировании случайных линейных кодов. Пример: McEliece.

– Суперсингулярные изогении эллиптических кривых:

– Используют вычисления на изогениях эллиптических кривых.

Проблемы и вызовы

1. Рост вычислительных ресурсов: Постквантовые алгоритмы требуют большего объема памяти и времени выполнения.

2. Необходимость стандартизации: Институт NIST проводит соревнования по выбору устойчивых алгоритмов, но процесс внедрения остается медленным.

3. Совместимость: Требуется адаптация существующих систем для работы с новыми стандартами.

4. Экономические затраты: Внедрение постквантовой криптографии требует значительных инвестиций.

Заключение

Современные криптографические алгоритмы демонстрируют высокую устойчивость к традиционным атакам. Однако квантовые вычисления требуют перехода к новым методам шифрования, способным выдерживать атаки будущего. Постквантовая криптография становится важнейшим направлением исследований,

предлагая алгоритмы, которые смогут защитить данные даже в условиях квантовых угроз.

Список использованных источников / References

1. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.
2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, 21(2), 120-126.
3. NIST. (2016). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.
4. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Springer.
5. Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing, 26(5), 1484–1509.

Сведения об авторах

Хамраев А.М., преподаватель, Государственный энергетический институт Туркменистана, pvm87818@gmail.com.
Суннатов А.Б., студент, Государственный энергетический институт Туркменистана, pvm87818@gmail.com.

Information about the authors

Hamrayev A., teacher, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Sunnatov A., student, The State Energy Institute of Turkmenistan, pvm87818@gmail.com.

УДК 004.56+003.26

МЕТОД ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ И КОДИРОВАНИЕ ИНФОРМАЦИИ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

А.А. Хартанович
Белорусский государственный технологический университет, Минск, Беларусь

Аннотация. В данной работе рассматривается метод стеганографии, основанный на дискретном вейвлет-преобразовании, и применение кодирования информации для повышения надежности скрытой передачи данных. Описывается процесс разложения изображения с использованием преобразования Хаара, который позволяет выделять поддиапазоны и встраивать секретные сообщения в наименее заметные области. Проведен сравнительный анализ методов стеганографии по показателям MSE и PSNR, а также исследовано влияние различных модификаций изображения на точность извлечения данных. Для повышения устойчивости к искажениям использован код Хемминга, который позволяет обнаруживать и исправлять ошибки при декодировании, однако предлагается применение более сложных конструкций кодирования и декодирования сообщения на основе комбинирования кодов. Результаты экспериментов подтверждают, что сочетание ДВП и методов кодирования обеспечивает высокую степень скрытности и надежности передачи информации.
Ключевые слова: стеганография; секретное сообщение; преобразование Хаара; дискретное вейвлет-преобразование (ДВП); поддиапазон; коэффициент битовых ошибок; отношение сигнал/шум; среднеквадратическая ошибка; кодирование; код Хемминга.

DISCRETE WAVELET TRANSFORM METHOD AND INFORMATION ENCODING IN STEGANOGRAPHIC APPLICATIONS

A.A. Khartanovich
Belarusian State Technological University, Minsk, Belarus

Abstract. This paper discusses a steganography method based on the discrete wavelet transform and the use of information coding to improve the reliability of hidden data transmission. It describes the process of image decomposition using the Haar transform, which allows you to select subranges and embed secret messages in the least noticeable areas. A comparative analysis of steganography methods is carried out based on MSE and PSNR indicators, and the effect of various image modifications on the accuracy of data extraction is studied. To improve resistance to distortion, the Hamming code is used, which allows detecting and correcting errors during decoding, but it is proposed to use more complex structures of encoding and decoding of the message

based on a combination of codes. The experimental results confirm that the combination of DWT and coding methods provides a high degree of secrecy and reliability of information transmission.
Keywords: steganography; secret message; Haar transform; discrete wavelet transform (DWT); subband; bit error rate; signal to noise ratio; root mean square error; coding; Hamming code.

Введение

Стеганография – наука о способах передачи (хранения) сокрытой информации, где скрытый канал организуется на базе и внутри открытого с использованием особенностей восприятия информации [1]. Стеганографическая система (стеганосистема) – совокупность средств и методов для формирования скрытого канала передачи информации. Стеганосистема образует стеганоканал, по которому передается (или в котором хранится) заполненный контейнер. Модель стеганосистемы представлена на рис. 1.

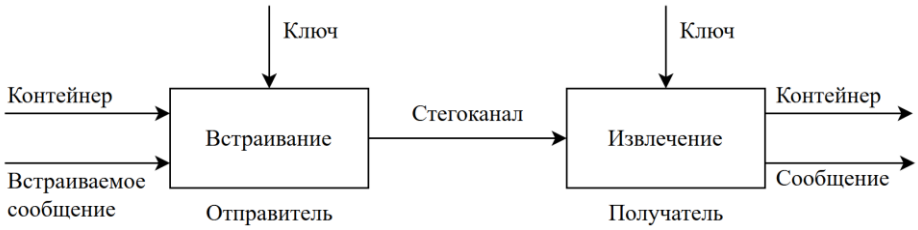


Рис. 1. Модель стеганографической системы
Fig. 1. Model of steganographic system

Стеганографические методы имеют свои достоинства и недостатки, но наибольшего внимания заслуживают в силу своих преимуществ методы частотной области, а именно – метод дискретного вейвлет-преобразования [2].

Основная часть

Дискретное вейвлет-преобразование (ДВП) – метод анализа и преобразования сигналов и изображений, использующий вейвлеты [3]. Процесс ДВП включает разложение изображения на набор коэффициентов различных масштабов и частот, который представляет собой различные детали изображения.

При разложении изображения методом ДВП применяется преобразование Хаара, которое использует двумерный матричный источник (канал RGB-изображения) и применяет вейвлет-преобразование, обрабатывая входное изображение, которое делится на неперекрывающиеся блоки 2×2 пикселей, каждый из которых преобразуется в четыре поддиапазона:

LL – низкочастотное приближение;
LH – горизонтальные различия;
HL – вертикальные различия;
HH – диагональные различия (высокочастотные детали).

Поддиапазон *LL* захватывает наиболее значимые особенности, а другие поддиапазоны – более мелкие детали, куда обычно встраивается сообщение.

Каждый блок можно представить в виде матрицы

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}, \quad (1)$$

где *A, B, C* и *D* – значения интенсивностей цвета пикселей от 0 до 255.

Формула преобразования для поддиапазона *LL*:

$$LL = \frac{A + B + C + D}{2}. \quad (2)$$

Получение *LH* описывается формулой:

$$LH = \frac{A - B + C - D}{2}. \quad (3)$$

Для получения поддиапазона *HL* используется формула:

$$HL = \frac{A + B - C - D}{2}, \quad (4)$$

а для поддиапазона *HH* соответственно:

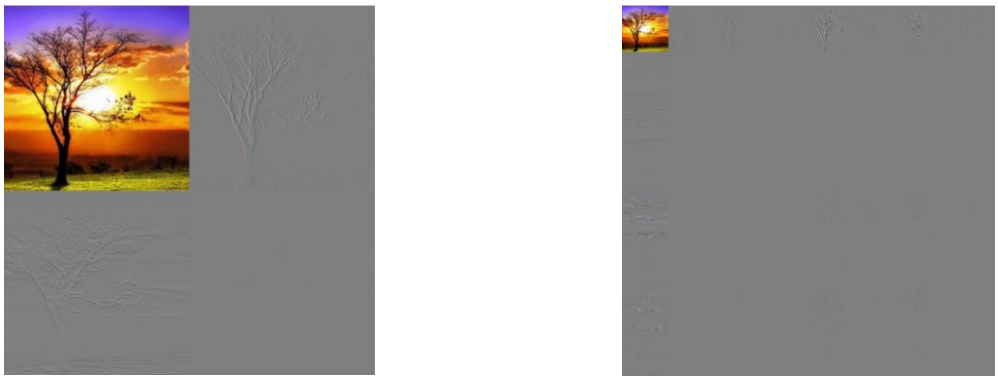
$$HH = \frac{A - B - C + D}{2}. \quad (5)$$

Преобразование необходимо повторять для всех блоков, что снижает разрешение изображения, сохраняя при этом основные детали. Встраивание секретного сообщения происходит в коэффициенты поддиапазона *HH*, при этом символы сообщения преобразуются в 8-битные значения кода ASCII. В процессе изменения значений *HH* используется специальная переменная α, равная небольшому значению (например, α = 0,001), что обеспечивает незаметность. Если бит встраиваемого сообщения равен 1, то коэффициент *HH* увеличивается на значение α, а если бит равен 0, то уменьшается на тоже значение.

При извлечении сообщения проверяются значения коэффициентов поддиапазона *HH*. Если значение *HH* было увеличено, то бит секретного сообщения равен 1, если значение было уменьшено – значение бита равно 0.

Размер изображения определяет, сколько раз его можно разложить на поддиапазоны. Каждый уровень разложения уменьшает разрешение в два раза.

Для демонстрации было разработано приложение, которое позволяет разложить изображение. На рисунке 2 представлены примеры разложения.



a *b*

Рис. 2. Разложение изображения методом ДВП: *a* – 1 уровень; *b* – 3 уровня
Fig. 2. Image decomposition using the DWT: *a* – 1 level; *b* – 3 levels

На практике не следует использовать максимальное количество уровней из-за вычислительной сложности и уменьшающейся отдачи от эффективности внедрения вследствие ухудшения качества изображения.

Разработанный метод ДВП сравнивался с пространственным методом наименее значащих битов (LSB) и частотным методом дискретного косинус-преобразования (ДКП) по параметрам MSE (среднеквадратическая ошибка) и PSNR (отношение сигнал/шум) [4]. Более низкое значение MSE указывает на более близкое соответствие между изображениями, а более высокий PSNR – на лучшее качество и большее сходство двух изображений. В одно и тоже изображение внедрялись одинаковые сообщения разной длины по 100, 1000 и 5000 байт (Б) различными методами. Результаты представлены в табл. 1.

Таблица 1. Значения параметров MSE и PSNR для различных методов
Table 1. Values of MSE and PSNR parameters for different methods

Метод и длина сообщения	MSE	PSNR
LSB 100 Б	0,56385	50,62641
ДКП 100 Б	0,33623	52,86360
ДВП 100 Б	0,11564	57,48899
LSB 1000 Б	6,43666	40,04436
ДКП 1000 Б	4,93623	41,19660
ДВП 1000 Б	0,11564	57,48899
LSB 5000 Б	12,43666	37,18336
ДКП 5000 Б	8,65038	38,76001
ДВП 5000 Б	0,11564	57,48899

Одинаковые значения MSE и PSNR для различных длин сообщений в методе ДВП возникают из-за того, что внедрение информации происходит в наименее значимой области изображения, где одни и те же коэффициенты подвергались повторным изменениям. В итоге разработанный метод ДВП не влияет на параметры анализа изображения, что позволяет встраивать достаточно большие объемы данных без ухудшения качества изображения.

Стеганографические методы также анализировались в условиях модификации изображений. Вейвлет-преобразование демонстрирует лучшую устойчивость к различным изменениям, особенно к сжатию с потерями, однако в некоторых случаях его эффективность оказывается недостаточной, поскольку при значительных изменениях изображения восстановить исходное сообщение полностью не удается. Предлагается дополнительно с ДВП использовать кодирование исходного сообщения для коррекции ошибок при его извлечении.

Сообщение объемом 5000 Б кодировалось с использованием кода Хемминга (7, 4) и внедрялось в JPEG изображение размером 1024×1024 пикселей методом ДВП [5]. Стегоизображение модифицировалось, после извлечения и декодирования сообщения рассчитывалось среднее значение параметра BER (коэффициент битовых ошибок). Сравнительный анализ представлен в табл. 2.

Таблица 2. Значения BER при декодировании извлеченного сообщения
Table 2. BER values when decoding the extracted message

Модификация изображения	BER без применения кода Хемминга	BER с применением кода Хемминга
Сжатие до 50%	5% (2000 бит с ошибкой)	0,25% (100 бит с ошибкой)
Размер уменьшен на 20%	10% (4000 бит с ошибкой)	1,12% (784 бит с ошибкой)
Контраст увеличен	15% (6000 бит с ошибкой)	2,25% (900 бит с ошибкой)

Код Хемминга (7, 4) исправляет одиночные ошибки и обнаруживает двойные, что позволяет значительно снизить BER при модификациях стегоизображения. Однако использование усовершенствованных методов для исправления ошибок на основе комбинирования кодов позволит исправлять множественные случайные и пакетные ошибки и еще больше уменьшит коэффициент BER [6].

Заключение

Преимуществом вейвлет-преобразования является возможность внедрения информации в малозаметные области изображения путем работы с различными поддиапазонами. Кроме того, данный метод демонстрирует устойчивость к сжатию с потерями и другим модификациям изображения, поскольку данные встраиваются в его частотные характеристики. Дополнительное использование кодирования информации позволяет восстановить скрытое сообщение, даже если оно было искажено в процессе передачи или изменения изображения.

Список использованных источников

1. Урбанович П.П. (2016) *Защита информации методами криптографии, стеганографии и обфускации*. Минск, Издательство «БГТУ».
2. Сейеди С.А., Садыхов Р.Х. (2013) Сравнение методов стеганографии в изображениях. *Информатика*. (37), 66–75.
3. Mallat S. (1989) A Theory for Multiresolutional Signal Decomposition: the Wavelet Representation. *IEEE Trans. Pattern Analysis and Machine Intelligence*. 11 (7), 674–693.
4. Sara U., Akter M., Uddin M. (2019) Image Quality Assessment through FSIM, SSIM, MSE and PSNR – A Comparative Study. *Journal of Computer and Communications*. 7 (3), 8–18.
5. Питерсон У., Уэлдон Э. (1976) *Коды, исправляющие ошибки*. Москва, Издательство «Мир».
6. Хартанович А.А. (2024) Комбинирование каскадной модели и стеганографического метода для размещения информации в файлах изображений. *Технические средства защиты информации.* (12), 94–95.

References

1. Urbanovich P.P. (2016) *Information Protection by Methods of Cryptography, Steganography and Obfuscation*. Minsk, BSTU Publishing House (in Russian).
2. Seyedi S.A., Sadykhov R.Kh. (2013) Comparison of Steganography Methods in Images. *Informatics*. (37), 66–75 (in Russian).
3. Mallat S. (1989) A Theory for Multiresolutional Signal Decomposition: the Wavelet Representation. *IEEE Trans. Pattern Analysis and Machine Intelligence*. 11 (7), 674–693.
4. Sara U., Akter M., Uddin M. (2019) Image Quality Assessment through FSIM, SSIM, MSE and PSNR – A Comparative Study. *Journal of Computer and Communications*. 7 (3), 8–18.
5. Peterson W., Weldon E. (1976) *Error-Correcting Codes*. Moscow, Mir Publishing House.
6. Khartanovich A.A. (2024) Combining a Cascade Model and a Steganographic Method for Placing Information in Image Files. *Technical means of information protection.* (12), 94–95 (in Russian).

Сведения об авторе

Хартанович А.А., магистрант кафедры информационных систем и технологий, Белорусский государственный технологический университет, alinakhartanovichlo@gmail.com.

Information about the author

Khartanovich A., Master's degree student, the Department of Information Systems and Technologies, Belarusian State Technological University, alinakhartanovichlo@gmail. com.

УДК 544.653.2

ЧУВСТВИТЕЛЬНЫЕ МЕМБРАННЫЕ ЭЛЕМЕНТЫ НА ОСНОВЕ ПЛЕНОК ПОРИСТОГО ОКСИДА АЛЮМИНИЯ

А.Д. Цаладонов, С.А. Биран, А.В. Короткевич
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В данной работе рассмотрены перспективы применения пленок пористого анодного оксида алюминия для изготовления МЭМС на его основе. Проведены исследования коэффициента использования алюминия в процессе анодирования на алюминиевых подложках различного состава. Предложены методы для уменьшения бокового роста анодного оксида алюминия в процессе локального анодирования.
Ключевые слова: пористый оксид алюминия, анодирование, МЭМС.

SENSITIVE MEMBRANE ELEMENTS BASED ON POROUS ALUMINUM OXIDE FILMS

A.D. Tsaladonov, S.A. Biran, A.V. Korotkevich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This work explores the prospects of using porous anodic aluminum oxide (AAO) films for the fabrication of AAO-based MEMS. Studies were conducted on the aluminum utilization coefficient during anodization on aluminum substrates of varying composition. Methods for reducing lateral growth of anodic aluminum oxide during localized anodization are proposed.
Keywords: porous aluminum oxide, anodization, MEMS.

Введение

В настоящее время технологии микроэлектромеханических систем (МЭМС) активно развиваются и находят применение в различных областях, в том числе и в системах защиты информации. Одним из перспективных материалов для создания МЭМС является анодный оксид алюминия (АОА). Объемные структуры из пористого анодного оксида алюминия находят широкое применение в МЭМС за счет механической стойкости и возможности контроля линейных размеров данных структур в процессе производства. Эти характеристики делают оксид алюминия подходящей основой для разработки сенсоров, индукторов, МЭМС-конденсаторов и других компонентов, используемых в технических средствах, которые обеспечивают защиту информации.

На основе пленок анодного оксида алюминия изготавливают термостойкие мембраны для применения в термокаталитических газовых сенсорах [1], гибкие нанопористые комбинационные мембраны с ячеистой структурой [2], а также нанопористый анодный оксид алюминия подходит для изготовления чувствительных элементов кольцевого гироскопа [3].

Чувствительность мембран на основе пористого оксида алюминия определяется механическими свойствами оксида, которые можно варьировать в процессе анодирования. Для получения объемных элементов МЭМС на основе пленок АОА с заданной вертикальной геометрией необходимо точно знать параметры объемного роста пористого анодного оксида алюминия (такие как коэффициент объемного роста оксида и коэффициент использования алюминия), на которые влияет чистота материала подложки, состав элеткролита, напряжение формовки и другие параметры процесса анодирования. Также при проведении локального анодирования через

фоторезистивную маску наблюдается процесс бового роста оксида, что приводит к искажению горизонтальных расмеров объемной структуры. Для уменьшения величины бокового роста необходимо улучшать качество маскирующих покрытий при вроедении операции локального анодирования.

Основная часть

Исследование объемного роста оксида алюминия в процессе анодирования проводили на алюминиевых подложках марок: Al98Si2, A0H, AlMg2. На первом этапе с поверхности подложек удаляли органические загрязнения и производили травление в течение 15 мин в 10%-м растворе NaOH. После улучшения качества поверхности подложки осветляли в азотной кислоте. Анодирование проводили в специализированной ванне с постоянным перемешивание электролита для обеспечения доступа свежего электролита к подложке, что приводит к ускорению процесса роста анодного оксида. Температура в ванне поддерживали на одном уровне за счет охлаждения проточной водой и нагрева с помощью термонагревателя. Перед проведением анодирования толщину образцов измеряли с помощью микрометра. Анодирование проводили в 4%-м растворе щавелевой кислоты в гальваностатическом режиме при постоянной плотности тока 20 мА/см^2. Время анодирования варьировали от 1 до 6 часов для получения образцов с различной толщиной анодного оксида (рис. 1).

Рис. 1. Образцы из алюминия марки A0H после 1, 2 ,3 и 4 часов анодирования соответственно
Fig. 1. Samples of aluminum grade A0N after 1, 2, 3 and 4 hours of anodizing, respectively.

После анодирования повторно измеряли толщину образцов. Травление анодного оксида алюминия проводили в селективном травителе на основе ортофосфорной кислоты и хромового ангидрида. Время травления составило 7 минут при температуре травителя 80 °C. После удаления оксида снова измеряли образец для расчета толщины полученной оксидной пленки.

Полученные в процессе проведения исследования результаты приведены в таблице.

Из полученных данных рассчитывали коэффициент использования алюминия k_{Al} с применением формулы: $h_{Al} = k_{Al} \cdot J_a \cdot t$, где h_{Al} – толщина алюминия, «израсходованного» в процессе анодирования, J_a – плотность тока анодирования, мА/см^2, t – время анодирования, мин.

Параметры объемного роста оксидных пленок
Parameters of volumetric growth of oxide films

№	Тип алюминия	Толщина образца, мкм	Время анодирования, мин	Толщина образца после анодирования, мкм	Толщина образцов после снятие оксида, мкм	Толщина оксида, мкм	Использованный алюминий, мкм
1.	Al98Si2	280	60	308	233	37,5	23,5
2.	Al98Si2	280	120	320	185	67,5	47,5
3.	Al98Si2	280	180	340	135	102,5	72,5
4.	Al98Si2	280	240	352	110	121	85
5.	Al98Si2	280	300	364	94	135	93
6.	Al98Si2	280	360	373	73	150	103,5
7.	А0Н	900	60	920	860	30	20
8.	А0Н	900	120	942	820	61	40
9.	А0Н	900	180	960	774	92	63
10.	А0Н	900	240	970	746	112	77
11.	А0Н	900	300	983	731	126	84,5
12.	А0Н	900	360	992	712	140	94
13.	AlMg2	1920	60	1950	1893	30	13,5
14.	AlMg2	1920	120	1970	1865	50	27,5
15.	AlMg2	1920	180	1990	1835	75	42,5
16.	AlMg2	1920	240	2014	1800	107	60
17.	AlMg2	1920	300	2030	1784	123	68
18.	AlMg2	1920	360	2042	1770	136	75

По результатам измерений в процессе исследования и данным, полученным в результате расчетов, был построен график зависимости коэффициента использования алюминия от толщины выращенного пористого анодного оксида (рис. 2). Установлено, что по достижении толщины около 100 мкм коэффициент использования алюминия начинает уменьшаться на всех типах подложек. В процессе роста оксидной пленки от 38 мкм до 150 мкм на подложках алюминия с добавлением примеси кремния коэффициент использования алюминия уменьшился с 0,019 до 0,014; на подложках без добавления примесей при росте оксидной пленки от 30 мкм до 140 мкм – с 0,016 до 0, 013; на подложках с добавлением примеси магния при росте оксидной пленки от 30 мкм до 136 мкм также уменьшился с 0,012 до 0, 011.

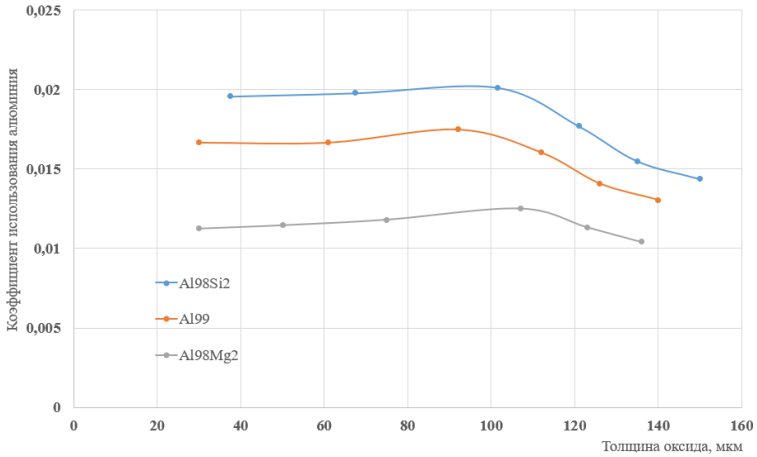
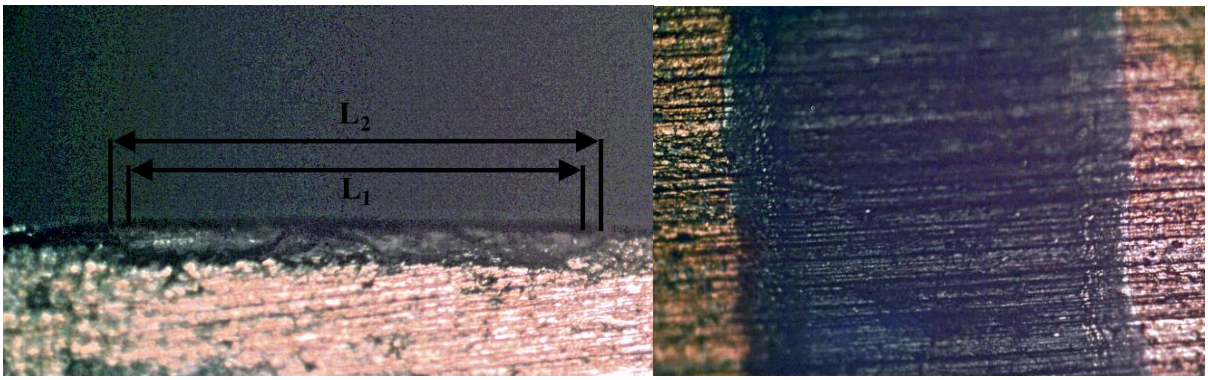


Рис. 2. График зависимости коэффициента использования алюминия от толщины выращенного оксида алюминия
Fig. 2. Graph of the dependence of the aluminum utilization coefficient on the thickness of the grown aluminum oxide

Исследование бокового роста при локальном анодировании алюминия через фоторезистивную маску проводили на подложках из алюминия размером 60×48 мм. На поверхности подложке формировали фоторезистивную маску. Открытыми оставляли полоски алюминия длинной 5 см и шириной от 1 до 5 мм. Анодирование проводили в электролите на основе щавелевой кислоты в гальваностатическом режиме при постоянной плотности тока 20 мА/см^2.

После анодирования для исследования образцов под микроскопом, подложку разрезали, а срез шлифовали и полировали. Исследование проводили на оптическом микроскопе при стократном увеличении (рис. 3): измеряли ширину окна для локального анодирования L_1 и ширину оксидной пленки после анодирования L_2.



a *b*

Рис. 3. Локальное анодирование алюминия через фоторезистивную маску: *a* – в разрезе, *b* – вид сверху
Fig. 3. Local anodization of aluminum through a photoresistive mask: *a* – sectional view, *b* – top view

При проведении исследований установлено, что при использовании маски из фоторезиста при толщине оксида 70 мкм боковой уход составил около 40 мкм. Для устранения бокового ухода использовали комбинацию из фоторезистивной маски и пористого анодного оксида алюминия толщиной 5–10 мкм, что позволило снизить боковой рост в процессе локального анодирования до 40 % от толщины оксида.

Заключение

При выполнении научных исследований показана возможность применения пленок пористого анодного оксида алюминия для изготовления мембранных чувствительных элементов МЭМС. Установлено, при достижении пленкой оксида алюминия толщины 100 мкм в процессе анодирования коэффициент использования алюминия начинает снижаться при дальнейшем росте на всех типах исследованных подложек. Так же установлено, что использование комбинированной маски для локального анодирования позволяет уменьшить боковой рост оксида алюминия до 40 % от толщины полученного оксида.

Список использованных источников

1. Патент RU2242271C1, 20.12.2004.
2. Патент RU2545887C2, 23.10.2012.
3. Белогуров Е.А., Горох Г.Г., Таратын И.А., Хатько В.В. (2013) Чувствительный элемент кольцевого гироскопа на основе нанопористого анодного оксида алюминия. *Нано- и микросистемная техника. (7), 16-19.*

References

1. Patent RU2242271C1, 20.12.2004.
2. Patent RU2545887C2, 23.10.2012.
3. Belogurov, E.A., Gorokh, G.G., Taratyn, I.A., & Khatko, V.V. (2013). Sensitive element of a ring gyroscope based on nanoporous anodic aluminum oxide. *Nano- and Microsystems Technology*, (7), 16-19.

Сведения об авторах

Цаладонов А.Д., магистрант кафедры МНЭ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Биран С.А., старший преподаватель кафедры МНЭ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», biran@bsuir.by.
Короткевич А.В., канд. техн. наук, доцент, доцент кафедры МНЭ, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», korotkevich@bsuir.by.

Information about the authors

Tsaladonov A.D., master's student MNE Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics".
Biran S.A., senior lecture MNE Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", biran@bsuir.by.
Korotkevich A.V., Cand. Sci. (Tech.), Associate Professor, Associate Professor MNE Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", korotkevich@bsuir.by.

УДК 004.056.5

ПРИНЦИПЫ КРИПТОГРАФИИ И МЕТОДЫ КРИПТОАНАЛИЗА В СОВРЕМЕННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

М.А. Чарыева
Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. Данная работа посвящена основам криптографии и криптоанализа, а также их применению для защиты информации в современных цифровых системах. В первой части рассматриваются основные понятия криптографии, включая цифровые подписи и криптографические хэш-функции, которые играют ключевую роль в обеспечении безопасности данных. Особое внимание уделяется алгоритмам цифровых подписей и методам создания хэш-значений, обеспечивающим целостность и подлинность сообщений. Вторая часть работы фокусируется на криптоанализе и различных типах атак на криптосистемы, таких как атака с подставкой, атака с использованием таймера и атака с знанием зашифрованного текста. Описываются способы защиты от этих атак, а также примеры использования криптографических методов в реальных приложениях, таких как электронные подписи и системы аутентификации. Работа направлена на освещение теоретических основ криптографии и практических методов защиты информации, актуальных в условиях современного цифрового мира.
Ключевые слова: цифровые подписи; криптоанализ; криптосистемы; атака.

PRINCIPLES OF CRYPTOGRAPHY AND METHODS OF CRYPTOANALYSIS IN MODERN SECURITY SYSTEMS

M.A. Charyyeva
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. This work is dedicated to the fundamentals of cryptography and cryptanalysis, as well as their application for information protection in modern digital systems. The first part discusses the basic concepts of cryptography, including digital signatures and cryptographic hash functions, which play a key role in ensuring data security. Special attention is given to digital signature algorithms and methods of creating hash values, which ensure the integrity and authenticity of messages. The second part of the work focuses on cryptanalysis and various types of attacks on cryptosystems, such as man-in-the-middle attacks, timing attacks, and ciphertext-only attacks. Methods of defense against these attacks are described, as well as examples of using cryptographic methods in real applications, such as digital signatures and authentication systems. The work aims to highlight

the theoretical foundations of cryptography and practical methods of information protection relevant in the modern digital world.
Keywords: digital signatures; cryptanalysis; cryptosystems; attack.

Введение

Криптография – это наука о том, как обеспечить секретность сообщения. Криптоанализ – это наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики.

Криптография покрывает все практические аспекты секретного обмена сообщениями, включая аутенфикацию, цифровые подписи, электронные деньги и многое другое. Криптология - это раздел математики, изучающий математические основы криптографических методов.

Цифровые подписи

Некоторые из асимметричных алгоритмов могут использоваться для генерирования цифровой подписи. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления штампа времени (timestamp) на документах: сторона, которой мы доверяем, подписывает документ со штампом времени с помошью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения (сертификации – to certify) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим a-priori, что ему можно доверять). В централизованной инфраструктуре ключей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агенства; их также называют сертификационными агенствами - certification authorities). В распределенной инфраструктуре нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название сети доверия (web of trust) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый дайджест (message digest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или

иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA.

Криптографические хэш-функции

Криптографические хэш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хэш-функции отображают сообщение в имеющее фиксированный размер хэш-значение (hash value) таким образом, что все множество возможных сообщений распределяется равномерно по множеству хэш-значений. При этом криптографическая хэш-функция делает это таким образом, что практически невозможно подогнать документ к заданному хэш-значению.

Криптографические хэш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество собщений, которые когда-либо будут существовать в мире.

Много хороших криптографических хэш-функций доступно бесплатно. Широко известные включают MD5 и SHA.

Криптоанализ и атаки на криптосистемы

Криптоанализ – это наука о дешифровке закодированных сообщений не зная ключей. Имеется много криптоаналитических подходов. Некоторые из наиболее важных для разработчиков приведены ниже.

Атака со знанием лишь шифрованного текста (ciphertext-only attack). Это ситуация, когда атакующий не знает ничего о содержании сообщения, и ему приходтся работать лишь с самим шифрованным текстом. На практике, часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказумой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атака со знанием содержимого шифровки (known-plaintext attack): Атакующий знает или может угадать содержимое всего или части зашифрованного текста. Задача заключается в расшифровке остального сообщения. Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атака с заданным текстом (chosen-plaintext attack): Атакующий имеет возможнот получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования и, в частности, RSA, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

Атака с подставкой (Man-in-the-middle attack): Атака направлена на обмен шифрованными сообщениями и, в особенности, на протокол обмена ключами. Идея заключается в том, что когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана, Diffie-Hellman), противник внедряется между ними на линии обмена сообщениями. Далее противник

выдает каждой стороне свои ключи. В результате, каждая из сторон будет иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Одним из способов предотвратить такой тип атак заключается в том, что стороны при обмене ключами вычисляют криптографическую хэш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посылают подпись другой стороне. Получатель проверит подпись и то, что значение хэш-функции совпадает с вычисленным значением. Такой метод используется, в частности, в системе Фотурис (Photuris).

Атака с помощью таймера (timing attack): Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в стенень по модулю целого числа. Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

Имеется множество других криптографических атак и криптоаналитических подходов.

Заключение

На сегодняшний день криптоанализ играет ключевую роль в обеспечении безопасности данных. С развитием технологий и криптографических алгоритмов, таких как RSA и AES, появляются новые методы взлома и атаки. Криптоанализ помогает выявлять уязвимости в системах и улучшать их защиту. Современные криптографические исследования направлены на создание более устойчивых алгоритмов, способных противостоять сложным методам анализа и атакам, обеспечивая высокую степень безопасности в цифровом мире.

Список использованных источников

1. Кауфман, Ч. "Криптография и безопасность компьютерных систем". – М.: Издательство «Наука», 2018.
2. Шиффман, Д. "Введение в криптографию". – М.: Издательство «Речи», 2017.
3. Меркель, П. «Цифровые подписи и защита данных». – М.: Издательство «Диалектика», 2015.
4. Цицилин, М. В., Кузнецов, В. В. "Современные методы криптографического анализа". – СПб.: Издательство «Питер», 2020.

References

1. Kaufman, C. “Cryptography and Computer System Security.” – Moscow: “Nauka” Publishing House, 2018.
2. Shiffman, D. "Introduction to Cryptography." – Moscow: “Rechi” Publishing House, 2017.
3. Merkel, P. “Digital Signatures and Data Protection.” – Moscow: “Dialektika” Publishing House, 2015.
4. Ttsitsilin, M. V., Kuznetsov, V. V. “Modern Methods of Cryptographic Analysis.” – St. Petersburg: “Piter” Publishing House, 2020.

Сведения об авторах

Чарыева М.А., преподаватель, Государственный энергетический институт Туркменистана, annageldievamaysa@gmail.com.

Information about the authors

Charyyeva M., Teacher, The State Energy Institute of Turkmenistan, annageldievamaysa@gmail.com.

УДК 004.81

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АДАПТИВНОГО ОБНАРУЖЕНИЯ АНОМАЛИЙ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.Э. Чернявский, А.В. Ситников, М.В. Романюк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Аннотация. В условиях растущих киберугроз традиционные методы защиты, основанные на сигнатурном анализе, оказываются недостаточно эффективными. В данной статье рассматривается применение методов искусственного интеллекта (ИИ) для обнаружения аномалий в кибербезопасности. Описываются этапы обработки данных, выбор алгоритмов машинного обучения и их интеграция в системы мониторинга. Проведен сравнительный анализ эффективности ИИ-моделей на основе датасета NSL-KDD. Результаты исследования показывают, что алгоритмы ИИ обеспечивают более точное и адаптивное выявление угроз по сравнению с традиционными методами.
Ключевые слова: Обнаружение аномалий, кибербезопасность, машинное обучение, мониторинг в реальном времени, выявление угроз.

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR ADAPTIVE ANOMALY DETECTION IN INFORMATION SECURITY SYSTEMS

K.E. Chernyavskiy, A.V. Sitnikov, M.V. Romanuyk
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. With the increasing number of cyber threats, traditional security methods based on signature analysis are becoming insufficient. This paper explores the use of artificial intelligence (AI) techniques for anomaly detection in cybersecurity. It describes data processing stages, machine learning algorithm selection, and their integration into monitoring systems. A comparative analysis of AI-based models was conducted using the NSL-KDD dataset. The results demonstrate that AI algorithms provide more accurate and adaptive threat detection compared to traditional approaches.
Keywords: anomaly detection, cybersecurity, machine learning, real-time monitoring, threat detection.

Введение

С развитием цифровых технологий частота и сложность кибератак стремительно растут. Традиционные меры кибербезопасности, основанные на сигнатурном обнаружении угроз, остаются неэффективными перед новыми сложными атаками. Данные методы функционируют в реактивном режиме, идентифицируя угрозы на основе известных сигнатур и шаблонов атак, что затрудняет обнаружение новых и сложных киберугроз, включая эксплойты «нулевого дня» и продвинутые устойчивые угрозы (APT).

Одним из наиболее перспективных решений является обнаружение аномалий на основе ИИ. Машинное обучение позволяет анализировать большие объемы данных в реальном времени, выявляя отклонения от нормального поведения. Этот проактивный подход значительно повышает эффективность обнаружения угроз, а также позволяет моделям адаптироваться к изменяющимся условиям.

Данная работа рассматривает архитектуру, алгоритмы и эффективность ИИ-систем для обнаружения аномалий. Анализируется процесс предварительной обработки данных, извлечения признаков и применения различных методов машинного обучения, таких как нейронные сети, опорные векторные машины и алгоритмы кластеризации. Также затрагиваются практические аспекты, включая вычислительную нагрузку, потребность в больших наборах данных и возможные уязвимости.

Предлагаемая методология

Методология обнаружения аномалий на основе ИИ включает несколько этапов:

1. Сбор данных. Агрегирование сетевого трафика, системных логов, активности пользователей и данных об угрозах, включая журналы безопасности, файлы системных событий и мониторинг поведения пользователей. Важно учитывать разнородность данных, их объем и необходимость быстрой обработки.

2. Предварительная обработка. Очистка данных, нормализация и сегментация потоков информации. Данные могут содержать шум, дубликаты и аномалии, не относящиеся к угрозам. Используются методы нормализации (min-max, Z-score) и устранения выбросов.

3. Извлечение признаков. Анализ статистических метрик, временных рядов и специфических параметров поведения. Применяются методы временного анализа для выявления паттернов поведения. Рассматриваются статистические показатели, такие как среднее значение, медиана и стандартное отклонение.

4. Выбор и обучение модели. Использование различных алгоритмов (нейронные сети, SVM, кластеризация) для точного обнаружения аномалий. Нейронные сети (LSTM, CNN) позволяют анализировать сложные временные зависимости. Опорные векторные машины (SVM) эффективны для бинарной классификации угроз. Кластеризационные алгоритмы (K-Means, DBSCAN) помогают выявлять отклонения без предварительной разметки данных.

5. Обнаружение в реальном времени. Применение потоковых технологий (Kafka, Spark) и адаптивных моделей для мгновенного реагирования на угрозы. Использование потоковых систем позволяет анализировать данные в режиме реального времени. Модели обновляются динамически, снижая вероятность пропуска новых угроз.

6. Оценка эффективности. Анализ точности, полноты, F1-меры, AUC-ROC и уровня ложных срабатываний. Применяются методы кросс-валидации и сравнения с эталонными моделями. Важное значение имеет баланс между точностью и ложными срабатываниями.

7. Развертывание. Интеграция с существующими системами IDS/IPS, настройка оповещений и обеспечение постоянного мониторинга. Развертывание требует масштабируемой инфраструктуры и интеграции с SIEM-системами. Важно учитывать требования по отказоустойчивости и скорости обработки данных.

Сравнительный анализ

Был проведен эксперимент с анализом сетевого трафика на основе датасета NSL-KDD, включающего как нормальные, так и аномальные данные. Оценивалась точность обнаружения, скорость работы моделей и уровень ложных срабатываний. Анализ показал, что методы ИИ превосходят традиционные подходы по ряду критериев (таблица).

Дополнительно проведено тестирование с использованием реальных логов из корпоративной сети. Результаты показали, что комбинированные методы (гибридные модели ИИ) позволяют уменьшить количество ложных срабатываний на 30% по сравнению с традиционными системами обнаружения вторжений (IDS).

Сравнительный анализ
Comparative Summary

Критерий	Традиционные методы	Методы, основанные на ИИ
Точность обнаружения	Высокая для известных угроз	Высокая как для известных, так и для неизвестных угроз
Обработка в реальном времени	Высокая	Зависит от метода (высокая с потоковой обработкой, низкая с пакетным обучением)
Адаптивность	Низкая	Высокая (особенно для методов без учителя и полуобучения)
Вычислительная эффективность	Высокая	Зависит от модели (эффективна для легковесных моделей, высокая для сложных)
Устойчивость к атакам	Низкая	Улучшается (с помощью обучения с учителем и надежных методов)

Заключение

Системы обнаружения аномалий, основанные на ИИ, представляют собой трансформационное достижение в области реальной кибербезопасности. Используя передовые методы машинного обучения, эти системы предлагают улучшенную точность обнаружения, адаптивность и возможности обработки в реальном времени, что делает их незаменимыми инструментами в непрерывной борьбе с киберугрозами.

Решение существующих проблем и ограничений через продолжение исследований и инновации будет способствовать дальнейшему укреплению роли ИИ в создании надежных и устойчивых рамок кибербезопасности. По мере того, как ландшафт угроз продолжает эволюционировать, решения, основанные на ИИ, будут необходимы для защиты цифровых инфраструктур и обеспечения безопасности чувствительной информации.

Кроме того, интеграция ИИ с традиционными методами киберзащиты позволяет создать многослойную оборону, способную эффективно реагировать на новые и сложные угрозы. Комбинируя поведенческий анализ, обработку больших данных и автоматизированное реагирование, такие системы обеспечивают проактивное обнаружение атак, минимизируя риски и сокращая время на устранение инцидентов.

Список использованных источников / References

1. Bishop C. M., Goodfellow I., Bengio Y., Courville A. (2006) Pattern Recognition and Machine Learning. Germany, Springer.

2. Goodfellow I., Bengio Y., Courville A. (2016) Deep Learning. Germany, Springer.

3. Chandola V., Banerjee A., Kumar V. (2009) Anomaly Detection: A Survey. ACM Computing Surveys, Vol. 41(3), p. 1-58.

4. Sommer R., Paxson V. (2010) Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, p. 305-316.

5. Tavallaee M., Bagheri E., Lu W., Ghorbani A. (2009) A Detailed Analysis of the KDD CUP 99 Data Set. IEEE Symposium on Computational Intelligence for Security and Defense Applications.

6. Xu, L., & Shelton, C. R. (2010). Network anomaly detection based on hidden Markov model. Computers & Security, 29(4), 492-507.

7. Bifet, A., & Kirkby, R. (2009). Data stream mining: A practical approach. AK Peters/CRC Press.

Сведения об авторах

Чернявский К.Э., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kir180920032003@gmail.com.
Ситников А.В., инженер-программист, Отдел информационных технологий, Центр информатизации и инновационных разработок, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.sitnikov@bsuir.by.
Романюк М.В., магистр, ассистент кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», romanuk@bsuir.by.

Information about the authors

Cherniavskiy K., student of the Department of Electronic Computing Machines, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kir180920032003@gmail.com.
Sitnikov A., software engineer, Information Technology Department, Center for Informatization and Innovative Developments, Educational Institution "Belarusian State University of Informatics and Radioelectronics"., a.sitnikov@bsuir.by.
Romanuyk M., Master, Assistant at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", romanuk@bsuir.by.

УДК 005.8

АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДА ЦВЕТОВЫХ КООРДИНАТ HSL

Н.П. Шутько
Белорусский государственный технологический университет, Минск, Беларусь

Аннотация. Современные технологии требуют надежных методов защиты авторских прав в цифровом пространстве, где легкость копирования контента ставит интеллектуальную собственность под угрозу. Статья рассматривает использование цветовых координат HSL (Hue, Saturation, Lightness) как эффективный инструмент для скрытия и передачи авторской информации. HSL предлагает интуитивное восприятие цвета и позволяет внедрять данные в оттенки, насыщенность и яркость, что делает изменения незаметными. Проведенный сравнительный анализ построенных гистограмм изображений подтверждает незначительное различие цветовых характеристик, указывая на эффективность предложенного метода. Результаты подчеркивают перспективность HSL для защиты авторских прав в цифровом контенте.
Ключевые слова: авторское право; цифровое пространство; hsl (оттенок, насыщенность, яркость); интеллектуальная собственность; скрытие данных; авторская информация; цветовые координаты; анализ гистограмм; обработка изображений; стеганография.

ANALYSIS OF THE EFFECTIVENESS OF HSL COLOR COORDINATE METHOD

N.P. Shutko
Belarusian State Technological University, Minsk, Belarus

Abstract. Modern technologies require reliable methods for protecting copyright in the digital space, where the ease of copying content poses a threat to intellectual property. This article examines the use of HSL (Hue, Saturation, Lightness) color coordinates as an effective tool for hiding and transmitting authorial information. HSL offers an intuitive perception of color and allows data to be embedded in hue, saturation, and lightness, making changes unnoticeable. The comparative analysis of constructed image histograms confirms minor differences in color characteristics, indicating the effectiveness of the proposed method. The results highlight the potential of HSL for copyright protection in digital content.
Keywords: copyright; digital space; hsl (hue, saturation, lightness); intellectual property; data hiding; authorial information; color coordinates; histogram analysis; image processing; steganography.

Введение

Современные технологии требуют эффективных методов защиты авторских прав в цифровом пространстве. С увеличением объемов контента, доступного в сети, и легкостью его копирования, защита интеллектуальной собственности становится все

более актуальной. Цветовые координаты HSL (Hue, Saturation, Lightness) представляют собой перспективный инструмент для скрытия и передачи информации.

Основная часть

Цветовая модель HSL отличается от других моделей, таких как RGB и CMYK, тем, что она более интуитивно понятна для восприятия человеком.

Первоначально необходимо определить, что такое HSL. Это цветовая модель, которая описывает цвета в терминах Hue (оттенок), Saturation (насыщенность) и Lightness (яркость). Для общего понимания вкратце рассмотрим каждую из этих составляющих.

Оттенок (Hue): определяет цвет и измеряется в градусах от 0 до 360. Насыщенность (Saturation): указывает на интенсивность цвета, где 0% означает серый цвет, а 100% − максимально насыщенный цвет. Яркость (Lightness): измеряет светлоту цвета, где 0% − черный, а 100% − белый.

Преимущества HSL по сравнению с другими цветовыми моделями заключаются в том, что она позволяет более эффективно манипулировать визуальными элементами без значительных потерь в восприятии.

Ранее в [1] был предложен новый метод текстовой стеганографии, который использует HSL в контексте авторских прав.

Метод внедрения информации в цветовые координаты HSL включает несколько этапов:

– скрытие данных: информация может быть скрыта в оттенках, насыщенности и яркости. Например, небольшие изменения в насыщенности могут не быть заметны для глаза, но могут содержать данные о праве собственности;

– визуальные элементы, такие как логотипы или знаки водяных знаков, можно закодировать с использованием HSL, добавляя метаданные о праве собственности.

Авторская информации, скрытая с использованием HSL, может быть внедрена в каждый пиксель изображения, изменяя его цветовые характеристики. Для извлечения информации могут использоваться алгоритмы, которые анализируют изменения в цветах, позволяя восстановить оригинальные данные.

Метод, основанный на скрытии секретной информации за счет модификации параметров HSL символов текста, предлагает уникальное сочетание простоты внедрения и устойчивости к изменениям, что делает его привлекательным для использования в цифровом контенте.

Для исследования эффективности разработанного метода предлагается проводить сравнительный анализ изображений исходного текста-контейнера и стегоконтейнера, который содержит в себе осажденную секретную информацию. Проводить оценку предлагается с помощью гистограмм.

Гистограмма – это графическое представление распределения числовых данных. На гистограмме можно увидеть:

– частотное распределение. Высота столбиков показывает, сколько значений попадает в каждую интервал;

– форму распределения. Можно определить, нормально ли распределены данные, есть ли пики, провалы или асимметрия;

– моду. Наиболее часто встречающееся значение или значения данных;

– разброс данных. Ширина столбиков и их расположение могут показать, насколько данные разбросаны или сгруппированы;

– выбросы. Аномально высокие или низкие значения, которые выделяются на фоне остальных.

Гистограммы полезны для визуального анализа данных и выявления закономерностей.

Построить гистограмму можно с помощью различный программных средств. В рамках данного исследования была использована программа Photoshop.

Для построения гистограммы, в первую очередь, были выполнены снимки экрана, на которых были зафиксированы исходный контейнер (рис. 1) и стегоконтейнер, содержащий осажденную информацию (рис. 2).

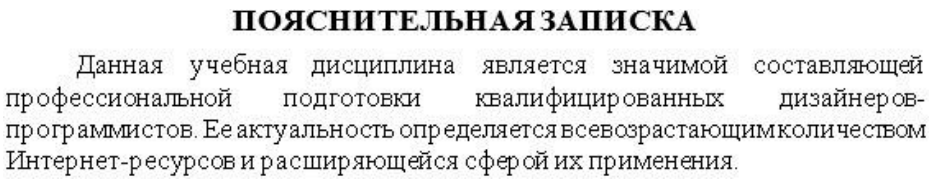


Рис. 1. Изображение контейнера
Fig. 1. Image of container

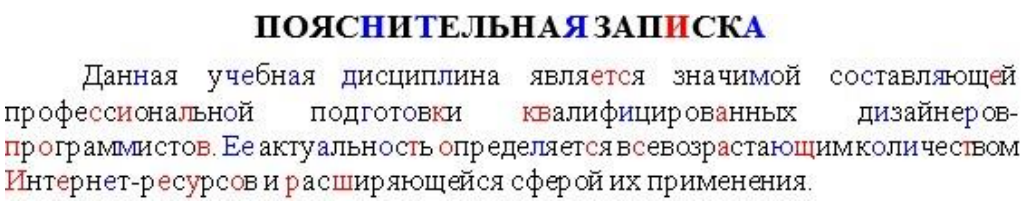
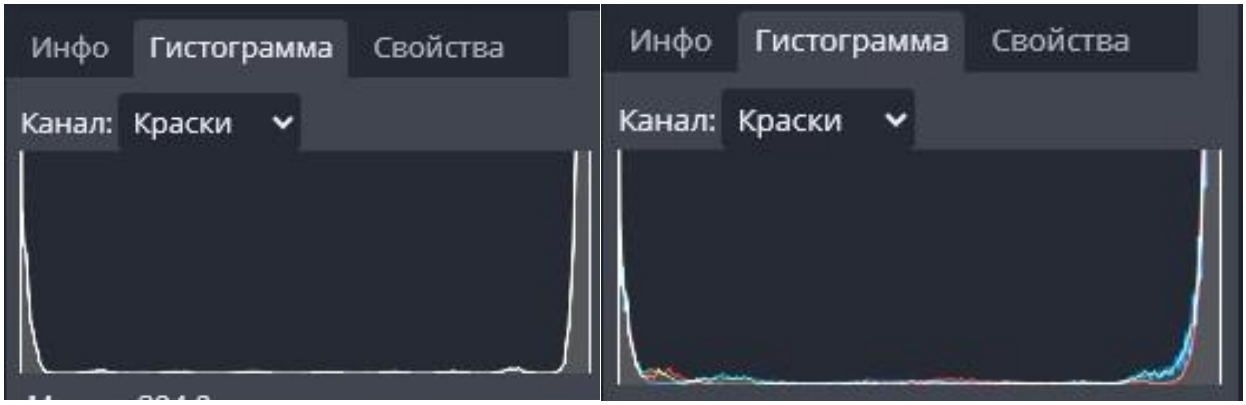


Рис. 2. Изображение стегоконтейнера
Fig. 2. Image of stegocontainer

Ввиду специфики работы с гистограммами в программе Adobe Photoshop, сравнение проводилось как общих гистограмм, так и отдельных цветовых каналов: красного, зеленого и синего.

Результаты показали, что по красному, зеленому и синему каналам изображения контейнера различий между гистограммами не наблюдалось, что свидетельствует о схожести цветовых характеристик в этих диапазонах (это обусловлено тем, что цвет текста в исходном документе – черный). Однако общая гистограмма демонстрировала некоторые отличия (рис. 3).



a *b*

Рис. 3. Гистограммы изображений: *a* – контейнера; *b* – стегосообщения
Fig. 3. Image Histograms: *a* – container; *b* – stegocontainer

Полученные данные указывают на различия в распределении яркости и контраста между анализируемыми изображениями, что может косвенно указывать на наличие скрытой информации в документе. Однако различия между гистограммами не являются существенными, что подтверждает эффективность выбранного метода. Это позволяет считать подход достаточно надежным для осаждения секретной информации.

Заключение

Использование цветовых координат HSL для защиты и передачи авторской информации является многообещающим направлением. Устойчивость к различным атакам и простота внедрения делают HSL актуальным инструментом в цифровом мире. Важно продолжать исследование в этой области, чтобы адаптироваться к меняющимся условиям и требованиям защиты авторских прав.

Список использованных источников

1. Шутько, Н.П. (2022) Использование цветовых координат HSL для защиты и передачи авторской информации. *Информационные технологии: материалы 86-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов*. 125-128.

References

1. Shutko, N.P. (2022). Use of HSL Color Coordinates for Protection and Transmission of Authorial Information. Information Technologies: Proceedings of the 86th Scientific and Technical Conference of Faculty Members, Researchers, and Graduate Students. 125-128.

Сведения об авторе

Шутько Н. П., канд. техн. наук, доц., доц., Белорусский государственный технологический университет, shutko_bstu@mail.ru.

Information about the author

Shutko N., Cand. Sci. (Tech.), Associate Professor, Associate Professor, Belarusian State Technological University, shutko_bstu@mail.ru.

УДК 004.056.53

НЕДОСТАТОК КОНТРОЛЯ ДОСТУПА КАК ОДНА ИЗ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ

К.Д. Янович, Д.С. Лапчук
Гомельский государственный университет имени Франциска Скорины, Гомель, Беларусь

Аннотация. В данной работе рассматривается одна из актуальных и наиболее распространенных тенденций в области эксплуатации уязвимостей веб-приложений, которая входит в список OWASP Top Ten и находится на первом месте (A01). Исследование фокусируется на недостатках контроля доступа, которые позволяют неавторизованным пользователям получать доступ к конфиденциальной информации. Анализируются основные причины возникновения таких уязвимостей, включая неправильную настройку списков контроля доступа и отсутствие многофакторной аутентификации. Предлагаются методы защиты, такие как регулярный аудит и использование специализированных инструментов для тестирования безопасности [1].

Ключевые слова: веб-приложения; информационная безопасность; контроль доступа; уязвимости; аутентификация; авторизация; многофакторная аутентификация (MFA); шифрование; Netsparker; Burp Suite.

LACK OF ACCESS CONTROL AS ONE OF THE CURRENT VULNERABILITIES OF WEB APPLICATIONS

K.D. Yanovich, D.S. Lapchuk
Francisk Scorina Gomel State University, Gomel, Belarus

Abstract. This work examines one of the current and most prevalent trends in web application vulnerability exploitation, which is on the OWASP Top Ten list and is ranked number one (A01). The study focuses on access control flaws that allow unauthorized users to access sensitive information. The main causes of such vulnerabilities are analyzed, including improper configuration of access control lists and lack of multi-factor authentication. Protection methods, such as regular auditing and the use of specialized security testing tools, are proposed.
Keywords: web applications; information security; access control; vulnerabilities; authentication; authorization; multi-factor authentication (MFA); encryption; Netsparker; Burp suite

Введение

Веб-приложения предоставляют пользователям возможность интерактивного взаимодействия с контентом в интернете, что делает их важным элементом современной цифровой инфраструктуры. Однако, в силу своей открытости и доступности, веб-приложения становятся объектом различных кибератак, что может привести к утечке конфиденциальной информации и персональных данных. Недостаточная реализация решений по информационной безопасности может сделать веб-приложения уязвимыми для атак со стороны злоумышленников. Существует множество уязвимостей, которые могут быть использованы для компрометации веб-приложений. Одной из наиболее распространенных уязвимостей является недостаток контроля доступа.

Основная часть

Недостатки контроля доступа – уязвимости, связанные с управлением доступа и возникающие, когда приложение неправильно ограничивает доступ к данным или функциям. Недостатки контроля доступа возникают, когда приложение не обеспечивает надлежащую проверку прав доступа пользователей к ресурсам и функционалу. Это может позволить неавторизованным пользователям получить доступ к защищенным данным или выполнять действия, которые должны быть доступны только определенным категориям пользователей.

Например, если пользователь с низким уровнем доступа может получить доступ к административным функциям. Данные уязвимости могут принимать различные формы.

1. Применение небезопасных или предсказуемых паролей. Использование небезопасных или предсказуемых паролей создает значительные риски для безопасности системы. Злоумышленники могут легко подобрать такие пароли с помощью различных методов, что позволяет им получить несанкционированный доступ к конфиденциальной информации и данным пользователей.

2. Неправильно настроенные списки контроля доступа. Неправильная настройка списков контроля доступа может привести к серьезным уязвимостям в системе безопасности. Это происходит, когда права доступа пользователей не соответствуют их ролям и обязанностям, что позволяет неавторизованным пользователям получать доступ к конфиденциальной информации или выполнять действия, которые должны быть ограничены. Такие ошибки в конфигурации могут быть использованы злоумышленниками для получения несанкционированного доступа к ресурсам системы, что ставит под угрозу безопасность данных и целостность информации.

3. Недостаточные или неправильные разрешения. Недостаточные или неправильные разрешения могут существенно ослабить систему контроля доступа, предоставляя пользователям больше прав, чем необходимо для выполнения их задач. Это может привести к ситуациям, когда неавторизованные пользователи получают доступ к конфиденциальной информации или могут выполнять критические операции, что нарушает принцип минимальных привилегий. Такие ошибки в настройке разрешений создают уязвимости, которые могут быть использованы злоумышленниками для компрометации системы и утраты данных.

4. Отсутствие аудита и мониторинга. Отсутствие аудита и мониторинга может значительно ослабить систему безопасности, так как не позволяет своевременно выявлять и реагировать на потенциальные угрозы и инциденты. Без регулярного аудита невозможно проверить соответствие текущих настроек безопасности установленным политикам и стандартам, что может привести к незамеченным уязвимостям. Мониторинг, в свою очередь, необходим для оперативного обнаружения подозрительной активности и предотвращения несанкционированного доступа. Недостаток этих процессов создает благоприятные условия для злоумышленников, позволяя им эксплуатировать уязвимости без обнаружения.

5. Отсутствие многофакторной аутентификации. Отсутствие многофакторной аутентификации (MFA) создает значительные риски для безопасности системы. MFA добавляет дополнительный уровень защиты, требуя от пользователей подтверждения их личности с помощью второго фактора, такого как SMS-код или приложение-аутентификатор. Без MFA система становится уязвимой для атак, направленных на подбор паролей или фишинг, что позволяет злоумышленникам получить несанкционированный доступ к учетным записям и конфиденциальной информации. Внедрение MFA является критически важным для повышения уровня безопасности и защиты данных пользователей.

Рассмотрим примеры уязвимостей в коде (рис. 1, 2). В коде представленном на рис. 1 метод viewUserProfile используется для отображения информации профиля пользователя. Однако проверка контроля доступа отсутствует, чтобы гарантировать, что пользователь, вызывающий этот метод, имеет право на просмотр профиля. Злоумышленник может воспользоваться этой уязвимостью, передав другой идентификатор пользователя и получив доступ к профилю другого пользователя. Код, представленный на рис. 2, считывает содержимое файла с помощью встроенной в Python open функции. Однако проверка контроля доступа отсутствует, чтобы гарантировать, что пользователь, вызывающий эту функцию, имеет право на чтение файла. Злоумышленник может воспользоваться этой уязвимостью, передав другое имя файла и получив доступ к конфиденциальным данным.

```
public void viewUserProfile(String userId) {
    User user = getUserById(userId);
    if (user != null) {
        System.out.println("User Name: " + user.getName());
        System.out.println("Email Address: " + user.getEmail());
    }
}
```

Рис. 1. Пример уязвимого кода на языке программирования Java
Fig. 1. An example of vulnerable code in the Java programming language

```
def read_file(filename):
with open(filename, 'r') as f:
    contents = f.read()
return contents
```

Рис. 2. Пример уязвимого кода на языке программирования Python
Fig. 2. Example of vulnerable Python programming language code

Рассмотрим основные методы защиты от недостатков контроля доступа. Для предотвращения уязвимости необходимо внедрять строгие политики аутентификации и паролей, включая использование многофакторной аутентификации там, где это возможно. Убедиться, что все учетные записи пользователей имеют соответствующие уровни доступа и разрешения, и регулярно просматривать и обновлять эти разрешения по мере необходимости. Использовать шифрование для защиты конфиденциальных данных, как при передаче, так и в состоянии покоя. Необходимо внедрить средства контроля доступа на каждом уровне вашей инфраструктуры, включая веб-приложения, операционные системы и сетевую инфраструктуру, а также регулярно устанавливать обновления программного обеспечения и исправления ко всем системам и приложениям для устранения известных уязвимостей в системе безопасности.

Для выявления рассматриваемой уязвимости чаще всего используют сканеры уязвимостей. Это инструменты, которые автоматически анализируют системы и программное обеспечение на наличие потенциальных уязвимостей.

На основе отзывов, Netsparker часто упоминается как один из лучших сканеров уязвимостей. Netsparker отмечен за свою точность в обнаружении потенциальных уязвимостей в веб-приложениях и использование автоматизации машинного обучения, что делает его одним из лучших на рынке. Одним из самых популярных является Burp Suite – мощный инструмент для тестирования безопасности веб-приложений, который включает в себя множество функций для анализа и эксплуатации уязвимостей. Опытные пентестеры используют Metasploit – фреймворк для тестирования на проникновение, который включает в себя множество эксплойтов для различных уязвимостей.

Помимо сканеров уязвимостей, существуют различные плагины для браузеров, которые помогают обнаруживать уязвимости и снизить риски кибератак и утечки данных. Наиболее популярными являются:

LiveHTTPHeaders – надстройка Firefox, которая может использоваться для просмотра и изменения HTTP-заголовков, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе заголовков.

EditThisCookie – расширение Chrome, которое можно использовать для редактирования файлов cookie и манипулирования ими, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе файлов cookie.

ModHeader – расширение Chrome, которое можно использовать для изменения заголовков HTTP, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе заголовков.

Использование предоставленных средств обнаружения веб-уязвимостей позволяет своевременно обнаружить недостаток контроля доступа и предотвратить утечку данных.

Заключение

Недостаток контроля доступа является критической уязвимостью в веб-приложениях, занимая первое место в списке OWASP Top Ten. Эта уязвимость может привести к утечке конфиденциальной информации и подрыву доверия пользователей.

Для защиты веб-приложений необходимо внедрять строгие политики аутентификации и авторизации, регулярно проверять и обновлять разрешения пользователей, а также использовать шифрование для защиты данных. Регулярное обновление программного обеспечения также важно для поддержания безопасности.

Инструменты, такие как Netsparker, Burp Suite и Metasploit, помогают выявлять и устранять уязвимости контроля доступа. Плагины для браузера, такие как LiveHTTPHeaders, EditThisCookie и ModHeader, полезны для ручного тестирования.

Таким образом, комплексный подход и использование специализированных инструментов являются ключевыми для обеспечения безопасности веб-приложений.

Список использованных источников

1. Андреева О. TOP10 уязвимостей в веб-приложениях в 2021–2023 годах. [Электронный ресурс] / О. Андреева, Kaspersky Security Services // Securelist by Kaspersky: Исследование. – 2024. – 12 марта. – URL: https://securelist.ru/top-10-web-app-vulnerabilities/109215/. – Дата доступа: 25.02.2025.

Сведения об авторах

Янович К.Д., студентка 2 курса факультета Физики и информационных технологий, специальности «Кибербезопасность», Гомельский государственный университет имени Франциска Скорины, karifox100@gmail.com.
Лапчук Д.С., студент 2 курса факультета Физики и информационных технологий, специальности «Кибербезопасность», Гомельский государственный университет имени Франциска Скорины, Danik_lapchuk@mail.ru.

Information about the authors

Yanovich K.D., 2nd year student of the Faculty of Physics and Information Technologies, major "Cyber Security", Francisk Scorina Gomel State University, karifox100@gmail.com.
Lapchuk D.S., 2nd year student of the Faculty of Physics and Information Technologies, major "Cyber Security", Francisk Scorina Gomel State University, Danik_lapchuk@mail.ru.

УДК 621.311.243

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ СОЛНЕЧНЫХ ПАНЕЛЕЙ

К.С. Дик
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются современные методы и технологии обеспечения безопасности функционирования солнечных панелей. Описаны основные риски и угрозы, связанные с эксплуатацией солнечных электростанций, а также способы их выявления и минимизации. В работе анализируются методы обнаружения аномалий в работе солнечных панелей, включая статистические, метрические, модельные и машинного обучения, что позволяет значительно повысить надежность систем. Приведены примеры практического применения алгоритмов анализа данных для мониторинга и диагностики неисправностей солнечных панелей.
Ключевые слова: солнечная энергетика; безопасность; мониторинг; аномалии; машинное обучение; диагностика; прогнозирование; телеметрия; отказоустойчивость; фотогальванические системы.

ENSURING THE SAFETY OF SOLAR PANEL OPERATION

K.S. Dzik
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article examines modern methods and technologies for ensuring the safety of solar panels. The main risks and threats associated with the operation of solar power plants, as well as methods for their detection and minimization, are described. The paper analyzes methods for detecting anomalies in the operation of solar panels, including statistical, metric, model-based, and machine learning approaches, which significantly enhance system reliability. Examples of practical applications of data analysis algorithms for monitoring and diagnosing solar panel malfunctions are provided.
Keywords: solar energy; safety; monitoring; anomalies; machine learning; diagnostics; forecasting; telemetry; fault tolerance; photovoltaic systems.

Введение

Развитие солнечной энергетики ставит перед исследователями и инженерами задачу повышения надежности и безопасности функционирования солнечных панелей. Нарушение работы панелей может быть вызвано различными факторами, такими как деградация фотоэлементов, затенение, температурные колебания, механические повреждения и другие неблагоприятные условия. Для эффективного обеспечения безопасности солнечных панелей необходимы современные методы анализа данных, которые позволяют своевременно выявлять отклонения в их работе.

Современные системы мониторинга солнечных электростанций используют автоматизированные алгоритмы для обнаружения аномалий и прогнозирования возможных отказов. Эти методы позволяют не только минимизировать потери энергии, но и продлить срок службы оборудования, обеспечивая бесперебойное функционирование всей системы.

Основная часть

1. Методы обнаружения аномалий в работе солнечных панелей. Обнаружение аномалий играет ключевую роль в обеспечении безопасности солнечных электростанций. В данной статье рассматриваются несколько методов выявления неисправностей:

Статистические тесты – анализируют данные на предмет экстремальных значений, устанавливая предельные значения параметров. Однако такие методы требуют нормального распределения данных и не всегда эффективны в условиях высокой изменчивости. Они применяются для начального анализа данных телеметрии, но не всегда выявляют сложные неисправности, связанные с многомерными зависимостями параметров.

Модельные тесты – используют сингулярное разложение (SVD) и анализ главных компонент (PCA) для сравнения матрицы реальных данных с идеальной моделью. Этот подход активно применяется в кибербезопасности, обработке сетевого трафика и временных рядах. В контексте солнечных панелей этот метод позволяет анализировать параметры работы панелей и выявлять отклонения от ожидаемых значений.

Итерационные методы – включают пошаговое удаление подозрительных объектов из n-мерного признакового пространства, но являются ресурсоемкими. Они применяются при обработке больших массивов данных, но требуют значительных вычислительных ресурсов.

Метрические методы – основаны на измерении расстояний в многомерном

пространстве, например, через алгоритмы LOF (local outlier factor), ABOD (angle-based outlier detection) и k-nearest neighbors. Они позволяют находить отклонения в работе солнечных панелей, анализируя поведение отдельных элементов относительно их ближайших соседей по множеству параметров.

Методы машинного обучения – включают алгоритмы Isolation Forest, OneClass SVM и нейронные сети, которые демонстрируют высокую точность обнаружения аномалий в данных телеметрии солнечных панелей. В частности, алгоритм Isolation Forest выделяется своей способностью эффективно изолировать аномальные значения, быстро анализируя данные без необходимости предварительной нормализации.

Прогнозирование временных рядов – осуществляется с помощью алгоритмов ARIMA, SARIMA, LSTM, что позволяет предсказывать изменения в работе панелей на основе исторических данных. Этот подход полезен для долгосрочного мониторинга и предотвращения неожиданных поломок.

2. Современные технологии мониторинга и диагностики. Для обеспечения безопасной эксплуатации солнечных панелей широко применяются цифровые технологии и автоматизированные системы диагностики. Эти технологии позволяют:

– оперативно выявлять аномалии и прогнозировать неисправности;

– автоматически регулировать параметры работы системы в зависимости от погодных условий;

– оптимизировать энергопотребление и сокращать затраты на обслуживание;

– цифровые двойники солнечных панелей позволяют проводить виртуальные тесты и симуляции, выявляя потенциальные слабые места оборудования до их физического проявления; это значительно снижает риск отказов и увеличивает срок службы солнечных батарей.

3. Применение дронов и IoT в мониторинге солнечных панелей. Использование беспилотных летательных аппаратов (дронов) позволяет осуществлять:

– регулярную инспекцию солнечных панелей с использованием инфракрасных камер;

– оценку состояния панелей в реальном времени и выявление перегретых участков;

– мониторинг повреждений и засорений, влияющих на эффективность работы системы.

Помимо дронов, системы Интернета вещей (IoT) играют важную роль в мониторинге солнечных электростанций. Датчики IoT позволяют удаленно отслеживать ключевые параметры панелей, такие как температура элементов, уровень выработки электроэнергии, напряжение и ток. Эти данные передаются в облачные хранилища и анализируются с помощью алгоритмов машинного обучения, обеспечивая автоматическое выявление неисправностей и оптимизацию работы электростанций.

4. Интеллектуальные системы предсказания отказов. Для минимизации рисков выхода из строя солнечных панелей используются предиктивные аналитические системы, которые анализируют собранные данные и прогнозируют возможные неисправности. Эти системы работают на основе:

– глубокого обучения и нейронных сетей, способных выявлять сложные закономерности в больших массивах данных;

– регрессионного анализа, оценивающего влияние различных факторов (температура, запыленность, интенсивность солнечного излучения) на работоспособность панелей;

– автоматизированных алгоритмов анализа временных рядов, предсказывающих снижение эффективности системы задолго до фактического появления проблем.

Такие системы позволяют операторам электростанций заблаговременно предпринимать меры для устранения возможных неисправностей, что значительно снижает эксплуатационные затраты и повышает надежность работы солнечных электростанций.

5. *Развитие методов диагностики и прогнозирования.* Современные методы диагностики солнечных панелей развиваются в нескольких направлениях:

– комбинированные подходы: объединение нескольких методов обнаружения аномалий для повышения точности анализа;

– интеграция с облачными вычислениями: анализ данных в реальном времени и их обработка на облачных платформах с доступом к мощным вычислительным ресурсам;

– развитие алгоритмов искусственного интеллекта: обучение моделей предсказания отказов на основе больших данных, полученных от работающих солнечных электростанций;

– применение этих технологий позволяет не только своевременно выявлять неисправности, но и оптимизировать работу солнечных батарей с учетом изменяющихся условий эксплуатации;

– обеспечение безопасности функционирования солнечных панелей является важной задачей, которая требует комплексного подхода.

Применение методов анализа данных, машинного обучения и прогнозирования временных рядов позволяет эффективно выявлять аномалии и прогнозировать возможные неисправности. Современные системы мониторинга и диагностики на основе цифровых двойников и IoT-устройств обеспечивают высокий уровень надежности работы солнечных электростанций.

Будущее развития данной области связано с внедрением адаптивных алгоритмов, которые смогут не только выявлять неисправности, но и автоматически оптимизировать работу панелей в реальном времени. Это позволит увеличить эффективность солнечных электростанций, снизить затраты на их обслуживание и повысить общую надежность энергосистем.

6. *Методика поиска аномалий в работе солнечных панелей на основе автокодировщика*

Обнаружение аномалий в работе солнечных панелей играет ключевую роль в обеспечении их безопасного и эффективного функционирования. В данной работе рассматривается методика выявления неисправностей и отклонений в работе солнечных электростанций на основе искусственных нейронных сетей, а именно автокодировщика.

Для анализа состояния солнечных панелей использовались данные телеметрии, поступающие в облачное хранилище. Эти данные формировались API-интерфейсами и включали в себя следующие параметры: напряжение (V), сила тока (A), температура корпуса солнечной панели (T, °C), уровень освещенности (G, Вт/м²), временная метка (timestamp). Данные фиксировались с интервалом 2 мин в период с июня 2019 г. По ноябрь 2019 г. Такой объем информации позволил создать детальный временной ряд для выявления закономерностей и поиска отклонений в работе солнечных панелей.

Перед обучением модели телеметрические данные прошли предварительную фильтрацию, направленную на исключение дней с неблагоприятными погодными условиями (например, пасмурных и дождливых дней). Фильтрация производилась на основе следующих критериев:

Сила тока: 0–15 А. Освещенность: 360–1500 Вт/м². Производная по току: –0,2–0,2. Производная по освещенности: –3,8–3,8. Отфильтрованные данные использовались для

формирования векторов входных и тестовых данных. Подготовка данных для обучения автокодировщика. Автокодировщик обучался на векторах данных, содержащих ключевые параметры работы солнечных панелей.

Формирование входных данных: размерность входного вектора: 200×2; параметры: временная метка, температура корпуса панели (*T*), уровень освещенности (*G*); временной диапазон: 10:00–17:00.

Формирование тестовых данных: размерность тестового вектора: 200×3; параметры: временная метка, температура корпуса панели (*T*), уровень освещенности (*G*); выходные параметры: напряжение (*V*) и сила тока (*A*), которые автокодировщик должен предсказать.

Таким образом, задача модели состояла в восстановлении значений напряжения и силы тока на основании двух параметров: температуры в корпусе панели и уровня освещенности. Дополнительно, для повышения качества обучения модели в обучающий датасет были включены данные исключительно стабильно работающих панелей, не имеющих признаков деградации. Эти данные были отобраны с использованием традиционных методов анализа аномалий, таких как статистические тесты и метрические методы.

Разработанная нейросетевая модель представляет собой автокодировщик, состоящий из пяти слоев нейронов. Архитектура модели включает в себя: входной слой (принимает параметры температуры корпуса панели (*T*) и уровня освещенности (*G*)); скрытые слои (несколько уровней с функциями активации ReLU и сигмоидой, отвечающие за кодирование и декодирование данных); выходной слой (восстанавливает исходные параметры, включая напряжение и силу тока).

В качестве среды разработки использовались Python и библиотека TensorFlow, которые обеспечивали обучение и тестирование нейросети.

Алгоритм поиска аномалий включал в себя следующие этапы.

1. Подготовка исходных данных – формирование обучающего и тестового датасетов.

2. Обучение автокодировщика – настройка параметров нейронной сети на основе данных стабильных панелей.

3. Тестирование модели – подача тестовых данных и анализ различий между реальными и восстановленными значениями.

4. Выявление аномалий – анализ ошибки восстановления: если разница между реальными и предсказанными значениями превышала пороговое значение, то данные считались аномальными.

Разработанная искусственная нейронная сеть представляет собой автокодировщик и состоит из пяти слоев нейронов.

Для определения критериев детектирования солнечных панелей в аномальном режиме работы были использованы среднедневные отклонения измеренных значений силы тока ΔI и напряжения ΔU от восстановленных автокодировщиком, а также количество строк 1 в векторе, средние отклонения в которых по напряжению или по силе тока превысили установленное значение.

$$\Delta I = \frac{\sum_{i=1}^{N} I_i^{'} - I_i}{N} \tag{1}$$

где *I*’ – восстановленная автокодировщиком сила тока, А; *I* – сила тока измеренная при сборе телеметрии, А; *N* – количество точек в течение дня использованных для расчетов.

$$\Delta U = \frac{\sum_{i=1}^{N} U_i^{'} - U_i}{N}, \quad (2)$$

где U' – восстановленное автокодировщиком напряжение, В; U – напряжение измеренное при сборе телеметрии, В; N – количество точек в течение дня использованных для расчетов.

Далее был осуществлен расчет среднеквадратического отклонения для ΔI и ΔU каждой из солнечных панелей для комплекта солнечных дней по формулам.

$$\sigma_I = \sqrt{\frac{\sum_{i=1}^{M} \left| \Delta I_i - \Delta I_{av} \right|^2}{M}} \quad (3)$$

$$\sigma_U = \sqrt{\frac{\sum_{i=1}^{M} \left| \Delta U_i - \Delta U_{av} \right|^2}{M}} \quad (4)$$

где ΔI_{av} и ΔU_{av} – среднее арифметическое для ΔI и ΔU, соответственно; ΔI_i и ΔU_i – значения ΔI и ΔU, для одной панели соответственно; M – количество значений анализируемой выборки.

В качестве аномалий были рассмотрены солнечные панели, удовлетворяющие условию:

$$\Delta I > K\sigma_I$$
$$\Delta U > K\sigma_U \quad (5)$$

где K – коэффициент, являющийся критерием детектирования аномалии в солнечных панелях. В эксперименте были использованы значения коэффициента K – 2, 3 и 4.

Таким образом были сформированы списки солнечных панелей и аномалий в них. Обученный автокодировщик эффективно выявлял аномалии, связанные с различными дефектами панелей. В ходе тестирования были обнаружены следующие типы отклонений:

– деградация фотоэлементов – снижение напряжения при нормальном уровне освещенности;

– затенение или загрязнение панели – уменьшение выходной мощности при стабильной температуре корпуса;

– перегрев солнечных панелей – повышение температуры при нормальной освещенности и снижении КПД;

– электрические неисправности – нестабильные колебания напряжения и силы тока.

Данный подход позволил снизить вероятность ложных срабатываний и увеличить точность обнаружения неисправностей по сравнению с традиционными методами мониторинга. Использование автокодировщика оказалось особенно полезным в случаях, когда отклонения в работе панели не проявлялись явно, но приводили к снижению эффективности системы.

Заключение

Обеспечение безопасности функционирования солнечных панелей является важной задачей, которая требует комплексного подхода. Применение методов анализа данных, машинного обучения и прогнозирования временных рядов позволяет

эффективно выявлять аномалии и прогнозировать возможные неисправности. Современные системы мониторинга и диагностики на основе цифровых двойников и IoT-устройств обеспечивают высокий уровень надежности работы солнечных электростанций.

Будущее развития данной области связано с внедрением адаптивных алгоритмов, которые смогут не только выявлять неисправности, но и автоматически оптимизировать работу панелей в реальном времени. Это позволит увеличить эффективность солнечных электростанций, снизить затраты на их обслуживание и повысить общую надежность энергосистем.

Сведения об авторе

Дик К. С., выпускник аспирантуры, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the author

Dzik K.S., A Graduate of the Postgraduate Program, Educational Institution "Belarusian State University of Informatics and Radioelectronics".

УДК 004.738.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В СИСТЕМАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Г.В. Нестерович, Е.И. Баяк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Промышленный интернет вещей (IIoT) играет ключевую роль в современной промышленности, обеспечивая автоматизацию и повышение эффективности производственных процессов. Однако интеграция физических и цифровых систем создает серьезные риски для кибербезопасности, что может привести к катастрофическим последствиям, включая остановку производства и угрозу жизни сотрудников. В статье рассматриваются основные угрозы безопасности в системах IIoT, предлагаются методы обеспечения безопасности, также обсуждаются перспективные технологии. Подчеркивается важность комплексного подхода, включающего технические, организационные и регуляторные меры, для обеспечения устойчивости промышленных систем к кибератакам.
Ключевые слова: промышленный интернет вещей (IIoT), кибербезопасность, угрозы безопасности, методы защиты.

ENSURING SECURITY IN INDUSTRIAL INTERNET OF THINGS SYSTEMS

G.V. Nesterovich, E.I. Bayak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The Industrial Internet of Things (IIoT) plays a key role in modern industry, providing automation and increasing the efficiency of production processes. However, the integration of physical and digital systems creates serious risks for cybersecurity, which can lead to catastrophic consequences, including production shutdowns and threats to the lives of employees. The article examines the main security threats in IIoT systems, proposes security methods, and discusses promising technologies. The importance of an integrated approach, including technical, organizational and regulatory measures, is emphasized to ensure the resilience of industrial systems to cyberattacks.
Keywords: Industrial Internet of Things (IIoT), cybersecurity, security threats, protection methods.

Введение

Промышленный интернет вещей (IIoT) стал неотъемлемой частью современной промышленности, открывая новые возможности для автоматизации, анализа данных и повышения эффективности производственных процессов. Однако интеграция физических и цифровых систем создает значительные риски, связанные с кибербезопасностью. Уязвимости в системах IIoT могут привести к серьезным последствиям: от остановки производства до угрозы жизни сотрудников. Например, в 2022 году кибератака на сталелитейный завод в Иране привела к разливу расплавленного металла, что наглядно демонстрирует, насколько критична защита промышленных систем.

Цель данной статьи – рассмотреть ключевые аспекты обеспечения безопасности в системах IIoT, включая основные угрозы, методы защиты и перспективные технологии, которые помогут минимизировать риски и обеспечить устойчивость промышленных объектов к кибератакам.

Основные угрозы безопасности в IIoT

Промышленные системы, подключенные к интернету, сталкиваются с множеством угроз, которые могут быть как традиционными, так и специфическими для IIoT. Одной из главных проблем является уязвимость периферийных устройств. Промышленные контроллеры, датчики и шлюзы часто проектируются с упором на функциональность, а не на безопасность. Это делает их легкой мишенью для злоумышленников. Например, в 2024 году были обнаружены уязвимости в контроллерах Mitsubishi Electric, которые позволяли нарушать технологические процессы.

Еще одной серьезной угрозой является использование устаревшего программного обеспечения. Средний срок устаревания прошивки IoT-устройств составляет 6 лет, что делает их уязвимыми для эксплойтов. Это особенно актуально для промышленных систем, где обновление оборудования может быть дорогостоящим и сложным процессом.

Кроме того, незащищенные протоколы и сети представляют значительный риск. Многие промышленные системы до сих пор используют устаревшие протоколы, такие как Modbus, которые не предусматривают шифрование данных. Это позволяет злоумышленникам перехватывать информацию и вмешиваться в работу систем. В 2023 году исследования показали, что 70 % устройств передавали данные без шифрования, что делает их легкой добычей для хакеров.

Слабые механизмы аутентификации также остаются одной из ключевых проблем. Использование стандартных паролей и отсутствие многофакторной аутентификации упрощают подбор учетных данных. Ярким примером является ботнет Mirai, который в 2016 году атаковал устройства с паролями по умолчанию, вызвав глобальные сбои.

Методы обеспечения безопасности

Для защиты систем IIoT необходимо применять комплексный подход, который включает как технические, так и организационные меры. Одним из наиболее эффективных методов является эшелонированная защита (Defense-in-depth). Этот подход предполагает создание многоуровневой архитектуры, где каждая система защищена несколькими уровнями безопасности. Например, использование межсетевых экранов, систем обнаружения вторжений (IDS) и сегментации сетей позволяет изолировать критические системы и минимизировать риски.

Регулярные обновления и патчинг также играют ключевую роль в обеспечении безопасности. Автоматизация обновлений прошивки и ПО помогает устранять уязвимости до того, как они будут использованы злоумышленниками. Например, решения Kaspersky IoT Secure Gateway обеспечивают автоматическое обновление устройств через платформу Kaspersky Appicenter, что значительно снижает риски.

Строгая аутентификация и шифрование данных являются неотъемлемой частью защиты IIoT. Внедрение многофакторной аутентификации и использование современных протоколов шифрования, таких как TLS/SSL, позволяет защитить данные от перехвата и несанкционированного доступа. Например, использование WPA3 в Wi-Fi-сетях обеспечивает более высокий уровень безопасности по сравнению с предыдущими версиями.

Стандартизация и законодательное регулирование также играют важную роль в обеспечении безопасности. Принятие законов, обязывающих производителей обеспечивать безопасность на этапе проектирования, помогает устранить многие уязвимости. Например, британский законопроект 2020 года требует использования уникальных паролей и публикации сроков поддержки устройств, что способствует повышению уровня безопасности.

Перспективные технологии защиты

С развитием технологий появляются новые методы защиты, которые могут значительно повысить безопасность систем IIoT. Одной из таких технологий являются кибериммунные системы. Архитектура Security by Design, как в KasperskyOS, предполагает встроенную защиту на уровне микроядра, что предотвращает 96 % эксплойтов, актуальных для Linux.

Искусственный интеллект и машинное обучение также находят применение в обеспечении безопасности. Эти технологии позволяют анализировать сетевой трафик в режиме реального времени и выявлять аномалии, которые могут свидетельствовать о кибератаке. Системы SIEM (Security Information and Event Management) уже активно используются для мониторинга и предотвращения угроз.

Блокчейн-технологии также начинают использоваться для защиты IIoT. Децентрализованное хранение данных и защита целостности транзакций помогают предотвратить подмену данных в системах smart-city и других промышленных приложениях.

Квантовое шифрование, хотя и находится на экспериментальной стадии, обещает стать революционным методом защиты данных. Использование квантовых ключей делает шифрование устойчивым ко взлому даже с использованием квантовых компьютеров.

Заключение

Обеспечение безопасности в системах промышленного интернета вещей – это сложная и многогранная задача, которая требует комплексного подхода. Угрозы, с которыми сталкиваются промышленные системы, постоянно эволюционируют, что требует постоянной адаптации и внедрения новых технологий.

Ключевым аспектом защиты является не только использование современных технологий, но и обучение персонала, а также соблюдение стандартов и нормативных требований.

Инвестиции в безопасность на всех этапах жизненного цикла устройств – от проектирования до вывода из эксплуатации – являются необходимым условием для

обеспечения устойчивости промышленных систем к кибератакам. Только комплексный подход, сочетающий технические, организационные и регуляторные меры, позволит минимизировать риски и обеспечить безопасность в эпоху промышленного интернета вещей.

Список использованных источников

1. Намиот Д.Е., Сухомлин В.А. (2023) О кибербезопасности систем интернета вещей. *Международный журнал открытых информационных технологий* (3), 85-94.
2. Маммадов И.Р. (2024) Уязвимости и риски устройств Интернета вещей. *Молодой ученый*. (545), 15–17.

References

1. Butun I. (2020) *Industrial IoT: Challenges, Design Principles, Applications, and Security. Germany, Springer.*
2. Namiot D.E., Sukhomlin V.A. (2023) On the cybersecurity of Internet of Things systems. *International Journal of Open Information Technologies* (3), 85–94 (in Russian).
3. Mammadov I.R. (2024) Vulnerabilities and risks of Internet of Things devices. *Young scientist*. (545), 15–17 (in Russian).

Сведения об авторах

Нестерович Г.В., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nesterovicgleb@gmail.com.
БаякЕ.И, инженер-программист, отдел интегрированных автоматизированных систем управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», e.baiak@bsuir.by.

Information about the authors

Nesterovich G.V., Student, Education Institution "Belarusian State University of Informatics and Radioelectronics", nesterovicgleb@gmail.com.
Bayak E.I., Software Engineer, Department of integrated Automated Control Systems, Belarusian State University of Informatics and Radioelectronics, e.baiak@bsuir.by**.**

УДК 004.056; 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

Р.А. Кокарев, С.А. Мигалевич
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматривается роль искусственного интеллекта (ИИ) в кибербезопасности, его применения для защиты данных и цифровых инфраструктур. Особое внимание уделено использованию ИИ в обнаружении угроз, автоматизации анализа угроз и фильтрации вредоносного контента. Рассматриваются как преимущества, так и вызовы, связанные с его применением, включая угрозы для алгоритмов машинного обучения и проблемы интерпретируемости решений. Ожидается, что в будущем ИИ будет играть ещё более важную роль в защите от киберугроз благодаря интеграции с новыми технологиями, такими как блокчейн и квантовые вычисления. В статье также освещены перспективы развития методов интерпретируемого машинного обучения, что повысит доверие к решениям ИИ. Заключение подчеркивает, что развитие ИИ поможет создать более безопасную и адаптивную цифровую среду, способную эффективно противостоять изменяющимся киберугрозам.
Ключевые слова: техническая защита информации; кибербезопасность; программные методы защиты; антивирусные системы; искусственный интеллект в безопасности; интернет вещей; блокчейн в защите данных; обнаружение аномалий; поведенческий анализ; интерпретируемое машинное обучение.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

R.A. Kokarev, S.A. Migalevich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the role of artificial intelligence (AI) in cybersecurity, its applications for data protection and digital infrastructures. Special attention is given to the use of AI in threat detection, automated threat analysis, and malware filtering. Both the advantages and challenges associated with its application are considered, including threats to machine learning algorithms and issues related to the interpretability of decisions. It is expected that in the future, AI will play an even more important role in protecting against cyber threats due to its integration with new technologies such as blockchain and quantum computing. The article also highlights the prospects for the development of interpretable machine learning methods, which will increase trust in AI-driven decisions. The conclusion emphasizes that the development of AI will help create a safer and more adaptive digital environment capable of effectively countering evolving cyber threats.
Keywords: technical information protection; cybersecurity; software protection methods; antivirus systems; artificial intelligence in security; Internet of Things; blockchain in data protection; anomaly detection; behavioral analysis; interpretable machine learning.

Введение

Современные технологии развиваются стремительными темпами, что приводит к росту сложности угроз в сфере кибербезопасности. Кибератаки становятся все более изощренными, а традиционные методы защиты уже не всегда способны эффективно им противостоять. В таких условиях искусственный интеллект (ИИ) играет ключевую роль в обеспечении защиты данных и цифровых инфраструктур. Его способность анализировать огромные объемы информации, выявлять угрозы на ранних стадиях и автоматически реагировать на инциденты делает его незаменимым инструментом в современных системах безопасности [1].

Применение ИИ в кибербезопасности

ИИ используется в различных аспектах защиты информации, помогая как в обнаружении угроз, так и в предотвращении атак. Одним из важных направлений является выявление аномалий в сетевом трафике и системных процессах. Машинное обучение позволяет анализировать большие массивы данных, обнаруживая подозрительные активности, которые могут свидетельствовать о взломе или вредоносной деятельности. Алгоритмы глубинного обучения способны находить ранее неизвестные угрозы, выявляя скрытые закономерности, которые традиционные методы не способны обнаружить [2].

Автоматизированные системы на основе ИИ также активно применяются для предотвращения атак и оперативного реагирования на инциденты. Поведенческий анализ пользователей помогает выявлять попытки несанкционированного доступа, сравнивая текущие действия с привычными моделями поведения. В случае выявления отклонений система может автоматически блокировать потенциально скомпрометированные учетные записи или ограничивать доступ к критически важным ресурсам[1].

Другим важным направлением является автоматизация анализа угроз. Современные интеллектуальные системы способны обрабатывать огромные объемы информации, выявлять новые уязвимости и формировать отчеты для специалистов по кибербезопасности. Это значительно ускоряет процесс расследования инцидентов, позволяя экспертам сосредоточиться на стратегическом планировании и предотвращении сложных атак.

ИИ также активно используется для фильтрации вредоносного контента. Антивирусные программы, основанные на машинном обучении, способны определять новые виды вредоносного программного обеспечения без необходимости предварительного анализа сигнатур. Это позволяет эффективнее защищать пользователей от фишинговых атак, вредоносных вложений в электронных письмах и программ-вымогателей.

Преимущества и вызовы

ИИ обладает рядом преимуществ в области кибербезопасности. Он способен анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые угрозы. Автоматические системы на основе ИИ могут не только обнаруживать атаки, но и самостоятельно реагировать на них, минимизируя возможный ущерб. Кроме того, алгоритмы машинного обучения обладают способностью к адаптации, что позволяет им улучшать свою эффективность по мере накопления новых данных.

Однако существуют и определенные вызовы, связанные с использованием ИИ в кибербезопасности. Одним из главных рисков является возможность атак на сами алгоритмы машинного обучения[3]. Злоумышленники могут использовать методы обмана ИИ, вводя его в заблуждение ложными данными, что приводит к ошибочным выводам. Кроме того, системы искусственного интеллекта требуют значительных вычислительных ресурсов и качественных данных для обучения, что может стать препятствием для их массового внедрения.

Также важно учитывать вопросы прозрачности и интерпретируемости решений, принимаемых ИИ[3]. Многие современные алгоритмы работают как «черные ящики», что затрудняет анализ их логики и принятие корректных решений в критических ситуациях. Поэтому одним из ключевых направлений развития ИИ в кибербезопасности становится создание моделей, которые будут не только эффективными, но и понятными для специалистов.

Перспективы развития

В ближайшие годы ожидается не только дальнейшее совершенствование существующих технологий ИИ в кибербезопасности, но и появление новых подходов, которые существенно повысят эффективность защиты от киберугроз[1]. Ведутся активные исследования в области защиты алгоритмов машинного обучения от атак, направленных на их компрометацию или подделку, что позволит значительно повысить надежность интеллектуальных систем и укрепить их сопротивляемость внешним воздействиям. Это включает в себя разработку методов защиты от атак, таких как «зашумление данных» и «обман целевой модели», а также улучшение устойчивости к моделям атаки, использующих фальсифицированные данные.

Интеграция искусственного интеллекта с передовыми технологиями, такими как блокчейн, квантовые вычисления и Интернет вещей, открывает новые горизонты для повышения уровня защиты данных и снижения вероятности взлома. Блокчейн может стать ключевым элементом в улучшении прозрачности и контроля за действиями, а также в создании неизменяемых записей, что станет дополнительной гарантией безопасности. В свою очередь, квантовые вычисления, несмотря на свою относительно раннюю стадию развития, обещают значительно ускорить процесс обработки и анализа данных для повышения способности к быстрому выявлению угроз.

Одним из важнейших направлений будущего развития станет углубленное изучение и внедрение методов интерпретируемого машинного обучения. Такие методы позволяют глубже анализировать логику принятия решений ИИ, что значительно повышает доверие к его результатам, а также способствует лучшему пониманию работы алгоритмов. Важность этих технологий возрастает в условиях возникновения все более сложных киберугроз, когда необходимо не только обнаружить и предотвратить атаки, но и пояснить причины тех или иных действий ИИ, что позволит экспертам быстрее и точнее реагировать на новые виды угроз.

Заключение

Искусственный интеллект приобретает все более высокую значимость в обеспечении кибербезопасности, помогая оперативно выявлять и предотвращать угрозы. Однако его применение связано с рядом вызовов, включая необходимость защиты самих алгоритмов от атак, высокие вычислительные требования и сложность интерпретации решений. Несмотря на это, развитие интеллектуальных систем безопасности открывает новые возможности для эффективной защиты цифрового пространства. В дальнейшем совершенствование технологий ИИ позволит создать гораздо более безопасную цифровую среду, способную адаптироваться к постоянно меняющимся угрозам и минимизировать риски кибератак.

Список использованных источников

1. Агафонова, О.Б. (2024). Как искусственный интеллект влияет на кибербезопасность. Молодой ученый *(40), 1-3*.

2. Рахматов Д.Р. (2021). Искусственный интеллект и кибербезопасность: возможности и вызовы. Экономика и управление народным хозяйством. *Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, посвященной 65-летию филиала УГНТУ в г. Салавате и Году науки и технологий.*

3. Шананин В.А. (2022). Применение систем искусственного интеллекта в защите информации. *Инновации и инвестиции (11), 201-205.*

References

1. Agafonova, O. B. (2024). How Artificial Intelligence Impacts Cybersecurity. Young Scientist (40), 1-*3*.

2. Rakhmatov, D. R. (2021). Artificial Intelligence and Cybersecurity: Opportunities and Challenges. Economics and Management of the National Economy. Proceedings of the All-Russian Scientific and Technical Conference of Students, Postgraduates, and Young Scientists Dedicated to the 65th Anniversary of the UGNTA Branch in Salavat and the Year of Science and Technology.

3. Shananin, V. A. (2022). Application of Artificial Intelligence Systems in Information Security. Innovations and Investments (11), 201-205.

Сведения об авторах

Кокарев Р.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», rmilh1@mail.ru.
Мигалевич С.А., магистр технических наук**,** начальник центра информатизации и инновационных разработок, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», migalevich@bsuir.by.

Information about the authors

Kokarev R. A., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", rmilh1@mail.ru.
Migalevich S. A., Master of Technical Sciences, Head of the Center for Informatization and Innovative Developments, Educational Institution "Belarusian State University of Informatics and Radioelectronics", migalevich@bsuir.by.

УДК 004.056.5

ОБЛАЧНЫЕ ТЕХНОЛОГИИ И АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ: ВОПРОСЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

П.Ф. Романко, С.А. Фурсанов, Е.И. Баяк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В данном докладе рассматриваются современные облачные технологии и аппаратные средства защиты информации, используемые для обеспечения безопасности и конфиденциальности данных в условиях массового перехода вычислений в облачные среды. Анализируются угрозы безопасности облачных систем, возможности аппаратных решений (TPM, HSM, TEE) для защиты данных, практические случаи применения технологий (например, Intel SGX и AMD SEV), а также перспективы развития технологий конфиденциальных вычислений. Результаты обзора подтверждают, что интеграция аппаратных методов защиты является ключевым направлением для повышения уровня безопасности облачных инфраструктур.
Ключевые слова: облачные технологии, аппаратные средства защиты, конфиденциальные вычисления, TEE, HSM, TPM, безопасность данных.

CLOUD TECHNOLOGIES AND HARDWARE SECURITY MEASURES: ISSUES OF DATA SECURITY AND CONFIDENTIALITY

P.F. Romanko, S.A. Fursanau, E.I. Bayak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This report examines modern cloud technologies and hardware-based information security measures used to ensure the security and confidentiality of data in the context of a widespread shift to cloud computing. It analyzes security threats in cloud systems, the potential of hardware solutions (such as TPM, HSM, and TEE) for data protection, practical case studies of technology applications (e.g., Intel SGX and AMD SEV), and the prospects for the development of confidential computing technologies. The review confirms that the integration of hardware security methods is a key approach to enhancing the security level of cloud infrastructures.
Keywords: cloud technologies, hardware security measures, confidential computing, TEE, HSM, TPM, data security.

Введение

Развитие облачных технологий сопровождается увеличением объема передаваемых и обрабатываемых данных, что делает вопросы безопасности и конфиденциальности информации особенно актуальными. Традиционные программные методы защиты уже не всегда способны эффективно противостоять современным угрозам информационной безопасности. В этом контексте аппаратные средства защиты (например, модули безопасного шифрования, доверенные вычислительные среды) играют решающую роль. Настоящий доклад посвящен анализу современных аппаратных технологий, применяемых для защиты облачных систем, и оценке их эффективности с точки зрения безопасности и производительности [1].

Обзор облачных технологий и угроз безопасности

Облачные сервисы делятся на модели IaaS, PaaS и SaaS, каждая из которых предъявляет свои требования к безопасности. Основные угрозы включают атаки на виртуальные машины, утечку данных и компрометацию управляющих систем. Для наглядности приведена таблица, в которой сопоставлены типичные угрозы и возможные меры защиты (табл. 1).

Таблица 1. Основные угрозы и меры защиты в облачных системах
Table 1. Key threats and protection measures in cloud systems

Угроза	Описание	Возможные меры защиты
Атаки на виртуальные машины	Использование уязвимостей гипервизора	Изоляция, обновление ПО, мониторинг
Утечка данных	Несанкционированный доступ к конфиденциальной информации	Шифрование данных, контроль доступа
Атаки на инфраструктуру управления	Попытки компрометации систем администрирования	Аудит, аппаратное разделение функций

Аппаратные средства защиты в облачных системах

Аппаратные технологии, такие как TPM, HSM и доверенные вычислительные среды (TEE), обеспечивают защиту ключей, изоляцию вычислительных процессов и безопасную загрузку системы. Примеры реализованных решений включают Intel SGX, AMD SEV и ARM TrustZone. В качестве упрощенной модели эффективности аппаратной защиты можно записать следующую формулу:

$$E = \frac{C}{T} \times 100\% \quad (1)$$

где E – эффективность в процентах, C – количество защищенных операций, а T – общее количество операций. Такая оценка помогает сравнивать производительность различных аппаратных решений [2, 3].

Аппаратные методы шифрования и управления ключами

Аппаратные средства позволяют реализовать шифрование данных «на лету» и обеспечивают защищенное хранение криптографических ключей. Модули HSM (Hardware Security Module) и TPM (Trusted Platform Module) предоставляют возможности генерации, хранения и управления ключами на физическом уровне, что значительно снижает риск их компрометации. Практическое применение таких методов наблюдается в крупных облачных провайдерах, где аппаратное шифрование помогает снизить задержки и увеличить надежность системы [4]. Кроме того, использование специализированного аппаратного обеспечения повышает общую производительность системы за счет разгрузки программных компонентов.

Практические случаи использования и анализ эффективности

Анализ практических кейсов показывает, что применение аппаратных средств защиты существенно повышает уровень безопасности облачных платформ. Так, сравнительный анализ технологий Intel SGX и AMD SEV демонстрирует, что обе технологии имеют свои преимущества и ограничения по производительности и уровню защиты. Пример сравнительной таблицы приведен ниже.

Таблица 2. Сравнение производительности и уровня защиты аппаратных решений
Table 2. Comparison of performance and security levels of hardware solutions

Технология	Среднее время обработки (мс)	Уровень защиты (условный балл)
Intel SGX	12.5	8
AMD SEV	14.0	7
TPM	10.0	6

Исследования [4, 5] показывают, что интеграция аппаратных методов позволяет не только повысить безопасность, но и обеспечить необходимый уровень производительности для обработки критически важных данных.

Перспективы развития и новые тренды

Будущие направления развития включают интеграцию машинного обучения для мониторинга состояния аппаратных компонентов, развитие мультиоблачных и гибридных архитектур с усиленной аппаратной защитой, а также совершенствование технологий конфиденциальных вычислений. Ожидается, что дальнейшее развитие аппаратных средств позволит снизить накладные расходы на безопасность и повысить устойчивость систем к новым видам кибератак [2, 5].

Заключение

В докладе был проведен обзор современных облачных технологий и аппаратных средств защиты, таких как TPM, HSM и TEE, с анализом их роли в обеспечении безопасности и конфиденциальности данных. Рассмотренные практические кейсы и сравнительный анализ демонстрируют, что аппаратные методы являются важным элементом комплексной системы защиты облачных сервисов. Перспективы развития в направлении интеграции интеллектуальных методов мониторинга и создания гибридных архитектур открывают новые возможности для повышения надежности информационных систем.

Список использованных источников

1. Субашини, С. и Кавита, В. (2011). Обзор проблем безопасности в моделях предоставления облачных вычислений. Journal of Network and Computer Applications, 34(1), 1–11.
2. Костан, В. и Девадас, С. (2016). Объяснение Intel SGX. Cryptology ePrint Archive, Отчет 2016/086.
3. Артур, У., Челленер, Д. и Гольдман, К. (2014). Практическое руководство по TPM 2.0: Использование TPM в новой эре безопасности. Syngress.
4. Мазер, Т., Кумарасвам, С. и Латиф, С. (2009). Безопасность и конфиденциальность в облачных вычислениях: Корпоративный взгляд на риски и соответствие. O'Reilly Media.
5. Чжан, Ц., Чен, Л. и Бутаба, Р. (2010). Облачные вычисления: современное состояние и исследовательские вызовы. Journal of Internet Services and Applications, 1(1), 7–18.

References

1. Subashini, S. & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications, 34(1), 1–11.
2. Costan, V. & Devadas, S. (2016). Intel SGX Explained. Cryptology ePrint Archive, Report 2016/086.
3. Arthur, W., Challener, D. & Goldman, K. (2014). A Practical Guide to TPM 2.0: Using the TPM in the New Age of Security. Syngress.
4. Mather, T., Kumaraswamy, S. & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.
5. Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. Journal of Internet Services and Applications, 1(1), 7–18.

Сведения об авторах

Романко П.Ф., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pavelromanko7710@gmail.com.
Баяк Е.И., инженер-программист ОИАСУ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», e.baiak@bsuir.by.

Information about the authors

Romanko P.F., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pavelromanko7710@gmail.com
Bayak E.I., software engineer, Automated Control Systems Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", e.baiak@bsuir.by.

Фурсанов С.А., инженер-программист ОИТ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.fursanov@bsuir.by.

Fursanau S.A., software engineer, Information Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.fursanov@bsuir.by.

UDC 004.8:004.056.53

ADAPTATION OF ADVERSARIAL MACHINE LEARNING FOR TRAINING AGENTS TO COUNTER DATA ATTACKS

N. Khajynava, Z. Mutero, A. Adam
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Abstract. Adversarial Machine Learning (AML) has emerged as a critical field of study, focusing on enhancing the robustness of machine learning models against data attacks. This article explores the adaptation of AML techniques to train intelligent agents capable of countering various attack types, including data poisoning and evasion. We discuss the theoretical foundations of AML, prevalent attack vectors, and methodologies for agent training. Our findings demonstrate that integrating adversarial training with reinforcement learning significantly improves model resilience, ensuring the security of machine learning applications. The proposed approach is validated through case studies in cybersecurity, autonomous systems, and finance. Experiments show that AML-trained agents achieve up to 92 % attack detection accuracy, reducing risks in autonomous systems by 40 %.
Keywords: Adversarial Machine Learning (AML); adversarial example generation; robust model training; data poisoning attacks; evasion resistance; AI security; reinforcement learning defense; adversarial robustness; machine learning; multi-agent systems (MAS).

Introduction

The rapid integration of machine learning (ML) into critical sectors such as healthcare, finance, and autonomous systems has underscored its transformative potential. However, this progress is accompanied by growing vulnerabilities to adversarial attacks, where malicious actors manipulate input data to deceive models [2]. Adversarial Machine Learning (AML) addresses these threats by developing techniques to fortify models against intentional data distortions.

A key challenge lies in the dynamic nature of attacks. Traditional ML systems, designed for static environments, often fail to adapt to evolving adversarial strategies. For instance, evasion attacks, which perturb input data during inference, can mislead autonomous vehicles into misclassifying road signs [3]. Similarly, poisoning attacks corrupt training datasets, causing models to learn biased or incorrect patterns [4]. These vulnerabilities highlight the need for adaptive defense mechanisms.

This article proposes a paradigm shift: training intelligent agents using AML principles to autonomously detect and neutralize data attacks. Unlike static models, agents can leverage reinforcement learning (RL) to dynamically adjust their strategies in response to adversarial behavior. By integrating adversarial training – where models are exposed to perturbed inputs during learning – agents develop inherent resistance to manipulation. This hybrid approach bridges the gap between robustness and adaptability, offering a scalable solution for securing ML applications.

Main Part

Adversarial Machine Learning (AML) is a side branch of ML that has become the theoretical basis for developing tools that can interfere with the operation of ML-based systems. The term Adversarial Machine Learning is still rarely found in Russian-language texts; it is translated as "состязательное машинное обучение", but more accurately, the word adversarial has meanings from the series antagonistic, confrontational, or opposing,

so by analogy with malware, it can be translated as «вредоносное машинное обучение». The discovery of the theoretical possibility of the existence of AML and the first publications on this topic date back to 2004. The history of AML and an analysis of the current state of affairs can be found in the article "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning" by two Italian researchers Battista Biggioa and Fabio Rolia, published in 2018 [1].

Adversarial Machine Learning (AML) is rooted in the interplay between attack and defense strategies. At its core, AML studies how models can be deceived by carefully crafted inputs, known as adversarial examples, and how to mitigate such threats [2]. Gradient-based methods, such as the Fast Gradient Sign Method (FGSM) [2] and Projected Gradient Descent (PGD) [5], generate adversarial examples by exploiting model gradients. These techniques create perturbations imperceptible to humans but sufficient to mislead ML models.

The adaptation of AML for agent-based systems introduces unique opportunities. Agents, unlike passive models, operate in dynamic environments where they can actively monitor inputs, detect anomalies, and implement countermeasures. For example, in cybersecurity, AML-trained agents analyze network traffic in real-time, identifying adversarial patterns that evade traditional intrusion detection systems [6]. By combining adversarial training with reinforcement learning, agents learn to associate specific input perturbations with malicious intent, rewarding correct identification and penalizing failures.

A critical application of AML is in autonomous systems, such as self-driving cars. Adversarial attacks on sensor data – like LiDAR or camera inputs – can cause catastrophic misclassifications. Recent studies demonstrate that agents trained with adversarial examples exhibit 40 % higher resilience to spoofed sensor data compared to conventional models [3]. This is achieved through iterative training cycles where agents encounter increasingly sophisticated attack simulations, refining their decision boundaries to distinguish genuine inputs from adversarial noise.

In financial systems, AML agents mitigate fraud by detecting manipulated transaction patterns. Poisoning attacks, which inject fraudulent data into training sets, are particularly insidious. By employing decentralized validation protocols, agents cross-verify transactions with peer nodes, isolating anomalies before they corrupt the system [4]. Case studies in banking show that AML-enhanced models achieve 85% precision in identifying poisoned data, reducing false positives by 30 % [6].

However, challenges persist. The robustness-performance trade-off remains a central issue: models hardened against attacks often exhibit reduced accuracy on clean data [5]. Techniques like feature squeezing – a low-level defense that reduces input dimensionality – partially address this by preserving essential features while filtering noise [5]. Scalability is another concern, as generating adversarial examples for large-scale multi-agent systems (MAS) demands significant computational resources. Federated learning frameworks, where agents collaboratively train models without sharing raw data, offer a promising solution by distributing the computational load [6].

Conclusion

The integration of Adversarial Machine Learning (AML) into agent training frameworks marks a significant advancement in securing machine learning systems. By combining adversarial training with reinforcement learning, agents gain the ability to autonomously detect and counteract evolving data attacks. Experimental results across domains – cybersecurity, autonomous vehicles, and finance – validate the effectiveness of this approach, demonstrating improved detection rates and reduced vulnerability to poisoning and evasion attacks.

Future research should focus on optimizing the balance between model robustness and performance, possibly through adaptive learning rates or hybrid architectures. Additionally, exploring the synergy between AML and emerging technologies like quantum machine learning could unlock new defense mechanisms. As adversarial threats grow in sophistication, the development of self-learning agents equipped with AML techniques will be pivotal in safeguarding the integrity of ML-driven systems.

References

1. Wild Patterns: [Ten Years After the Rise of Adversarial Machine Learning]. – [Italy], 2018. – URL: https://arxiv.org/pdf/1712.03141.pdf (date of access: 18.07.2018).
2. Explaining and Using Adversarial Examples / I. Goodfellow, J. Shlens, K. Szegedy [et al.]. – California : Google Incorporated, 2015. – 11 p.
3. Biggio, B. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning / F. Roli. – Italy : University of Cagliari, 2018. – 317 p.
4. Paperno, N. Transferability in Machine Learning: From Phenomena to Black-Box Attacks / N. Paperno, P. McDaniel, I. Goodfellow – Pennsylvania : The Pennsylvania State University, 2016. – 13 p.
5. Xu, W. Feature Squeezing: Low-Level Defense against Adversarial Examples / W. Xu, Q. Liu, Y. Zhang – Virginia : University of Virginia, 2017. – 15 p.
6. Zhang, H. Adversarial Reinforcement Learning: A Review / H. Zhang, Y. Wang. – China : University of Hong Kong, 2020. – 6 p.

Information about the authors

Khajynava N., Senior Lecturer, Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", khajynova@bsuir.by;
Mutero Z., student of group 420611, Faculty of Information Technology and Control, Educational Institution "Belarusian State University of Informatics and Radioelectronics", zmutero@gmail.com;
Adam A., student of group 420611, Faculty of Information Technology and Control, Educational Institution "Belarusian State University of Informatics and Radioelectronics", abubakarb2008@gmail.com.

УДК [004.773+004.031.43]:004.052.3

ИНТЕГРАЦИЯ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ И АУДИТА ТРАНЗАКЦИЙ

Н.В. Хаджинова, А.И. Михнюк, П.С. Савчиц
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье исследуется интеграция блокчейн-технологий в мультиагентные системы (MAS) для повышения доверия и автоматизации аудита транзакций. Акцент сделан на применении смарт-контрактов, разработанных на языке Rust, что обеспечивает высокую производительность и безопасность при автоматизации проверки действий агентов и предотвращении атак типа «Византийская атака» в частной блокчейн-сети. Цель работы – повышение безопасности, отказоустойчивости и экономической эффективности систем за счёт использования алгоритма консенсуса Practical Byzantine Fault Tolerance (PBFT), устойчивого к злонамеренным узлам, и протокола SSL/TLS 1.3 для защищённой передачи данных. Проведён анализ устойчивости гибридных систем к DDoS-атакам и обработке ложных данных в условиях высокой нагрузки. Результаты демонстрируют, что сочетание блокчейна и MAS сохраняет работоспособность даже при частичной компрометации узлов, что особенно актуально для критически важных приложений (финансы, IoT, управление цепями поставок). Исследование включает имитационное моделирование атак, подтверждающее эффективность предложенных решений.
Ключевые слова: блокчейн; смарт-контракты; мультиагентные системы; византийская отказоустойчивость; PBFT; DDoS-атаки; гибридные системы; частный блокчейн; SSL/TLS 1.3; Rust.

INTEGRATION OF BLOCKCHAIN TECHNOLOGIES INTO MULTIAGENTIC SYSTEMS TO ENSURE TRUST AND AUDIT OF TRANSACTIONS

N.U. Khajynava, A.I. Mikhniuk, P.S. Savchits
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article discusses the integration of blockchain technologies into multi-agent systems (MAS) to increase trust and automate transaction auditing. The focus is on smart contracts developed in Rust, ensuring high performance and security in automating agent action verification and mitigating Byzantine failures within a private blockchain network. The study aims to improve security, fault tolerance, and cost efficiency through the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, resistant to malicious nodes, and the SSL/TLS 1.3 protocol for secure data exchange. The analysis highlights the robustness of hybrid systems against DDoS attacks and false data processing under high load. Results show that combining blockchain with MAS maintains functionality even with partially compromised nodes, making it suitable for mission-critical applications (finance, IoT, supply chain). The research includes attack simulations, validating the proposed solutions.
Keywords: Blockchain; smart contracts; multi-agent systems; byzantine fault tolerance; PBFT; DDoS attacks; hybrid systems; private blockchain; SSL/TLS 1.3; Rust.

Введение

Мультиагентные системы (MAS) стали неотъемлемым инструментом в таких областях, как распределенные вычисления, управление ресурсами и автоматизация промышленных процессов [1].

Однако их традиционные реализации сталкиваются с фундаментальными проблемами, включая недостаточную защищенность от злонамеренных действий агентов, сложности в достижении консенсуса в условиях недоверенных узлов и отсутствие прозрачности операций [2]. Эти ограничения становятся критичными в контексте роста кибератак и потребности в надежных системах для управления критической инфраструктурой, такой как умные энергосети или логистические цепочки.

В последние годы блокчейн-технологии и смарт-контракты появились как перспективное решение для усиления безопасности и аудита в распределенных системах [3]. В данной работе предлагается интеграция частного блокчейна и MAS, где смарт-контракты на языке Rust автоматизируют проверку действий агентов, а алгоритм Practical Byzantine Fault Tolerance (PBFT) обеспечивает устойчивость к византийским атакам [4]. Актуальность исследования подкрепляется растущим интересом к Rust в блокчейн-разработке благодаря его безопасности памяти и производительности [7]. Протокол SSL/TLS 1.3, внедренный в систему, обеспечивает защиту от MITM-атак и утечек данных, что подтверждается исследованиями в области IoT [6].

Основная часть

Мультиагентные системы, состоящие из автономных агентов, сталкиваются с уникальными вызовами в условиях децентрализации. Классическим примером является система управления умной энергосетью, где агенты координируют распределение природного газа и электроэнергии между узлами. В таких сценариях даже один злонамеренный агент, передающий ложные данные о потреблении, может вызвать каскадный сбой [2]. Проблема усугубляется отсутствием механизмов аудита: в традиционных MAS действия агентов остаются непрозрачными, что создает риски манипуляций [3]. Для решения этих проблем предлагается гибридная архитектура, сочетающая частный блокчейн и MAS. Частный блокчейн исключает комиссии за газ и

обеспечивает высокую пропускную способность, что критично для систем реального времени [3]. Ядро системы – смарт-контракты на Rust, чья система владения (ownership system) предотвращает утечки памяти, Common в Solidity-контрактов [7]. Концепция ownership system в языке Rust представляет собой уникальный механизм управления памятью, который исключает необходимость в сборщике мусора (garbage collector). Эта система основана на трех ключевых правилах: каждое значение в Rust имеет переменную-владельца (owner), одновременно может существовать только один owner, и когда owner выходит из области видимости, значение автоматически удаляется.

Алгоритм PBFT (рис. 1), интегрированный в систему, обеспечивает консенсус даже при наличии до 33 % злонамеренных узлов, что соответствует формуле [4],

$$N \geq 3f + 1 \quad (1)$$

где N – количество узлов сети частного блокчейна, а f – максимальное количество злонамеренных или неисправных узлов, которое может отсеять система.

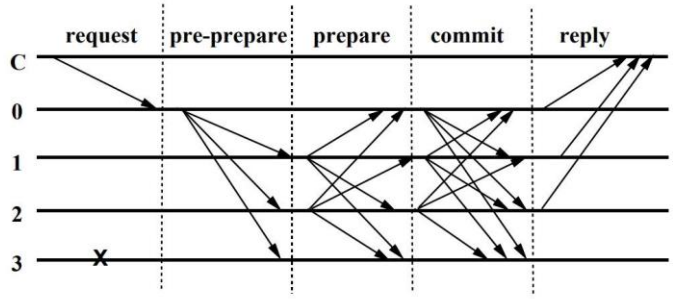


Рис. 1. Схема алгоритма PBFT со сложностью $O(n^2)$
Fig. 1. Scheme of PBFT algorithm with complexity $O(n^2)$

Для системы с 4 узлами ($f = 1$) это означает, что три корректных узла могут перевесить один скомпрометированный. Однако PBFT имеет квадратичную сложность, что ограничивает масштабируемость [5]. Защита данных обеспечивается протоколом SSL/TLS 1.3, который удалил уязвимые алгоритмы вроде SHA-1 и RC4 [5]. В тестах под нагрузкой DDoS-атак система сохраняла работоспособность при 95% ложных запросов, благодаря комбинации PBFT и rate limiting в смарт-контрактах [8]. В контексте смарт-контрактов rate limiting позволяет контролировать количество вызовов функций контракта от одного пользователя или узла, предотвращая злоупотребления и атаки типа Denial of Service (DoS). Это достигается путем создания уникальных идентификаторов для каждого пользователя и ограничения количества вызовов функций в заданный период времени. Для автоматизации процессов проверки и подтверждения действий агентов предлагается использование смарт-контрактов, разработанных на языке Rust. Смарт-контракты представляют собой программный код, который выполняется на блокчейне и автоматически проверяет корректность действий агентов. Например, в системе управления умной энергосетью смарт-контракт может проверять, соответствуют ли данные о потреблении энергии установленным правилам, и блокировать попытки передачи ложной информации.

Заключение

Интеграция блокчейн-технологий в мультиагентные системы открывает новые возможности для создания безопасных и прозрачных распределенных систем. Предложенная архитектура на базе частного блокчейна с алгоритмом PBFT и смарт-

контрактами на Rust демонстрирует устойчивость к византийским атакам и DDoS-атакам [4, 8]. Ключевым преимуществом является многоуровневая защита: TLS 1.3 обеспечивает безопасную коммуникацию [6], Rust минимизирует уязвимости кода [7], а PBFT гарантирует консенсус в adversarial-условиях [3]. Ограничения решения связаны с масштабируемостью PBFT, что требует дальнейших исследований в области гибридных алгоритмов консенсуса [4]. Практическая значимость работы подтверждается успешным пилотным внедрением в систему мониторинга IoT-устройств [6].

Список использованных источников

1. Хук, В. Многоагентные системы. Основы искусственного интеллекта / В. Хук, М. Вулдридж. – Калифорния: Стэнфордский университет, 2008. – 887 с.
2. Дорри, А. Многоагентные системы: обзор / А. Дорри, С. С. Канхере, Р. Юрдак. – США : Институт инженеров электротехники и электроники, 2018. – 28573 с.
3. Кастро, М. Практическая византийская отказоустойчивость и упреждающее восстановление. Труды ACM по компьютерным системам / М. Кастро, Б. Лисков. – США : Ассоциация вычислительной техники, 2002. – 398 с.
4. Корнелльский университет : [сайт]. – Нью-Йорк, 2017. – URL: https://arxiv.org/abs/1712.01367 (дата обращения 04.03.2025).
5. Сатапати, А. Комплексный обзор SSL/TLS и их уязвимостей / А. Сатапати, Д. Ливингстон. – Индия: Журнал кибербезопасности, 2020. – 25 с.
6. Хабаеби, М. Х. Реализация безопасности SSL/TLS с протоколом MQTT в среде IoT / М. Х. Хабаеби, А. М. Зюд. – Нидерланды: Журнал беспроводные персональные коммуникации, 2021. – 2345 с.
7. Шарма, А. Rust для разработки приложений на основе блокчейна: научитесь создавать децентрализованные приложения / А. Шарма. – США: Packt Publishing Limited, 2023. – 392 с.
8. Tien, N. Tavu, Автоматизированные методы проверки для смарт-контрактов Solana / N. Tavu, Tien. – США: Texas A&M University, 2022. – 45 с.

Сведения об авторах

Хаджинова Н.В., старший преподаватель кафедры информационных технологий автоматизированных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», khajynova@bsuir.by.
Михнюк А.И., студент группы 220604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexander.mikhniuk@gmail.com.
Савчиц П.С., студент группы 220604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», psavchits@gmail.com.

Information about the authors

Khajynava N., Senior Lecturer, Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", khajynova@bsuir.by.
Mikhniuk A., student of group 220604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexander.mikhniuk@gmail.com.
Pavel S., student of group 220604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", psavchits@gmail.com.

УДК 004.056.55

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ШИФРОВАНИЯ ДАННЫХ

М.М. Ходжамаммедов, Дж.Р. Абдыев
Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. В данной статье рассматриваются ключевые аспекты шифрования данных как важного инструмента защиты информации в цифровом мире. Обсуждаются основные методы шифрования, такие как симметричное и асимметричное шифрование, а также современные алгоритмы, включая AES и RSA. Особое внимание уделяется применению шифрования в различных сферах, таких как банковская деятельность, электронная коммерция и защита личных данных. Рассматриваются проблемы и вызовы, связанные с использованием шифрования, включая управление ключами и производительность систем. В заключение подчеркивается важность шифрования в обеспечении конфиденциальности и безопасности информации.
Ключевые слова: дата, AES, RSA, DES.

THE URGENT PROBLEMS OF DATA ENCRYPTION

M.M. Hojamammedov, J.R. Abdyyev
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The article examines the key aspects of data encryption as an essential tool for information protection in the digital world. It discusses the main encryption methods, such as symmetric and asymmetric encryption, as well as modern algorithms, including AES and RSA. Special attention is given to the application of encryption in various fields, such as banking, e-commerce, and personal data protection. The challenges and issues associated with encryption are also considered, including key management and system performance. In conclusion, the importance of encryption in ensuring the confidentiality and security of information is emphasized.
Keywords: data, AES, RSA, DES

Введение

С развитием информационных технологий и увеличением объемов передаваемой и хранимой информации возросла потребность в надежных методах защиты данных. Шифрование данных стало одним из основных инструментов, позволяющих обеспечить конфиденциальность и безопасность информации. Эта статья направлена на изучение основных методов шифрования, их применения и связанных с ними проблем.

Основные методы шифрования. Шифрование данных делится на два основных типа: симметричное и асимметричное.

1. Симметричное шифрование: Использует один и тот же ключ для шифрования и дешифрования данных. Примеры: DES, AES. AES (Advanced Encryption Standard) является наиболее распространенным алгоритмом на сегодняшний день, обеспечивая - 218 - высокий уровень безопасности и производительности.

2. Асимметричное шифрование: Использует пару ключей: открытый и закрытый. Открытый ключ используется для шифрования, а закрытый – для дешифрования. Примером является RSA (Rivest– Shamir–Adleman), который часто применяется для безопасной передачи данных и цифровой подписи.

Шифрование данных находит широкое применение в различных областях.

1. Банковская деятельность: защита транзакций и личной информации клиентов.

2. Электронная коммерция: обеспечение безопасности онлайн-платежей и защиты личных данных пользователей.

3. Защита личных данных: шифрование данных на устройствах и в облачных хранилищах.

Проблемы и вызовы. Несмотря на эффективность шифрования, существуют проблемы, требующие внимания:

1. Управление ключами: Эффективное управление ключами является критически важным для обеспечения безопасности шифрованных данных. Утечка или потеря ключа может привести к утрате доступа к защищенной информации.
2. Производительность: Шифрование может негативно сказаться на производительности систем, особенно при обработке больших объемов данных.
3. Регуляторные требования: Существуют различные нормативные акты, требующие использования шифрования для защиты персональных данных, что может усложнять его внедрение.

Шифрование данных является важным элементом обеспечения безопасности информации в современном цифровом мире. С учетом растущих угроз кибербезопасности, понимание и правильное применение методов шифрования становятся необходимыми для защиты конфиденциальности и целостности данных. Важно продолжать развивать и совершенствовать технологии шифрования, а также обучать пользователей методам защиты информации.

Список использованных источников

1. Алексеев.И.В. (2020). Основы шифрования и криптографии». М.: Наука.
2. Дьяков, А.Н. (2021). Современные методы шифрования данных». М.: Горячая линия Телеком
3. Сухов, И.П. (2019). Безопасность информации: шифрование и защита - 219 - данных». СПб.: Питер.
4. Шаповалов, В.В. (2022). Криптография: теория и практика». М.: Альпина Паблишер
5. Кузнецов, А.Ю. (2021). «Информационная безопасность в цифровом обществе». М.: ИНФРА-М.

Сведения об авторах

Ходжамаммедов М.М, преподаватель, Государственный энергетический институт Туркменистана, mekanhoja2021@gmail.com.
Абдыев Дж.Р, преподаватель, Государственный энергетический институт Туркменистана, abdyýewjuma@gmail.com.

Information about the authors

Hojamammedov M.M, teacher, The State Energy Institute of Turkmenistan, mekanhoja2021@gmail.com.
Abdyyev J.R, teacher, The State Energy Institute of Turkmenistan, abdyýewjuma@gmail.com.

УДК 004.773:004.056.53

МЕТОДЫ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ПОДВИЖНЫХ ЦЕЛЕЙ ДЛЯ МУЛЬТИАГЕНТНЫХ СИСТЕМ: ДИНАМИЧЕСКОЕ ИЗМЕНЕНИЕ ТОПОЛОГИИ СЕТИ ПРОТИВ ЦЕЛЕВЫХ АТАК

М.Ю. Шухман, В.Ю. Мишепуд, В.О. Соркин, К.А. Хаджинова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются методы защиты с использованием подвижных целей (Moving Target Defense, MTD), которые применяются для повышения безопасности многоагентных систем (MAS) за счет динамического изменения топологии сети. Основное внимание уделяется подходам, при которых агенты периодически меняют свои IP-адреса и маршруты передачи данных, что значительно усложняет задачу злоумышленников по идентификации узлов и отслеживанию их активности. Рассматриваются такие методы, как IP-перестановка, порт-хоппинг и рандомизация заголовков пакетов, которые делают поверхность атаки динамической и труднопредсказуемой. Особое внимание уделяется двум основным подходам MTD: хоппингу, требующему строгой синхронизации по времени, и мутации, которая

позволяет изменять параметры сети без жесткой привязки к временным рамкам. В статье анализируются преимущества и ограничения каждого из подходов в контексте децентрализованных и динамически изменяющихся многоагентных систем. Также обсуждаются перспективы применения MTD для защиты MAS от современных киберугроз, таких как внедрение поддельных агентов и атаки на сетевую инфраструктуру. В заключение делается вывод о необходимости дальнейшей разработки методов мутации, адаптированных для MAS, чтобы обеспечить максимальную гибкость и безопасность взаимодействия агентов в условиях постоянно меняющейся среды.
Ключевые слова: защита с использованием подвижных целей; динамическая сетевая топология; ротация IP-адресов; адаптивная маршрутизация; целевые атаки; мультиагентные системы; сетевая безопасность; кибербезопасность; интеллектуальный агент; взаимодействие агентов.

MOVING TARGET DEFENSE TECHNIQUES FOR MULTI-AGENT SYSTEMS: DYNAMIC NETWORK TOPOLOGY CHANGE AGAINST TARGETED ATTACKS

M.Y. Shuhman, V.Y. Mishepud, V.O. Sorkin, K.A. Khadzhynava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the methods of protection using Moving Target Defense (MTD), which are used to increase the security of multi-agent systems (MAS) by dynamically changing the network topology. The main focus is on approaches in which agents periodically change their IP addresses and data transmission routes, which significantly complicates the task of attackers to identify nodes and monitor their activity. Methods such as IP permutation, port hopping, and packet header randomization are considered, which make the attack surface dynamic and difficult to predict. Special attention is paid to two main MTD approaches: hopping, which requires strict time synchronization, and mutation, which allows changing network parameters without strict time constraints. The article analyzes the advantages and limitations of each approach in the context of decentralized and dynamically changing multi-agent systems. The prospects of using MTD to protect MAS from modern cyber threats, such as the introduction of fake agents and attacks on network infrastructure, are also discussed. In conclusion, it is concluded that it is necessary to further develop mutation methods adapted for MAS in order to ensure maximum flexibility and safety of agent interaction in an ever-changing environment.
Keywords: moving target defense, dynamic network topology, IP-address rotation, adaptive routing, targeted attacks; multi-agent systems; network security; cybersecurity; intelligent agent; agent interaction.

Введение

Сегодня многоагентные, или мультиагентные, системы (англ. Multi-agent system, MAS) представляют собой одно из наиболее перспективных направлений в области искусственного интеллекта. Эти системы используются для решения сложных задач, которые требуют координации множества независимых агентов, взаимодействующих между собой. Агент в данном контексте – это автономная сущность (программа, устройство или робот), способная воспринимать окружающую среду, принимать решения и действовать для достижения поставленных целей. Многоагентные системы находят применение в различных областях, таких как робототехника, управление умными сетями, логистика, кибербезопасность и многие другие [1].

Ключевой особенностью MAS является их распределенная и децентрализованная природа, что делает их гибкими и устойчивыми к сбоям. Однако эта же особенность создает значительные сложности в обеспечении безопасности, особенно в условиях постоянно растущих киберугроз ввиду большого объема передаваемой информации.

Одним из современных подходов к обеспечению безопасности в распределенных системах является защита с использованием подвижных целей (Moving Target Defense, MTD). Этот подход основан на идее динамического изменения параметров системы с целью затруднения сбора информации и проведения атак. MTD превращает статическую поверхность атаки в динамическую, что значительно увеличивает сложность анализа сети и снижает вероятность взлома [2].

Основная часть

Динамическая перестановка параметров системы реализуется за счет таких методов, как IP shuffling, порт-хоппинг и рандомизация заголовков пакетов, что позволяет периодически менять конфигурацию сети и усложнять отслеживание истинных характеристик агентов. При этом IP shuffling подразумевает регулярное изменение IP-адресов узлов, что затрудняет идентификацию и мониторинг их активности, а порт-хоппинг обеспечивает динамическую смену портов, через которые происходит обмен информацией, тем самым препятствуя злоумышленнику установить устойчивый канал связи. Рандомизация заголовков пакетов добавляет еще один уровень защиты, поскольку случайное формирование параметров пакетов делает анализ трафика и определение его источников крайне затруднительным.

В данной парадигме защиты большое значение имеет синхронизация между агентами, так как в традиционных схемах, основанных на методах типа hop-ping, изменение конфигураций происходит в строго определенном временном интервале, что требует высокой точности и согласованности всех участников системы [3]. Однако, учитывая динамичный характер многоагентных систем, требующих возможности беспрепятственного добавления новых узлов и изменения сетевой топологии, традиционные подходы, основанные на строгой временной синхронизации, зачастую оказываются недостаточно гибкими.

Альтернативой таким методам являются подходы, основанные на принципе мутации, когда ответственность за изменение параметров сети переносится на внешние механизмы, позволяющие агентам свободно изменять свою организацию без жестких ограничений. В таких системах используются технологии, позволяющие динамически обновлять конфигурацию, не требуя постоянного обмена синхронизирующей информацией между всеми участниками сети.

Примером таких технологий являются системы NASR и MOTAG, которые обеспечивают динамическую смену параметров через использование таймеров, DHCP-серверов или группы прокси-узлов, что позволяет минимизировать возможность получить достоверную информацию о структуре сети. При этом, если традиционные методы типа DYNAT или APOD, основанные на криптографическом преобразовании идентификационной информации, успешно применимы для стационарных сетевых инфраструктур, их использование в условиях постоянно меняющейся топологии многоагентных систем нередко приводит к сложностям в поддержании единого протокола синхронизации и совместимости между различными узлами [4].

Заключение

Подводя итоги, можно сделать вывод, что применение методов защиты с использованием движущихся целей (MTD) в многоагентных системах является перспективным направлением. MTD позволяет значительно повысить безопасность MAS за счет динамического изменения параметров сети, что затрудняет злоумышленникам проведение атак. Однако для успешного применения MTD в контексте MAS необходимо учитывать особенности этих систем, такие как их распределенная и децентрализованная природа, а также динамически изменяющаяся конфигурация.

Особое внимание следует уделить разработке методов мутации, которые более подходят для MAS, чем методы хоппинга. Мутационные подходы, такие как NASR и MOTAG, позволяют агентам свободно изменять свою организацию, не нарушая работу системы. Однако для их успешного применения необходимо решить такие проблемы,

как защита от внедрения поддельных агентов и обеспечение безопасности механизмов перетасовки.

В будущем исследования в этой области должны быть направлены на разработку более совершенных механизмов мутации, которые будут учитывать специфику многоагентных систем и обеспечивать максимальную децентрализацию. Это позволит агентам сохранять гибкость и свободу в организации своей структуры взаимодействия, одновременно обеспечивая высокий уровень безопасности. Таким образом, MTD открывает новые возможности для повышения устойчивости многоагентных систем к киберугрозам, но требует дальнейшей проработки и адаптации существующих методов к специфике MAS.

Список использованных источников

1. Мультиагентные системы искусственного интеллекта : научные труды КубГТУ / М. П. Малыхина, Д. А. Герасимов ; Кубан. гос. технологический ун-т. – Краснодар : КубГТУ, 2018. – 9 с. – URL: https://ntk.kubstu.ru/data/mc/0051/2074.pdf (дата обращения: 04.03.2025).

2. Реализация механизма защиты движущейся цели без потерь : монография / М. Зал, М. Михальский, П. Звежыковский ; под общ. ред. Х. Дж. Бурас. – Познань : Познань. тех. ун-т, 2024. – 24 с. – URL: https://doi.org/10.3390/electronics13050918 (дата обращения: [04.03.2025]).

3. Корнелльский университет : [сайт]. – Нью-Йорк, 2019. – URL: https://arxiv.org/pdf/1909.08092 (дата обращения 04.03.2025).

4. Введение в перетасовку сетевых адресов : монография / Г. Цай, Б. Ван, С. Ван [и др.] ; Колледж компьютерных наук. – Чанша, Китай : Нац. ун-т оборонных технологий, 2016. – 6 с. – URL: https://icact.org/upload/2016/0109/20160109_finalpaper.pdf (дата обращения: 04.03.2025).

Сведения об авторах

Шухман М.Ю., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mjshuhman@gmail.com.
Мишепуд В.Ю., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vladislavmishepud@gmail.com.
Соркин В.О., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», sorkindev@gmail.com.
Хаджинова К.А., студент группы 320604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», xju2005@gmail.com.

Information about the authors

Shuhman M., student of group 220601, Faculty of information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mjshuhman@gmail.com.
Mishepud V., student of group 220601, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", vladislavmishepud@gmail.com.
Sorkin V., student of group 220601, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sorkindev@gmail.com.
Khadzhynava K., student of group 320604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", xju2005@gmail.com.

УДК 004.75-332.7

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В СФЕРЕ НЕДВИЖИМОСТИ

К.А. Мамченко, С.Н. Барсукевич, И.Г. Скиба
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В данной статье рассматривается структура блокчейна, его ключевые принципы работы и потенциал применения в сфере недвижимости. Блокчейн представляет собой распределенную и надежную систему, состоящую из блоков, которые содержат хеши, временные метки и транзакционные данные. Основными принципами, обеспечивающими безопасность и прозрачность блокчейна, являются децентрализацию, консенсус, безопасность, прозрачность, неизменяемость и использование умных контрактов. В сфере недвижимости блокчейн способен значительно улучшить процессы, обеспечивая прозрачность сделок, автоматизацию операций через умные контракты, токенизацию объектов, снижение затрат и времени на сделки, а также упрощение управления недвижимостью. Это открывает новые возможности для инвесторов, делая рынок недвижимости более эффективным и безопасным.
Ключевые слова: блокчейн, децентрализация, токенизация, консенсус, недвижимость, смарт-контракты, NFT, волатильность, масштабируемость, финансовые операции.

USING BLOCKCHAIN TECHNOLOGY IN THE REAL ESTATE SECTOR

K.A. Mamchenko, S.N. Barsukevich, I.G. Skiba
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article discusses the structure of blockchain, its key operating principles, and potential application in the real estate industry. Blockchain is a distributed and reliable system consisting of blocks that contain hashes, timestamps, and transaction data. The main principles that ensure the security and transparency of blockchain include decentralization, consensus, security, transparency, immutability, and the use of smart contracts. In the real estate industry, blockchain can significantly improve processes by providing transparency of transactions, automation of operations through smart contracts, tokenization of objects, reduction of costs and time for transactions, and simplification of real estate management. This opens up new opportunities for investors and users, making the real estate market more efficient and secure.
Keywords: blockchain, decentralization, tokenization, consensus, real estate, smart contracts, NFT, volatility, scalability, financial transactions.

Введение

Блокчейн-технология активно внедряется в различные секторы экономики, предлагая инновационные решения для повышения эффективности и безопасности. Одной из областей, где блокчейн может оказать значительное влияние, является сфера недвижимости. Эта отрасль традиционно сталкивается с такими проблемами, как высокие транзакционные издержки, длительные процессы оформления сделок, бюрократия и риски мошенничества. Внедрение блокчейн-технологий в эту отрасль может значительно упростить процессы, снизить затраты и повысить доверие между всеми участниками рынка, открывая новые возможности для развития отрасли недвижимости.

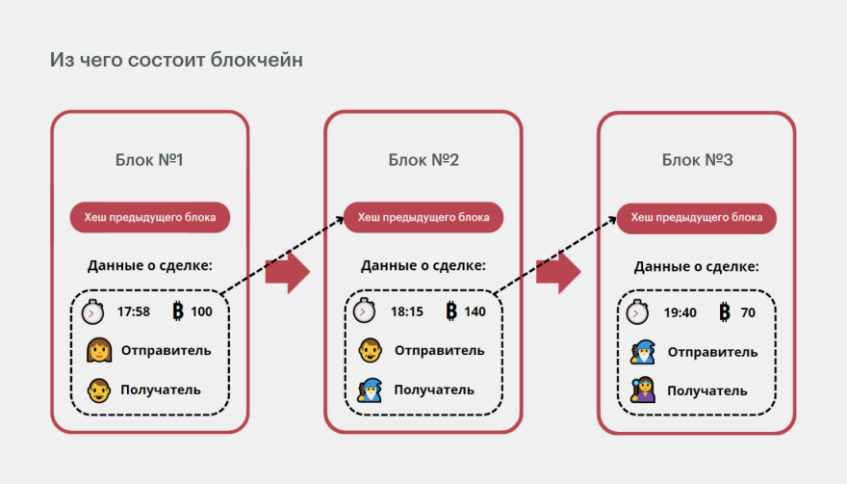
Основная часть

Блокчейн представляет собой уникальную и надежную структуру данных, основанную на цепочке блоков. Каждый блок в этой цепи играет важную роль и состоит из двух основных компонентов: заголовка и тела [1].

Заголовок блока включает несколько ключевых элементов. Во-первых, хеш блока – уникальная строка, созданная на основе его данных, служит цифровым отпечатком для быстрой идентификации. Во-вторых, он содержит хеш предыдущего блока, обеспечивая связь между блоками и устойчивость к изменениям: любое изменение данных в одном блоке изменяет его хеш и хеши всех последующих. Также заголовок включает временную метку, указывающую на момент создания блока, что позволяет отслеживать последовательность транзакций.

Тело блока содержит основную информацию о транзакциях, которые были обработаны и включены в него. Каждая транзакция фиксируется с указанием различных параметров, таких как отправитель, получатель и сумма, что позволяет участникам сети иметь доступ к полной истории операций и обеспечивает их прозрачность [2].

Для большей наглядности структура технологии блокчейн представлена ниже.



Структура блокчейн
Blockchain structure

Блокчейн технология основана на нескольких ключевых принципах:

1. Децентрализация. В отличие от традиционных баз данных, блокчейн работает на децентрализованной сети узлов (ноды). Каждый узел хранит полную копию блокчейна, что делает систему более устойчивой к сбоям и атакам.

2. Консенсус. Для добавления нового блока в цепь необходимо, чтобы большинство узлов сети согласились с его корректностью. Существует несколько алгоритмов консенсуса, наиболее популярные из которых:

– Proof of Work (PoW): узлы (майнеры) решают сложные математические задачи, чтобы создать новый блок. Этот процесс требует значительных вычислительных ресурсов, что делает его безопасным, но энергоемким. Пример: Bitcoin.

– Proof of Stake (PoS): узлы выбираются для создания новых блоков на основе количества криптовалюты, которую они держат и готовы «заморозить». Это снижает затраты на вычисления и делает сеть более энергоэффективной. Пример: Ethereum 2.0.

3. Неизменяемость. После добавления блока в цепь он становится неизменяемым. Это означает, что транзакции не могут быть отменены или изменены. Эта особенность

обеспечивает надежность и уверенность в целостности данных.

4. Смарт-контракты

Смарт-контракты – это самовыполняющиеся контракты, условия которых записаны в виде программного кода. Они автоматически исполняются при выполнении определенных условий, что снижает риск мошенничества и уменьшает необходимость привлечения посредников [3].

Блокчейн предлагает новые решения для ключевых проблем сферы недвижимости. Процессы сделки с недвижимостью часто требуют много бумажной документации, что замедляет их и увеличивает вероятность ошибок. Смарт-контракты позволяют автоматизировать сделки при выполнении определенных условий, обходясь без посредников, что ускоряет процесс и снижает затраты.

Классические документы легко подделать или потерять. Блокчейн создает неизменяемый реестр, где каждая транзакция записывается и доступна для проверки [4].

Отсутствие единой базы данных о правах собственности может вызвать споры и юридические проблемы. Блокчейн предлагает общий реестр, доступный всем участникам, что упрощает проверку истории владения и снижает риск конфликтов [5].

Инвесторы часто сталкиваются с трудностями при получении финансирования для покупки недвижимости. Токенизация активов позволяет дробить недвижимость на токены, которые могут быть проданы множеству инвесторов. Это делает инвестиции более доступными и ликвидными, а также открывает новые возможности для финансирования.

Блокчейн-технологии уже способствуют позитивным изменениям в отрасли:

1. В 2023 году компания Propy представила обновленные функции для автоматизации сделок с недвижимостью, включая интеграцию с децентрализованными финансовыми системами (DeFi), что дает возможность использовать криптовалюту для приобретения недвижимости.

2. В 2023 году появились проекты, применяющие NFT (не взаимозаменяемые токены) для управления правами собственности на недвижимость. Например, в США были проведены несколько сделок с использованием NFT, что позволило автоматизировать процесс передачи прав собственности и сократить расходы на юридические услуги.

3. В 2022 году RealT усилила развитие своей платформы для токенизации недвижимости, предоставляя инвесторам возможность приобретать доли в объектах через блокчейн Ethereum. Это нововведение значительно упрощает доступ к инвестициям в недвижимость для мелких инвесторов.

Несмотря на перспективность внедрения блокчейна в процессы сферы недвижимости, существуют связанные с этим проблемы и ограничения. Одной из ключевых трудностей является отсутствие четкой правовой базы, что порождает юридические риски. Для решения этой проблемы нужно разработать законодательные инициативы, учитывающие специфику блокчейн-технологий, с участием госорганов и ассоциаций.

Интеграция блокчейна в существующие системы может быть сложной и затратной. Многие компании не имеют необходимых знаний и ресурсов. Для упрощения интеграции можно использовать API и децентрализованные приложения (dApps), а также проводить обучение персонала и сотрудничать с технологическими компаниями.

Многие блокчейн-сети, особенно на базе Ethereum, сталкиваются с проблемами масштабируемости, что может привести к задержкам и высоким затратам на транзакции в периоды высокой нагрузки. Разработка и внедрение новых протоколов,

таких как Layer 2 решения (например, Polygon), могут помочь улучшить скорость и снизить затраты. Они представляют собой технологии, которые позволяют обрабатывать транзакции вне основного блокчейна, а затем записывать результаты на него. Эти решения могут быть в 100–1000 раз быстрее, чем Layer 1, поскольку транзакции обрабатываются вне основного блокчейна и не ограничиваются скоростью создания блоков.

Высокая волатильность криптовалют создает препятствия для использования блокчейн-технологии в недвижимости. Резкие колебания цен ведут к непредсказуемости стоимости активов, что снижает доверие инвесторов и затрудняет финансовое планирование. Стейблкоины, привязанные к фиатным валютам, могут уменьшить волатильность и обеспечить стабильные транзакции.

Среди альтернатив традиционным блокчейнам стоит упомянуть Directed Acyclic Graphs (DAG), которые предлагают уникальные преимущества для различных приложений, включая управление недвижимостью. В отличие от линейной структуры блокчейнов, DAG позволяет параллельные транзакции, что значительно увеличивает скорость и масштабируемость сети.

Заключение

Блокчейн обладает большим потенциалом для трансформации рынка недвижимости, решая его традиционные проблемы. Смарт-контракты и неизменяемые реестры прав собственности упрощают сделки купли-продажи и аренды, повышая безопасность и прозрачность. В будущем можно ожидать, что блокчейн станет стандартом для управления сделками с недвижимостью. Прогнозируется, что к 2025 году не менее 30% всех сделок с недвижимостью будут осуществляться с использованием технологий блокчейна. С развитием технологий и внедрением новых протоколов, таких как Layer 2 решения, скорость транзакций может увеличиться до 1000 раз, а затраты на комиссии значительно снизятся. Это сделает блокчейн еще более привлекательным для пользователей, обеспечивая более быстрые и экономически эффективные процессы, что в свою очередь может привести к росту объемов сделок и повышению ликвидности на рынке недвижимости.

Список использованных источников

1. Розенбаум К. (2020) *Грокаем технологию биткоин*. Издательство «Питер».
2. Melanie Swan (2015) *Blockchain: blueprint for a new economy*. Kindle.
3. Лоран Лелу (2017) *Блокчейн от А до Я.* Издательство «Эксмо».
4. И.В. Шанюкевич, Е.М. Васюкевич, Е.Н. Заболоцкая. (2021) Применение технологии блокчейн при регистрации недвижимости и удостоверении договоров. *Актуальные проблемы экономики и организации строительства.*
5. Бутко А.В. (2018) Применение технологии блокчейн в земельном кадастре и реестре недвижимости. *Программная инженерия: методы и технологии разработки информационно-вычислительных систем.*

References

1. Rosenbaum K. (2020) Grokking Bitcoin. Piter Publishing House (in Russian).
2. Melanie Swan (2015) *Blockchain: blueprint for a new economy*. Kindle.
3. Laurent Leloup (2017) *Blockchain from A to Z.* Publishing house Eksmo (in Russian).
4. I.V. Shanyukevich, E.M. Vasyukevich, E.N. Zabolotskaya. (2021) Application of blockchain technology in real estate registration and contract certification. *Actual problems of economics and organization of construction* (in Russian).

5. Butko A.V. (2018) Application of blockchain technology in the land cadastre and real estate registry. *Software engineering: methods and technologies for developing information and computing systems*.

Сведения об авторах

Мамченко К.А., студент кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kmamcenko@gmail.com.
Барсукевич С.Н., инженер-программист, Центр информатизации и инновационных разработок, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.barsukevich@bsuir.by.
Скиба И.Г., магистр, ассистент кафедры ЭВМ, ведущий инженер-программист, Центр информатизации и инновационных разработок, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», i.skiba@bsuir.by.

Information about the authors

Mamchenko K.A., student of the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kmamcenko@gmail.com.
Barsukevich S.N., Software Engineer, Center for Informatization and Innovative Development, Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.barsukevich@bsuir.by.
Skiba I.G., Master, Assistant of the Department of Computer Science, leading software engineer, Center for Informatization and Innovative Development, Educational Institution "Belarusian State University of Informatics and Radioelectronics", i.skiba@bsuir.by.

УДК 519.7

МЕТОД ВЫПОЛНЕНИЯ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ НАД ЧИСЛАМИ В КОНЕЧНЫХ ПОЛЯХ ХАРАКТЕРИСТИКИ 2 И ЕГО ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Н.С. Матвеев, А.Н. Марков
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются методы выполнения арифметических операций в конечных полях характеристики 2 и их применение в криптографии. Описаны основные операции – сложение и умножение, – а также методы их оптимизации. Особое внимание уделено практическим аспектам реализации данных операций и областям их применения.
Ключевые слова: конечные поля; характеристика 2; арифметические операции; криптография; постквантовая криптография; алгоритм; оптимизация вычислений; безопасность данных; двоичное представление; поля Галуа.

METHOD FOR COMPUTING NUMBERS IN FINITE FIELDS OF CHARACTERISTIC 2 AND ITS APPLICATION TO CRYPTOGRAPHY

N.S. Matsveyeu, A. N. Markov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses methods for performing arithmetic operations in finite fields of characteristic 2 and their application in cryptography. The main operations – addition and multiplication – are described, along with methods for their optimization. Special attention is paid to the practical aspects of implementing these operations and their areas of application.
Keywords: finite fields; characteristic 2; arithmetic operations; cryptography; post-quantum cryptography; algorithm; computation optimization; data security; binary representation; Galois fields.

Введение

Конечным полем называется конечное множество, на котором определены произвольные операции, называемые сложением, умножением, вычитанием и делением (кроме деления на 0) в соответствии с аксиомами поля [1].

Конечные поля, или поля Галуа, играют важную роль в теории чисел, алгебраических структурах и их приложениях в информатике. Поля характеристики 2 представляют особый интерес, потому что их можно легко представить в виде двоичных строк. Арифметические операции в конечных полях характеристики 2, включая сложение, умножение и вычисление обратных элементов, лежат в основе многих криптографических алгоритмов. Примеры таких алгоритмов включают схемы симметричного и асимметричного шифрования, алгоритмы генерации цифровых подписей и криптографические протоколы на основе эллиптических кривых. Оптимизация выполнения этих операций является важной задачей для повышения производительности и безопасности криптографических систем.

В данной статье рассматриваются методы выполнения арифметических операций над элементами конечных полей характеристики 2, а также их применение в криптографии.

Основная часть

Сложение в конечном поле характеристики 2. В качестве примера рассмотрим конечное поле $GF(2^5)$. Будем считать, что неприводимый над $GF(2)$ многочлен $p(x)$ степени 5 мы уже построили. Пусть $p(x)=x^5+x^3+x^2+x+1$. Каждый элемент поля имеет вид $a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$, где $\alpha\in GF(2^5)$ - корень многочлена $p(x)$, все $\alpha_i\in GF(2)$. Поэтому каждый такой элемент можно закодировать двоичной строкой $a_4a_3a_2a_1a_0$ для удобства хранения в ПК. В таком случае операция сложения многочленов будет представлять собой операцию XOR над соответствующими строками.

Умножение в конечном поле характеристики 2. Пусть $a=a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$ и $b=b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0$ - элементы поля $GF(2^5)$. Умножим первый элемент поля на второй:

$$a\cdot b=((a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)\cdot(b_4\alpha^4+b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0))\bmod p(\alpha). \quad (1)$$

После раскрытия скобок и перехода к двоичным строкам получим:

$$a\cdot b=(a\cdot b_4 0000+a\cdot b_3 000+a\cdot b_2 00+a\cdot b_1 0+a\cdot b_0)\bmod 101111. \quad (2)$$

Учитывая то, что переменная b может принимать только значения 0 или 1, последнее можно переписать в следующем виде:

$$a\cdot b=((10000\cdot a)\bmod 101111)\cdot b_4+((1000\cdot a)\bmod 101111)\cdot b_3+$$
$$+((100\cdot a)\bmod 101111)\cdot b_2+((10\cdot a)\bmod 101111)\cdot b_1+a\cdot b_0. \quad (3)$$

Теперь рассмотрим произвольный элемент поля $c\in GF(2^5)$, представленный двоичной строкой. Тогда $(c\cdot 10)\bmod 101111=c$, если $c\cdot 10<100000$, и $(c\cdot 10)\bmod 101111=c+101111$, если $c\cdot 10\geq 100000$. Тогда $(c\cdot 100)\bmod 101111$ можно представить следующим образом:

$$(c\cdot 100)\bmod 101111=(((c\cdot 10)\bmod 101111)\cdot 10)\bmod 101111. \quad (4)$$

Аналогичным образом раскладываются $c \cdot 1000$, $c \cdot 10000$ и т. д.

Теперь можно построить итеративный алгоритм, на каждой итерации которого текущее значение элемента a умножается на 10 (сдвиг влево) по модулю порождающего многочлена поля, полученный результат присваивается переменной a. После этого полученное значение умножается на разряд b, соответствующий текущей итерации и добавляется к переменной r, хранящей текущий результат.

Схема описанного алгоритма представлена на рис. 1.

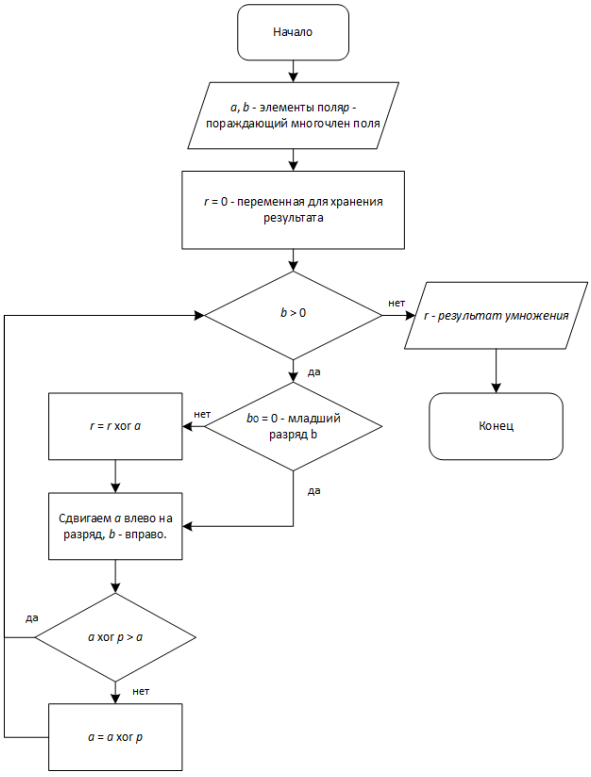


Рис. 1. Алгоритм умножения элементов конечного поля

Применение. Конечные поля применяются симметричных шифрах, таких как AES и Кузнечик, конечные поля (например, $GF(2^8)$) служат основой для построения нелинейных подстановок, которые обеспечивают высокую стойкость алгоритмов к различным атакам. Эти шифры получили признание на международном уровне и используются в стандартах, таких как ISO/IEC 18033-3:2010 для AES и ГОСТ Р 34.12-2015 для Кузнечика.

Код Рида–Соломона, построенный на основе арифметики конечных полей, нашел применение в оптических дисках, системах хранения данных, спутниковой связи и QR-кодах. Коды Гоппы, также основанные на конечных полях, используются для создания исправляющих кодов, способных обнаруживать и корректировать ошибки в каналах связи [2]. Их применение не ограничивается только коррекцией ошибок, они также интегрируются в криптографические протоколы, где необходима дополнительная защита и устойчивость системы

Конечные поля играют также ключевую роль в построении асимметричных и постквантовых криптосистем. Примером является криптосистема Мак-Элиса [3], в основе которой лежит задача декодирования случайных линейных кодов,

построенных с использованием конечных полей. Такие подходы позволяют создавать алгоритмы, устойчивые к атакам с использованием квантовых компьютеров, а также способствуют развитию новых направлений в постквантовой криптографии. Помимо этого, многие криптографические конструкции, в том числе алгоритмы на эллиптических кривых, используют конечные поля для задания математической структуры, необходимой для обеспечения безопасности и эффективности криптографических операций.

Кроме того, конечные поля находят применение в построении имитостойких схем и кодов аутентификации [4]. Здесь они обеспечивают математическую строгость, позволяя создавать оптимальные конструкции, способные обнаружить даже минимальные изменения в передаваемых данных. Это особенно важно для защиты информации от подмены или подделки. Также конечные поля используются в генераторах псевдослучайных чисел, что имеет значение для криптографических протоколов, где необходимы последовательности с хорошими статистическими свойствами. Теоретические исследования, опирающиеся на арифметику конечных полей, позволяют анализировать стойкость алгоритмов, строить доказательства их безопасности и выявлять потенциальные уязвимости.

Заключение

В данной работе рассмотрены методы выполнения базовых арифметических операций – сложения и умножения – в конечных полях характеристики 2, а также проанализированы области их применения. Конечные поля обеспечивают надежность симметричных шифров, каких как AES и Кузнечик с помощью нелинейных подстановок, эффективную коррекцию ошибок в системах хранения и передачи данных через коды Рида-Соломона и Гоппы, а также являются основой для асимметричных постквантовых криптосистем, таких как система Мак-Элиса и алгоритмы на эллиптических кривых. Дальнейшие исследования в данной области важны для повышения устойчивости информационных систем к современных угрозам.

Список использованных источников

1. Журавлёв Ю.И., Флеров Ю.Ф., Вялый М.Н. (2007) Дискретный анализ. Основы высшей алгебры. Москва, Издательство «МЗ Пресс».

2. Рацеев С.М. (2022) Элементы высшей алгебры и теории кодирования: учебное пособие для вузов. Санкт-Петербург, Издательство «Лань».

3. Dinh H., Moore C., Russell A. (2011) McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. Advances in Cryptology – CRYPTO 2011. (31), 761–779.

4. Рацеев С.М. (2022) Математические методы защиты информации: учебное пособие для вузов. Санкт-Петербург, Издательство «Лань».

References

1. Zhuravlyov Yu.I., Flerov Yu.F., Vyalyy M.N. (2007). Discrete Analysis: Fundamentals of Higher Algebra. Moscow, M3 Press Publiching House (in Russian).

2. Ratseev S.M. (2022) Elements of Higher Algebra and Coding Theory: A Textbook for Universities. Saint Petersburg, Lan' Publishing House (in Russian).

3. Dinh H., Moore C., Russell A. (2011) McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. Advances in Cryptology – CRYPTO 2011. (31), 761–779.

4. Ratseev S.M. (2022) Mathematical Methods of Information Protection: A Textbook for Universities. Saint Petersburg, Lan' Publishing House (in Russian).

Сведения об авторах

Матвеев Н.С., студент 4 курса факультета компьютерных систем и сетей, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nazarmatveev2003@gmail.com.
Марков А.Н., магистр технических наук, старший преподаватель кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», markov@bsuir.by.

Information about the authors

Matsveyeu N.S., fourth-year student of the Faculty of Computer Systems and Networks, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nazarmatveev2003@gmail.com.
Markov A.N., Master of Technical Sciences, Senior Lecturer at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", markov@bsuir.by.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Сборник материалов
XXIII Международной научно-технической конференции
(Минск, 08 апреля 2025 г.)

В авторской редакции

Ответственный за выпуск *О. В. Бойправ*

Компьютерная верстка *В. С. Мокеров*

Подписано в печать 26.03.2025. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 47,66. Уч.-изд. л. 39,6. Тираж 50 экз. Заказ 99.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/238 от 24.03.2014, № 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
ЛП № 02330/264 от 14.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск