Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СБОРНИК МАТЕРИАЛОВ
**60-ой научной конференции**
**аспирантов, магистрантов и студентов**
22–26 апреля 2024 года

Минск, БГУИР

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**60-я научная конференция
аспирантов, магистрантов и студентов**

Сборник материалов

22–26 апреля 2024 года
Минск, БГУИР

УДК 621.391

60-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 12-26 апреля 2024 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2024. – 219 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 60-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

# СОДЕРЖАНИЕ

## СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

# СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

## СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ»

# Статистика по 60-ой научной конференции аспирантов, магистрантов и студентов УО «Белорусский государственный университет информатики и радиоэлектроники»

## НАПРАВЛЕНИЕ

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

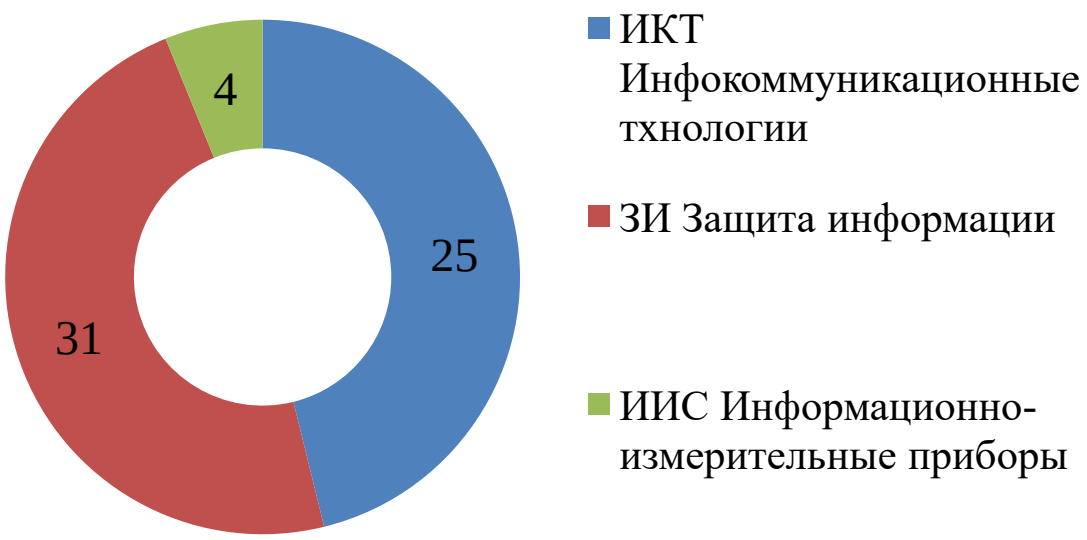



Рисунок 1 – Диаграмма «Количество статей по секциям»

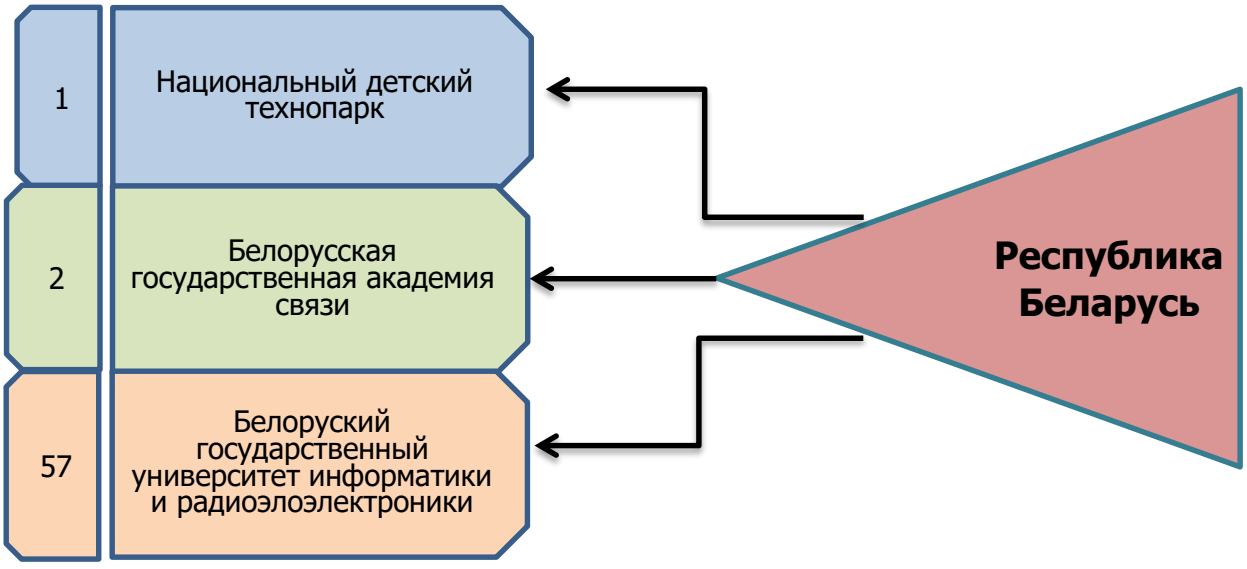



Рисунок 2 – Учреждения образования, принявшие участие в конференции


Рисунок 3 – Участники конференции

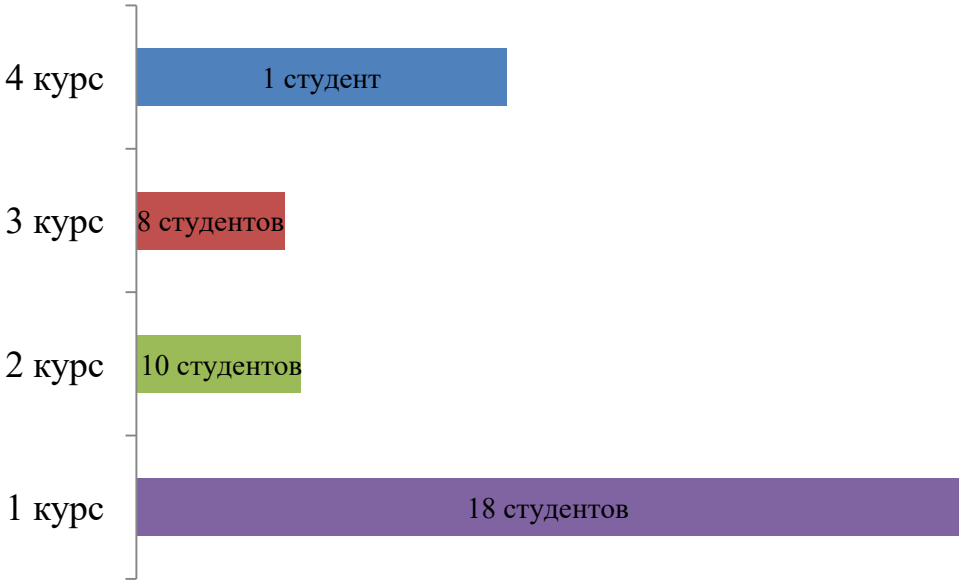



Рисунок 4 – Студенты-участники конференции

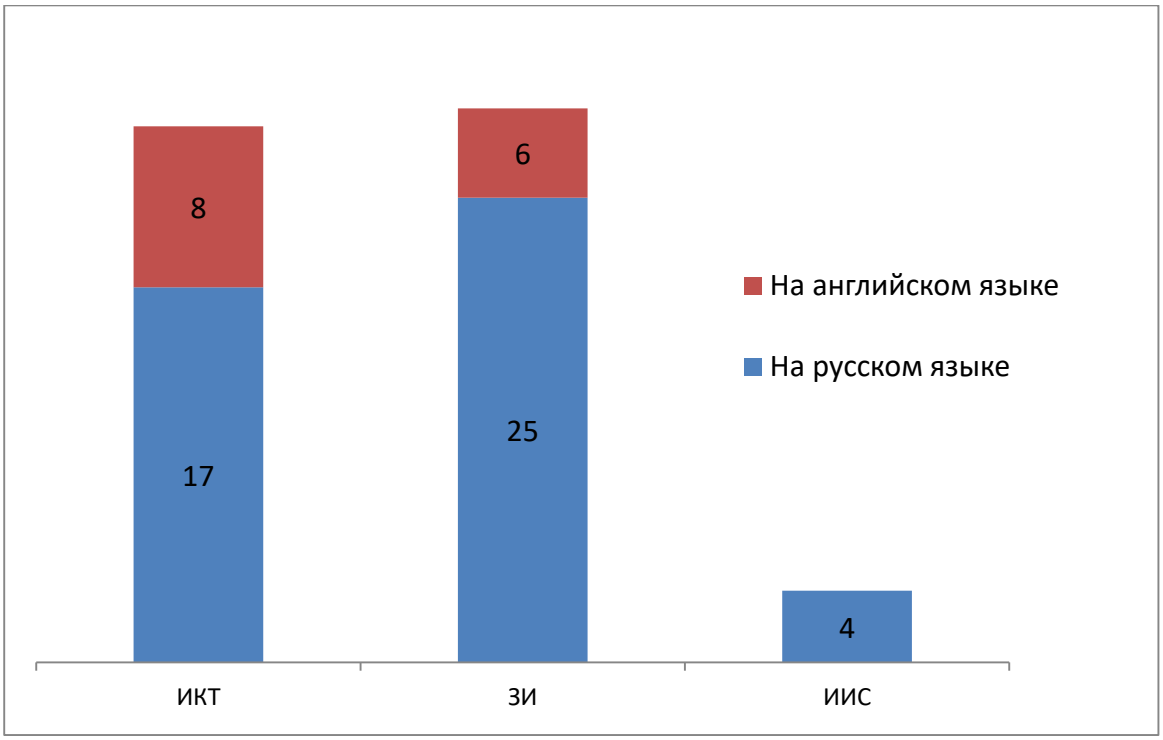



Рисунок 5 – Диаграмма «Материалы конференции на русском и английском языках»

# СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

UDC 004.056

## SQL INJECTION ATTACKS AND PREVENTION

*Deng Y.Y., gr.367311/ master student*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vrublevsky I.A. – PhD in Technical Sciences*

**Annotation.** The paper discusses SQL injection, a common editing language used to inject malicious SQL commands into input forms or queries in order to gain access to a database or manipulate its data. Corresponding precautions for each SQLI are considered.

**Keywords.** SQL language injection, attacks, query, prevention methods.

**Introduction.** A web application is a software system that provides an interface to its users through a web browser on any operating system (OS). Despite their growing popularity, web application security threats have become more diverse, resulting in more severe damage. Malware attacks, particularly SQLI attacks, are common in poorly designed web applications. This vulnerability has been known for more than two decades and is still a source of concern. This highlights the need to develop effective methods to protect data from unauthorized access. In this context, we need an effective self-detection method for prevention.

**The main part.** To grasp how SQL language can be abused, SQLI attackers and defenders need to understand how it functions [1]. The queries must be prepared in the SQL language and adhere to specified syntax to retrieve data from databases or modify the data, such as:

```
"SELECT * FROM authortable WHERE book_name = 'Advanced Database Systems'"
```

The aforementioned search will provide all books with book name "Advanced Database Systems." The queries are typically typed into a web browser and sent to the database management system [3].

What if the attacker in this case extends the original SQL query?

For example:

```
"SELECT * FROM authortable WHERE book_name = 'Advanced Database Systems' OR
'1'='1'"
```

The above query will return all book names in the database, not just the book names labeled as "Advanced Database Systems," because the sentence '1=1' is always true. If the stored list of book names is not a secret and the previous example might not pose a problem [4]. If successful, it might return sensitive data, such as passwords, bank accounts, trade secrets, and personal information, which might be regarded as a privacy breach among other negative effects. However, it could be applied to value using different syntax.

By using SQL injection, the attackers can alter the SQL statement by replacing user's supplied data with their own data as shown in Figure 1. Thus, the attackers can have direct access to a database server to retrieve confidential information. However, the impacts of the SQL injection attacks are far reaching and they vary depending on the database applications. Some of these impacts of a successful SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data, and remote command execution. Authentication bypass enables an attacker to access database application by using fake username and password. Information disclosure allows an attacker to obtain sensitive data from the database. Compromised data integrity assists an attacker to change some contents of the data in the database. Compromised availability data enables an attacker to delete some information from the database.

Remote command execution allows an attacker to affect the host operating system [3].

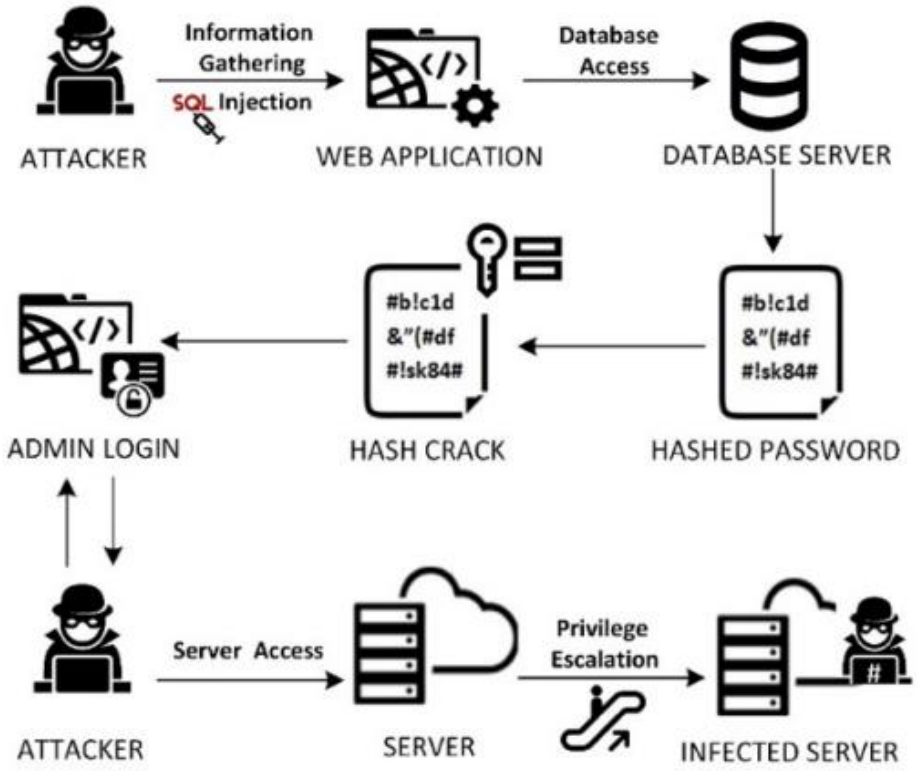



Figure 1. How SQL injection attacks work

**Most common attacks on SQLI**. As we know, SQL is a programming language that is used to create, update, and access data in a database. A hacker can intentionally cause the application to fail, delete data, steal data, or gain unauthorized access by carefully crafting SQL commands [5]. To address the aforementioned issue, we provide a detailed overview of the various types of SQLI attacks discovered to date. For each type of attack, we provide explanations and examples of how such attacks can be carried out.

**Tautology attack**

The attacker attempts to use a conditional query argument to test always true in the tautology attack, such as (1=1) or (− −). The attacker injects the condition and transforms it into a tautology that is always valid using the WHERE clause. This type of attack is commonly used to access databases without requiring authentication on websites [1].

**Union query**

In this category of attack, the UNION operator is only used if both queries have the same form, the attacker constructs a SELECT statement that is similar to the original query [5]. To do so, it must be known that the correct table name, as well as the number of columns and their data types from the first query. As a result, two conditions may be satisfied, or an attack on the union query will be launched, and each query returns the same number of columns [6]. If the data type of a column is incompatible with string data, the injected query will fail.

**Piggybacked query**

The piggybacked query attack concatenates more query statements onto the initial query ";" [1]. This technique is especially risky since it enables an attacker to insert virtually any SQL command. Data extraction, addition or modification of data, denial of service (DoS), and remote command execution are all examples of determined attacks [16]. In this type of attack, an attacker attempts to inject additional queries into the original query. Unlike other forms, attackers attempt to add new and distinct queries that "piggyback" on the original query rather than changing it [3].

**Illegal or incorrect query**

This kind of attacker takes advantage of a database query that was improperly executed [1]. It will show database error messages, which frequently provide crucial facts that enable an attacker to learn the application's database specifics. The attack goal includes identifying injection parameters,

performing database fingerprinting, and extracting data. This attack assists an attacker in gathering critical information concerning the nature and function of the back-end database of a web application [8]. The attack is thought to be a practice run for future attacks aimed at gathering information. This attack takes advantage of the fact that the default error pages on application servers are frequently excessively descriptive [7].

**Stored procedure query**

Here, an attacker can use this technique to modify the database's stored procedures [1]. Both authorized and unauthorized users will receive true or false results from the process. The users can save their features and use them whenever they want. A collection of SQL queries is provided with the feature to use it. The intruder uses malicious SQL codes to execute the database's built-in stored procedures [8]. This leads to cause the cached stored procedure query plans being recompiled. A stored procedure's constraint is that it can only be used in the database.

**Inference query**

In this attack, the query is recast as an operation and executed based on the answer to a true or false question about database data values [10]. For this method of injection, attackers attempt to break into a site that has been sufficiently protected that when an injection is successful and there is no accessible feedback in the form of database error messages. Since database error messages are not available to provide feedback and attackers must rely on another approach to get a response from the database.

**Existed prevention methods.** This section provides an overview of the existed approach and explains the rationale for detecting SQL injection.

A. Any comment character is present

Having a single or multiple lines comment character in a statement generated from an application is not a common practice by the programmers. The reason is that when a user executes her/his query in the applications, she/he never includes a comment with it. On the other hand, the attackers use this approach to include a comment character after their malicious command to let the system neglect the rest of the query maintained by the application.

B. Number of semicolons

The SQL statements are terminated with one semicolon at the end of it. When an attacker injects her/his malicious commands in the middle of the statement, she/he places a semicolon and then comments the rest of the statement, which result in having multiple semicolons. As we are dealing with it as a string and not command, we can identify if multiple semicolons are present or not.

C. Presence of always true conditions

Always true conditions rarely can be found in the benign SQL statements while they are the most common terms used by attackers in their injection to make the condition always satisfied after the OR operator. Researchers have considered this approach; however, they only have considered the checking for number1=number1, variable1=variable1, and 'string'='string'. In our approach, we add the checking for number1!=number2, variable1!=variable2, and 'string1'!='string2' so that it will also always return a true value.

D. The number of commands per statement

Regular queries generated by applications usually consist of one request only such as SELECT. When an attacker injects her/his code in the original SQL statement, it results in having one statement with more than one requests.

E. Presence of abnormal commands

When an application reads the input from a user and inserts it into a statement, it usually uses SELECT, INSERT, or DELETE requests. Having statement coming from the application with DROP, CREATE, COMMIT, ROLLBACK, GRANT, REVOKE, and DECLARE, requests may indicate that a malicious action is happening.

F. Presence of special keywords

Having a statement coming from an application, which is operated by a user requesting for the version of the SQL server, could indicate a malicious action. A set of similar keywords are used to

be checked in the statement through the developed features identifier code. If any of the keywords is present, the program will detect it.

**Conclusion**. This paper involves SQLI statements and analyzes them based on their principles to detect whether malicious commands are injected into the system and protect the system from this type of attack.

***List of literature:***

*1. A comprehensive study on SQL injection attacks, their mode, detection and prevention / S. Dasmohapatra [et al.] // Proceedings of Second Doctoral Symposium on Computational Intelligence: DoSCI 2021, Springer Singapore, 2022. –P. 617-632.*

*2. Static analysis approaches to detect SQL injection and cross-site scripting vulnerabilities in web applications: a survey / M.K Gupta [et al.] // Int Conf Recent Adv Innov Eng ICRAIE, 2014. –P. 9-13.*

*3. Open source web application security: a static analysis approach / M. Alenezi, Y. Javed // 2016 International Conference on Engineering & MIS (ICEMIS). IEEE, 2016. –P. 1-5.*

*4. A review of static code analysis methods for detecting security faws / B.S Basutakara, P.N. Jeyanthi // J Univ ShanghaiSci Technol, 2021. –P. 47-53.*

*5. Dynamic multi-process information fow tracking for web application security / S. Nanda [et al.] // Proceedings of the 2007 ACM/IFIP/USENIX international conference on Middleware companion, 2007. –P.1-20.*

*6. Hybrid approach to detect SQLi attacks and evasion techniques / A. Makiou [et al.] // 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE, 2014. –P. 452-456.*

*7. Analysis of vulnerability detection tool for web services / A. Murugan [et al.] // Int J Eng Technol, 2018. –P. 3-8.*

*8. Design and implementation of SQL injection vulnerability scanning tool / P. Techniques [et al.] // Journal of Physics: Conference Series. IOP Publishing, 2020. –P. 1-6.*

*9. Vulnerability detection and prevention of SQL injection / P.P Anaswara [et al.] // International Journal of Engineering & Technology, 2018. –P. 16-18.*

*10. Detection of SQL injection attacks: a machine learning approach / M. Hasan [et al.] // 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2019. –P. 1-6.*

UDC 004.934.8'1

## SPEAKER RECOGNITION USING NEURAL NETWORKS

*Lu Gangfan*

*group 267311*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus*

*Scientific supervisor: Petrov S.N., PhD, associate professor*

**Annotation.** This project demonstrates how to build a speaker recognition system using deep learning techniques. The system uses MFCC to extract features from audio data and capture spectral and time domain information of speech. After comparing traditional classification methods and neural network classification methods, then chooses a recurrent neural network (RNNs) to process of sequence data using. The project was trained and evaluated on the famous audio dataset VoxCeleb1 to train and evaluate various speaker recognition models using python. The system achieved a test accuracy of 93%. This result demonstrates that the system is able to effectively distinguish between different speakers.

**Keywords:** Speaker Recognition, MFCC, Deep Learning, Recurrent Neural Networks

***Introduction.*** Speaker recognition is a biometric technology that utilizes the voice characteristics of a speaker to verify or identify his or her identity. Traditional speaker recognition systems rely on manually created features and machine learning algorithms that can be limited in terms of accuracy and robustness. Deep neural networks can learn complex data representations and have achieved state-of-the-art results in various speaker recognition tasks.

In this paper, we introduce different classification methods and compare the limitations of traditional classification methods compared to neural networks. In recent years, deep learning has become a powerful tool for speech and audio processing tasks. Therefore, we propose a deep neural network-based speaker recognition system. In this system, the audio recordings are segmented into different segments, preprocessed to remove noise, features are extracted from the audio data by Mel Frequency Cepstrum Coefficients (MFCC), and then the sequence data is processed using Recurrent Neural Networks (RNN). We evaluated our system on the VoxCeleb1 dataset and tested it with 93% accuracy. Deep neural networks can learn complex representations of speech data and can be used to build robust and accurate speaker recognition systems.

***Main Part.*** The collected speech information is first removed from the muted portion and then noise reduction is performed using adaptive filtering or spectral subtraction to facilitate further subsequent processing. MFCC stands for Mel-Frequency Cepstral Coefficients, and it is a technique for extracting features from audio signals that are useful for speech recognition and other tasks. Here is the MFCC process:

1. Pre-emphasis. The first step is to apply a pre-emphasis filter to the audio signal, which boosts the high-frequency components and reduces the effect of noise. The pre-emphasis filter is a first-order high-pass filter, and it can be expressed as:

$$y[n] = x[n] - \alpha x[n-1]$$

Where x[n]is the input signal, y[n]is the output signal, and α is a constant between 0.9 and 1.0.

2. Framing and windowing. The next step is to divide the signal into short frames of equal length, typically 20 to 40 milliseconds. This is done because the frequency spectrum of the signal changes over time, and we want to capture the local characteristics of the signal. The frames are usually overlapped by 50% to avoid discontinuities at the frame boundaries. Each frame is then multiplied by a window function, such as a Hamming window, to reduce the spectral leakage caused by the finite length of the frame. The window function can be defined as:

$$w[n] = 0.54 - 0.46\cos\left(\frac{2\pi n}{N-1}\right)$$

Where w[n] is the window function, N is the frame length, and n is the sample index.

3. Fourier transform. The third step is to apply the discrete Fourier transform (DFT) to each frame to obtain the frequency spectrum of the signal. The DFT can be computed as:

$$X[k] = \sum_{n=0}^{N-1} x[n]w[n]e^{-j\frac{2\pi kn}{N}}$$

Where X[k] is the DFT of the frame, x[n]is the signal, w[n]is the window function, N is the frame length, k is the frequency index, and j is the imaginary unit.

4. Mel filter bank. The fourth step is to apply a set of triangular filters to the frequency spectrum to approximate the human perception of sound frequency. The filters are spaced according to the mel scale, which is a nonlinear scale that relates the perceived pitch of a sound to its actual frequency. The Mel scale can be defined as:

$$m = 2595\log_{10}\left(1 + \frac{f}{700}\right)$$

Where m is the Mel frequency, and f is the linear frequency. The filter bank consists of a number of filters, typically 20 to 40, that cover the entire frequency range. Each filter has a triangular shape, with a peak at the center frequency and zero values at the edges. The filter bank can be represented as a matrix, where each row corresponds to a filter and each column corresponds to a frequency bin. The filter bank can be applied to the spectrum by multiplying it element-wise and summing up the results. This produces a vector of filter bank energies, which represent the amount of energy in each filter.

5. Logarithm. The fifth step is to take the logarithm of the filter bank energies to compress the dynamic range and mimic the human loudness perception. The logarithm can be expressed as:

$$S[m] = \log\left(\sum_{k=0}^{K-1} H[m,k]\,|\,X[k]|^2\right)$$

Where S[m] is the log filter bank energy, H[m,k] is the filter bank matrix, X[k] is the spectrum, m is the filter index, k is the frequency index, and K is the number of frequency bins.

6. Discrete cosine transform. The final step is to apply the discrete cosine transform (DCT) to the log filter bank energies to obtain the MFCCs. The DCT can be computed as:

$$C[n] = \sqrt{\frac{2}{M}}\sum_{m=0}^{M-1} S[m]\cos\left(\frac{\pi n}{M}\left(m + \frac{1}{2}\right)\right)$$

Where C[n] is the MFCC, S[m] is the log filter bank energy, n is the cepstral index, m is the filter index, and M is the number of filters. The DCT reduces the correlation between the filter bank

energies and decorrelates the features. Usually, only the first 12 or 13 coefficients are kept, as they contain most of the relevant information. The MFCCs can also be augmented with the energy of the frame and the first and second derivatives of the MFCCs to capture the temporal dynamics of the signal.

A cornerstone in speech processing, MFCCs approximate the frequency resolution of the human auditory system. Through mathematical transformations applied to the frequency spectrum, MFCCs distill complex information into a compact yet expressive representation, crucial for nuanced speech pattern recognition. The resulting MFCC features are a compact representation of the speech signal that captures important information about the speaker's voice.

**Feature extraction** is the method and process of using computers to extract characteristic information in sound signals. During the speech recognition process, the text will be converted into a coded form and separated into syllables, phonemes, etc. Feature extraction is a crucial phase in the speech recognition process, involving the distillation of pertinent information from the preprocessed speech signal. This section delves into specific techniques employed to extract distinctive features, laying the groundwork for subsequent model training and recognition. Speaker recognition system whole workflow as Figure 1.

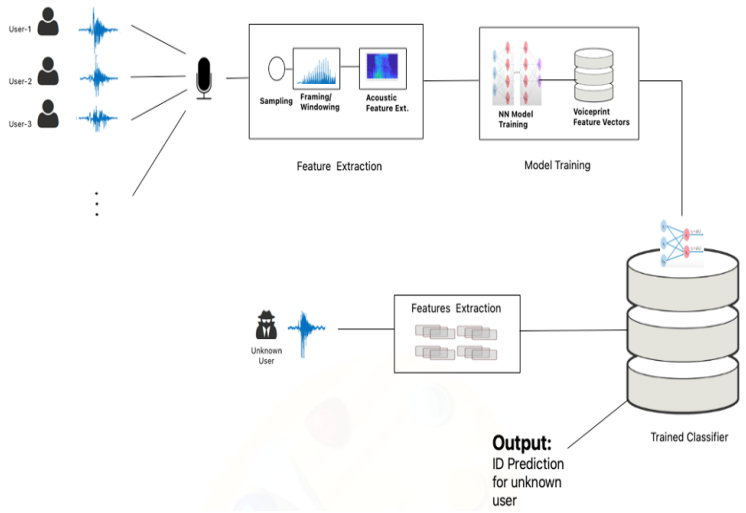



Figure 1 – Speaker recognition system workflow

## Spectrum Analysis

Spectrum analysis is an important part of feature extraction, aiming at revealing the basic frequency characteristics inherent in speech signals. The process of MFCC feature extraction is as follows: firstly, the speech signal is divided into several segments according to the time; then, the fast Fourier transform is performed on each segment of the signal, and the optical spectrum can be obtained after the transformation; according to the energy envelope of the optical spectrum, the energy envelope is discretized, and a vector can be obtained. This vector is the MFCC vector.

And the peaks and modes in the spectrogram can represent specific frequencies or modes in the audio signal. For example, a formant in speech can be recognized as a concentration of energy at a specific frequency.

**Temporal Feature**

Determines the fundamental frequency of the speech signal, representing the perceived pitch of the speaker's voice. Pitch extraction aids in capturing intonation patterns and is valuable for recognizing emotions and nuances in speech.

Zero Crossing Rate: Quantifies the rate at which the speech signal crosses the zero-amplitude axis. This feature is useful for discerning voicing characteristics and is applied in various speech analysis tasks.

**Statistcal Feature**

Extract statistical measures such as mean, variance, skewness, and kurtosis from the speech signal. These measures offer insights into the distribution and characteristics of the signal.
Energy Computation: Compute the energy of the speech signal over different frequency bands. Energy features help in distinguishing between voiced and unvoiced segments of speech.
The combination of spectral, temporal, and statistical features creates a comprehensive representation of the speech signal. These features collectively capture the nuanced patterns and variations essential for accurate speech recognition. To enhance computational efficiency and reduce redundancy, dimensionality reduction, the technique of Principal Component Analysis (PCA) is applied to the feature set. This step retains the most relevant information while minimizing the number of features.
Effective feature extraction transforms raw speech signals into compact, informative representations, laying the groundwork for subsequent stages in the speech recognition process. These features serve as the input to models, such as Recurrent Neural Networks (RNNs), fostering accurate and efficient recognition of spoken language.
This system uses Librosa (a Python package for audio analysis) provide tools to analyze and visualize audio data, including functions for optimizing feature extraction, time-series representation, and visualization of audio signals. It is commonly used in the field of music information retrieval and audio signal processing.

**Speech recognition technology classification**

The first category is model matching methods, including vector quantization (VQ), dynamic time warping (DTW), etc;
The second category is probabilistic statistical methods, including Gaussian Mixture Model (GMM), Hidden Markov Model (HMM), etc.;
The third category is discriminator classification methods, such as support vector machine (SVM), recurrent neural network (RNN), deep neural network (DNN), etc., as well as various combination methods.
Speaker recognition is actually a process of encoding first and then decoding. Signal processing and feature extraction are the encoding process. In other words, it is a pattern recognition based on speech feature parameters. That is, through learning, the system can classify the input speech according to a certain pattern, and then find the best matching result based on the judgment criteria.

**Neural networks**

Recurrent Neural Networks (RNNs) are neural networks that process sequential data, such as speech or text. In speech recognition, RNNs can learn the contextual information of the speech to improve the accuracy of the recognition. The role of MFCC is to extract relevant features from the audio data and then feed these features into subsequent layers of the RNN for higher level processing and interpretation. This integration improves the overall performance of the speech recognition model. Because of its ability to model sequential dependencies and capture temporal patterns in the data, the RNN is well suited for some aspects of speaker recognition. RNNs can also be used to model the variability in speech patterns, which is essential for robust speaker recognition systems.
When defining the RNN model, ReLu and SoftMax are activation functions used in different layers of the neural network model. ReLU (Rectified Linear Unit) is an activation function commonly used in hidden layers of neural networks. Mathematically, it is defined as ($f(x) = \max (0, x)$), which means that the output is zero for negative inputs and equal to the input for positive inputs. ReLU helps introduce non-linearity to the model, allowing it to learn complex patterns.
SoftMax is an activation function used in the output layer of a neural network for multi-class classification problems. It converts the raw output scores (logits) into probability distributions over multiple classes. The output of the SoftMax function is a vector where each element represents the probability of the corresponding class. The class with the highest probability is predicted as the final output. In the below model architecture, the last layer uses SoftMax activation to obtain probability distributions over the different classes (speakers) for the final prediction. The preceding layer uses relu activation for introducing non-linearity in the hidden layer. The choice of activation

functions depends on the nature of the problem and the desired properties of the network.
What's more, different types of loss functions serve different purposes, and the choice often depends on the nature of the problem you are trying to solve, this system uses Binary Crossentropy, Categorical Crossentropy, Sparse Categorical Crossentropy to evaluate the result.

***Conclusion.*** The proposed system implements a speaker recognition system based on Neural Networks using python. In experiments using the audio dataset VoxCeleb1 as the training set and test set, splitting the data into 70% train and the remaining will be split equally into validation and test datasets. The training parameters are set to learn at a rate of 0.001, and the optimizer uses Adam.

The training process monitors the classification accuracy and loss function changes. The project used accuracy, precision, recall, and F1-score as evaluation metrics. The results of the project showed that the neural network model performed the best on all metrics, achieving 0.95 accuracy, 0.93 precision, 0.95 recall, and 0.98 F1-score. The test results on the validation set can reach nearly 90% accuracy. In summary, the system achieved a test accuracy of 93% on the VoxCeleb1 dataset. It is shown that the use of neural networks combined with MFCC features is effective for speaker recognition tasks.

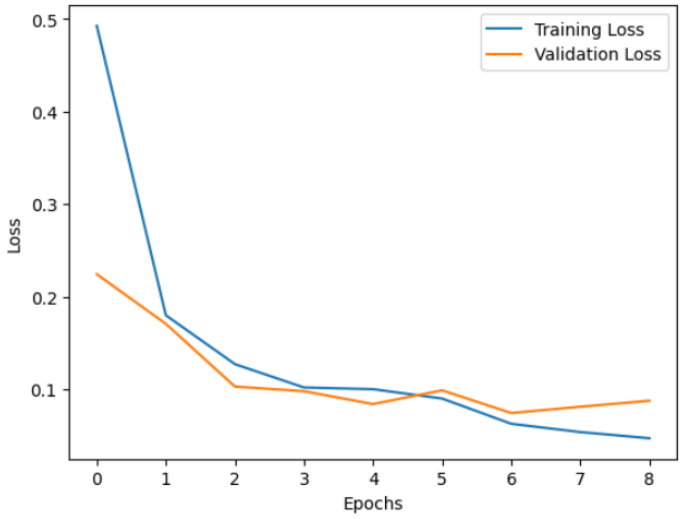



Figure 2 – Speaker recognition implementation and train results

Of course, it has many shortcomings and needs to deal with the effects of multiple factors, such as noise, accent, speech rate, intonation, and context. These factors can lead to changes and interference in the speech signal, reducing the accuracy and robustness of speech recognition. Therefore, algorithms and techniques for speech recognition need to be continuously optimized and improved to adapt to different speech scenarios and requirements.

## ***References***

*1. From Natural to Artificial Intelligence - Algorithms and Applications Edited by Ricardo Lopez-Ruiz*

*2. D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, "Speaker verification using adapted gaussian mixture models," Digital Signal Processing,*

*3. J. S. Chung, A. Nagrani, and A. Zisserman, "VoxCeleb2: Deep speaker recognition," Proc. Interspeech 2018, 2018, pp. 1086-1090.*

*4. Research on Speaker Recognition base on the Ensemble Deep Learning Model, Dewei Huang*

*5. Research on the Method of Voiceprint Recognition Based on Deep Neural Network, Pu Lili*

УДК 004.934.8'1

## РАСПОЗНАВАНИЕ ДИКТОРА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

*Лу Гангфань*

*гр. 267311*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Петров С.Н. – к.т.н., доцент*

**Аннотация.** Показан подход к построению системы распознавания диктора с использованием методов глубокого обучения. Система использует мел-частотные кепстральные коэффициенты в качестве характеристик аудиоданных. Проведено сравнение традиционных методов классификации и классификации с использованием нейронных сетей, по результатам сравнения для обработки речевых сигналов выбраны рекуррентные нейронные сети (RNNs). Модель, реализованная на языке программирования Python, была обучена на датасете VoxCeleb1. Точность распознавания (accuracy) составила 93%, что позволяет модели эффективно распознавать различных дикторов.

**Ключевые слова:** распознавание диктора, MFCC, глубокое обучение, рекуррентные нейронные сети

UDC 004.056

## TECHNIQUE OF INFORMATION SYSTEMS VULNERABILITIES MANAGEMENT

*C.A. Nguyen*

*group 367311*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus*

*Scientific supervisor: Boiprav O.V. – Cand. of Sci. (Tech.), Ass. Prof. of Department of IP*

**Annotation.** The report presents the results of the justification and development of the technique
of vulnerabilities searching and analyzing in information systems. This technique is based on the use of the OpenVAS vulnerability scanner and Windows or Kali Linux operating system.

**Keywords:** vulnerabilities, scanner OpenVAS, network security, CVE, NVD, Windows, Kali Linux.

***Introduction.*** Vulnerabilities, in the context of cybersecurity and software engineering, refer to weaknesses or flaws within a system that could be exploited by attackers to compromise
the security of the system. These vulnerabilities can exist in various components of software, hardware, networks, or even human processes. They create opportunities for unauthorized access, data breaches, denial of service attacks, or other malicious activities. Vulnerabilities have been registered by MITRE as a CVE (Common Vulnerability or Exposure), and assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to your organization. This central listing of CVEs serves as a reference point for vulnerability management solutions.
A vulnerability scanner is a software tool designed to assess computers, networks, or applications for security weaknesses or vulnerabilities. These tools typically automate

the process of identifying potential vulnerabilities by scanning for known security flaws in software, configurations, or network infrastructure. Vulnerability scanners can be either passive or active. Passive scanners observe network traffic and analyze it for potential vulnerabilities without interacting with the target system directly, while active scanners actively interact with the target system to identify vulnerabilities.

Several well-known commercial vulnerability scanners are widely used in the cybersecurity industry to assess the security posture of networks, systems, and applications: Nessus, GFI LANguard, XSpider (MaxPatrol). These scanners offer advanced features, comprehensive vulnerability databases, and professional support services. Unlike the listed scanners, OpenVAS, which stands for Open Vulnerability Assessment System, is an open-source vulnerability scanning and management tool. OpenVAS conducts comprehensive scans of network infrastructure, including servers, endpoints, and network devices, to identify security vulnerabilities. It employs various scanning techniques, including remote and authenticated scanning, to detect vulnerabilities in both online and offline systems. The OpenVAS vulnerability database includes about 52,000 checks, the so-called Network Vulnerability Tests (NVTs), as well as a connection to the CVE database, which describes known vulnerabilities. OpenVAS integrates with the National Vulnerability Database (NVD) and other sources of vulnerability intelligence to maintain an extensive database of known vulnerabilities. This enables it to provide up-to-date information on security flaws in software, operating systems, and third-party applications. Due to the indicated advantages of OpenVAS compared to other vulnerability scanners, this software tool was chosen as a tool for developing the technique [1–5].

***Main Part.*** The OpenVAS vulnerability scanner can be installed using VirtualBox as a virtual machine. To do this you need to follow these steps.

Step 1. Set the following parameters of the virtual machine to be installed in VirtualBox: operating system – Other Linux, RAM – 5120 MB, processors – 2, video memory – 9 MB, media – downloadable OVA file, network – network bridge.

Step 2. Complete the virtual machine installation process.

Step 3. Start installed machine and log in using the following login information: login – admin, password – admin.

Step 4. Create a new web administrator account.

Step 5. Open the web browser and enter the IP-address of virtual machine.

Step 6. Log in with the web administrator account created during the installation of the virtual machine.

The OpenVAS vulnerability scanner can also be installed in the Kali Linux operating system distribution. To do this, you need to follow the following steps.

Step 1. Completely upgrade your Kali Linux system by using the: sudo apt update && sudo apt upgrade -y command.

Step 2. Run the following command to download OpenVAS: sudo apt install openvas.

Step 3. Run the OpenVAS installer by running the following command: sudo gvm-setup.

Step 4. Generate a password for the first login.

Step 5. Check the OpenVAS settings by using the following command: sudo gvm-check-setup.

Step 6. Generate a new administrator password.

Step 7. Open the web interface: http://localhost:9293 or http://127.0.0.1:9392.

Step 8. Log in using the following credentials: username – admin, password – the new administrator password generated during installation

Generally speaking, the appliance can use two different approaches to scan a target: Simple scan or authenticated scan using local security checks. The following steps have to be executed to configure a simple scan:

Step 1. Creating a target.

Step 2. Creating a task.

Step 3. Running the task.

***Conclusion.*** During testing of the developed technique on 4 computers with operating systems Window 7 and Window 10, 4 vulnerabilities were discovered: 2 high risk vulnerabilities: SMB Brute Force Logins with Default Credentials (username and password are the same), Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (Microsoft MS17-010); 1 medium risk vulnerabilities: DCE/RPC and MSRPC services enumeration reporting; 1 low risk vulnerabilities: TCP timestamps.
It should be noted that OpenVAS provides the ability to generate reports based on the results of the scan performed. Reports can be displayed in the web interface and downloaded in a variety of formats making it easy for developers to use to fix vulnerabilities as well as monitor.

## *References*

*1. What are Vulnerabilities, Exploits, and Threats? [Electronic resource]. – Access mode: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/. – Date of access: 09.03.2024.*

*2. Best Vulnerability Scanning Tools. [Electronic resource]. – Access mode: https://thectoclub.com/tools/best-vulnerability-scanning-tools/. – Date of access: 09.03.2024.*

*3. OpenVAS. [Electronic resource]. – Access mode: https://www.bugcrowd.com/glossary/openvas-vulnerability-scanner/. – Date of access: 09.03.2024.*

*4. Greenbone Enterprise Appliance with Greenbone OS 22.04 – Manual // Greenbone AG. 2024. Chapter 5, chapter 10.*

*5. Kali Linux Install Guide – Greenbone Community Documentation. [Electronic resource]. – Access mode: https://greenbone.github.io/docs/latest/22.4/kali/index.html – Date of access: 09.03.2024.*

UDC 004.777

# SPEAKER IDENTIFICATION FOR SPEECH INFORMATION PROTECTION SYSTEMS

*Shakin K.P.[1], Makarenya E.A.[2], Dai Junyi [2]*

*[1] Joint Institute of Informatics Problems of the National Academy of Sciences of Belarus*
*Minsk, Republic of Belarus*
*[2] Belarusian State University of Informatics and Radio Electronics*
*Minsk, Republic of Belarus*

*O.B. Zelmansky – PhD, associate professor*

A structural diagram of the process of identifying an announcer using a neural network is considered. A method of identifying the voice of an announcer based on a neural network with a three-layer perceptron architecture is disclosed.

Today, one of the priority tasks for ensuring information security is to protect the speaker's speech. The solution of this problem is carried out using passive and active methods of information protection
In cases of protection of premises using active methods, white, pink and speech-like noise generators are used. In a number of experiments, it has been proven that the best masking effect is obtained using vibrations similar in spectral composition to the speech signal. Accordingly, in order to protect voice information, it is advantageous to give preference to speech-like interference protection systems.
In order to increase the efficiency of voice information protection, and thereby reduce the speaker speech intelligibility, it is proposed to use an announcer identification module for reconnaissance equipment using a

neural network, which will allow generating speech-like interference in the future in accordance with the voice features of the announcer.
The essence of identifying a speech announcer is to select, classify, and then respond to human speech from the input audio stream [1].
Announcer identification is the process of identifying a person from a voice pattern by comparing a given sample with patterns stored in the announcer database.
All speech recognition systems can be divided into two classes: ·

1. narrator-dependent systems; ·
2. systems independent of the announcer.

Given that human speech is highly variable, high-efficiency real-time identification of announcers requires high-speed computing. One way to solve speech identification problems is to use neural networks.
In any speech recognition system, there is always a step of comparing the input signal with the available standards. Regardless of the presence or absence of pre-processing of the signal (highlighting the main features, converting to another form in the new parametric space, etc.), the signal is a vector in the established parametric space, which will later be compared with vectors stored in memory to determine its belonging to a certain class.
Main stages of speech signal classification:
1. Extracting features from the input speech signal.
2. Build the narrator model (template) based on the feature vectors obtained in the previous step [2].
The procedure for identifying the announcer taken into account in the system by the input voice signal in all methods consists in selecting the most suitable saved model based on any criteria.
At the moment, there are various methods for classifying the speech signal, which allow solving the problem of identifying the announcer by voice. The most common are:

- dynamic programming method;
- vector quantization method;
- method of Gaussian mixtures;
- support vector method;
- hidden Markov model.

It is proposed to identify the announcer according to the scheme indicated in the figure below (Figure 1).
On an entrance of the module of voice identification of the announcer the audio signal arrives record of which happens via the microphone connected to an entrance of the sound card of the computer or already earlier written down signal is used. The acoustic component will transform a signal to a digital form with the set sampling frequency parameters. Then cleaning of a signal from noise, removal of the sites which are not bearing information is carried out, normalization of a signal and its splitting into the fixed intervals in a time domain on whom characteristics will be defined is carried out. In the block of allocation of characteristic signs there is an allocation of characteristic signs of a signal by means of Gilbert's transformation - Huanga. On an entrance of the "neural network" block the result from the previous block gets, further actions depend on the choice of an operating mode.

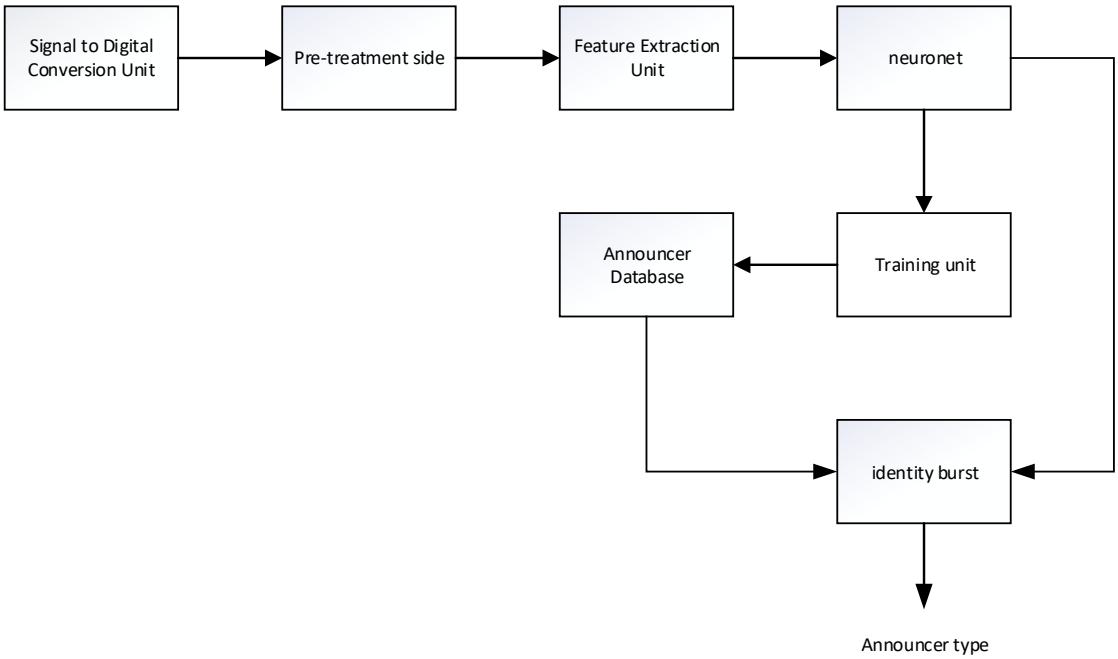



Figure 1. Block diagram of the narrator identification process

When choosing "training," data is transmitted to the training unit of the neural network, where it is trained and transmitted to the database. When choosing the "recognition" mode, the data goes to the identification unit, and data from the database unit with already stored data also comes to this unit. Then there is identification and classification (determination of belonging to a certain class), then the result of the announcer type is sent.

It is worth considering that before starting work, the user must add a database of announcers and train a neural network.

A neural network is a computational system or machine created to simulate analytical actions performed by a human brain and is a structure of neurons connected to each other and characterized by their internal properties, individual topology (architecture), as well as learning rules for obtaining the desired output signal.

Neural networks are models based on machine learning, that is, they acquire the necessary properties in the learning process, which consists in iteratively adjusting the network weights according to some rule called the learning algorithm.

One of the stages of the neural network functioning is training, during which data from the training set is alternately received at its input in order to adjust the weight coefficients of synaptic connections to obtain the most adequate signal at the output of the neural network. Training is carried out by sequential presentation of input vectors with simultaneous adjustment of weights in accordance with a certain procedure. During training, the weights of the network gradually become such that each input vector produces an output vector. There are three learning algorithms: "with teacher," "without teacher" (self-study) and mixed. In the first case, the neural network has the correct responses (network outputs) to each input example. Weights are adjusted so that the network produces answers as close as possible to the known ones. Teaching without a teacher is associated with such a concept as a pattern - by processing significant amounts of data, the algorithm must first independently identify patterns. At the next stage, based on the identified patterns, the machine interprets and systematizes the data. In mixed learning, some of the weights are determined through teaching with a teacher, while the rest is obtained through self-learning.

To solve the classification problem, it is proposed to use a neural network with a three-layer perceptron architecture. Its advantages include a comparative simplicity of analysis and a fairly high classification efficiency. By using the continuous excitation function, such networks are capable of generalizing the training set.

In conclusion, it is worth noting that the proposed method of identifying an announcer using a neural network with a three-layer perceptron architecture will reduce the time and resources spent, which in turn will increase the efficiency of the voice protection system.

***List of sources used:***

*1. Herbig T., Gerl F., Minker W. Self-Learning Speaker Identification: A System for Enhanced Speech Recognition. Berlin: Springer, 2011. 172 p*

*2. Speaker-by-voice-text identification [Electronic resource] – access mode: http://seminar.at.ispras.ru/wp-content/uploads/.*

*3. Koval, S. L. Comprehensive Voice and Speech Announcer Identification Methodology // S. L. Koval. Informatization and information security of law enforcement agencies: proceedings of the XX International Scientific Conference. Moscow.: Academy of Management of the Ministry of Internal Affairs of Russia, 2011. C. 364-370.*

UDC 528.854

## FACE RECOGNITION SYSTEM BASED ON PRINCIPAL COMPONENT ANALYSIS AND SUPPORT VECTOR MACHINE CLASSIFICATION

*Wang Kaiyu*

*group 267311*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus*

*Scientific supervisor: Boiprav O.V. – Cand. of Sci. (Tech.), Ass. Prof. of Department of IP*

**Annotation.** Principal component analysis is a commonly used feature extraction technology in face recognition. It can reduce the dimension of data while trying to retain the characteristics of the original data. Face images can be reduced in dimension through principal component analysis, which can effectively reduce the number of features and simplify the model. the complexity. The application of support vector machines in face recognition is based on its powerful classification ability that can effectively find decision boundaries in feature space and distinguish different categories (i.e. faces of different people). Based on the respective advantages of principal component analysis and support

vector machine, this article will discuss a face recognition method based on a combination of principal component analysis and support vector machine support vector machine method, and implement the system through MATLAB.

**Keywords:** face recognition, principal component analysis, support vector machine, MATLAB.

***Introduction.*** In recent years, with the rapid development of smart devices, facial recognition technology has become more and more widely used. At the same time, in the research field, various face recognition methods are emerging in endlessly. Among many methods, face recognition methods based on PCA and SVM are mainstream methods. Principal component analysis (PCA) [1], the discrete K-L transform, is the best orthogonal transform in image compression. PCA is a dimensionality reduction technique mainly used in the preprocessing stage of data. It transforms the original data into a new coordinate system through linear transformation, maximizing the variance of the data on the first few coordinate axes of the new coordinate system. Support vector machine (SVM) is a supervised learning method mainly used for classification and regression analysis. It separates different classes of data as accurately as possible by finding the best hyperplane in the feature space [2, 3].

In the process of combining PCA and SVM for image recognition, PCA is first used to reduce the dimensionality of the original high-dimensional data, extract the most important features, and then use SVM for classification. This combination takes advantage of the advantages of PCA in data preprocessing and feature extraction, and the efficiency and accuracy of SVM in high-dimensional data classification, making the entire recognition process both efficient and accurate. This paper implements a face recognition system based on PCA and SVM through MATLAB, and conducts experiments using the ORL face library. The recognition rate during training is as high as 94 %.

***Main Part.*** In the face recognition system based on PCA and SVM, the PCA method is first used to reduce the dimensionality of the image, which not only reduces the data size but also retains key features, thereby improving the efficiency of subsequent processing. Then, the SVM model is used to train and predict the dimensionally reduced data to achieve accurate face recognition. This process effectively combines the data reduction advantages of PCA and the powerful classification capabilities of SVM, making it an ideal choice for processing high-dimensional data and identifying complex patterns. Figure 1 shows the workflow of the entire system. This system will use the ORL face database as the training set and test set. This data set contains 40 directories, each directory has 10 images, and each directory represents a different person. All images are stored in PGM format, and each image is a 92×112 pixel, 256-level grayscale image. For the images in each directory, these images were collected at different times, under different lighting conditions, with different facial expressions and facial details. In the experiment of this system, 5 images of each person will be randomly selected as training images to form a training set of images, and the remaining 5 images form a test set.

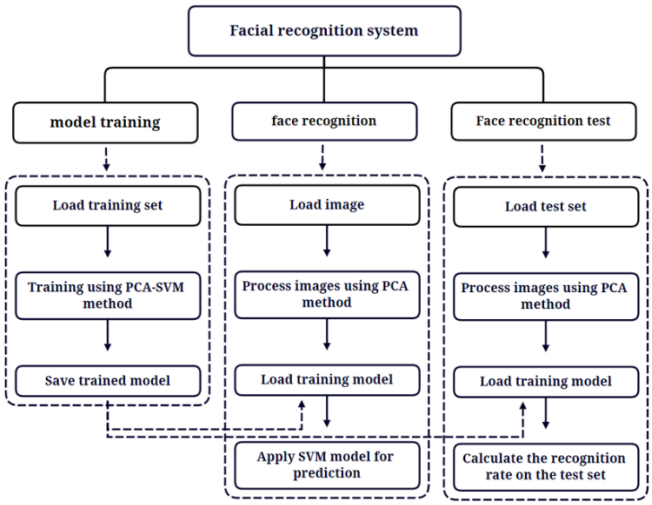



Figure 1 – PCA-SVM face recognition system workflow

The PCA method is an effective feature extraction method and is widely used in the field of pattern recognition, especially in face recognition research. By converting *mn*-dimensional two-dimensional face images into one-dimensional vectors, for example, a 92×112 image in the ORL face database can be regarded as a 10304-dimensional vector. In the high-dimensional space represented by these vectors, due to the similarity of the face structure, it can be effectively represented by a lower-dimensional subspace. This subspace is called "face space".

The main idea of PCA is to find those vectors that best describe the distribution of images in image space. These vectors can define the "face space". The length of each vector is *mn*, describes an image of $mn$, and is a linear combination of the original face image, called an "eigenface". For a face image of mn, connect each column to form a column vector of size $D = mn$ dimension. $D$ is the dimension of the face image, that is, the dimension of the image space. Assume $N$ is the number of training samples; $x$, represents the face vector formed by the $j^{th}$ face image; $u$ is the average image vector of the training samples, equation (1) represents the calculation of $u$, then the covariance matrix of the required samples is equation (2):

$$u = \frac{\sum_{j=1}^{N} x_j}{N}. \tag{1}$$

$$S_r = AA^T = \sum_{j=1}^{N} (x_j - u)(x_j - u)^{\mathrm{T}}. \tag{2}$$

According to the K-L transformation principle, the new coordinate system to be obtained consists of the eigenvectors corresponding to the non-zero eigenvalues of the matrix $AA^{\mathrm{T}}$. The calculation amount of direct calculation is relatively large, so the singular value decomposition (SVD) theorem is used to solve the eigenvalues and eigenvectors of $AA^{\mathrm{T}}$. According to the SVD theorem, let $l_i$ ($i = 1, 2, \ldots, r$) be the $r$ non-zero eigenvalues of the matrix $AA^{\mathrm{T}}$, and $v$ be the eigenvector of $AA^{\mathrm{T}}$ corresponding to 4. Since the larger the eigenvalue is, the greater the contribution of the corresponding eigenvector to image recognition is. Therefore, the eigenvalues are arranged according to size with use of equation (3):

$$p = \min_k \left( \frac{\sum_{i=1}^{k} l_i}{\sum_{i=1}^{r} l_i} \right) \geq 0.9, k \leq r. \tag{3}$$

Select the eigenvectors corresponding to the first p eigenvalues to form the dimensionally reduced eigenface subspace. Then the orthogonal normalized eigenvector $u$ of $AA^{\mathrm{T}}$. $T$ is according to the equation (4):

$$u_i = \frac{Av_i}{\sqrt{l_i}}, i = 1, 2, ..., p. \quad (4)$$

The eigenface space is according to the equation (5):

$$W = (u_1, u_2, u_3, ..., u_p). \quad (5)$$

Project the training sample y into the "eigenface" space $W$ to obtain a set of projection vectors $Y$, equation (6) represents the calculation of $Y$, which constitutes the training sample database for face recognition.

$$Y = W^{\mathrm{T}}Y. \quad (6)$$

After PCA transformation and dimensionality reduction of the image, an SVM classifier needs to be used for training and testing. The working principle of the classifier is to first learn the samples, pre-discriminate the samples, and learn and classify the extracted feature vectors. After classifying the classes, the test objects can be classified and discriminated by passing the test objects through the classifier. For this system, face recognition is also realized. The classification idea of SVM is based on structured risk minimization, taking into account the minimization of training error and test error, which is specifically reflected in the selection of classification models and model parameters. It can effectively guarantee the classification accuracy in small sample problems. The key to nonlinear support vector machines is how to map from low dimensions to high dimensions. This mapping relationship is called the kernel function and theoretically needs to satisfy Mercer's theorem. This system uses the currently mainstream RBF (radial basis kernel function), which implements a support vector machine classifier based on RBF [4]. This system directly uses the libsvm toolbox for SVM classification [5]. The libsvm toolbox is a simple, easy-to-use SVM pattern recognition and regression machine software package developed by C.JLin and others at National Taiwan University. This software package uses convergence The algorithm was improved based on the performance proof results and achieved good results. libsvm implements a total of 5 types of SVM; C-SVC, u-SVC, One Class-SVC, e-SVR and v-SVR, etc.

When training SVM, the impact of kernel functions and related parameters on model performance should be considered. This article uses the default RBF kernel function. First, the cross-validation method is used to find the best parameter $c$ (penalty factor) and parameter $g$ (variance in RBF kernel function), and then the best parameters are used to train the model. It is worth mentioning that when the performance of the models is the same, in order to reduce the calculation time, it is preferable to choose a parameter combination with a smaller penalty factor $c$. This is because the larger the penalty factor $c$, the more support vectors will be obtained in the end, and the amount of calculation will increase. The larger the value, the trained SVM model can be directly used for face image classification. The best accuracy obtained through cross-validation during the SVM training process is 94 %. After completing the SVM classification training, we have the SVM model, and we can use the trained SVM model to test the test set.

***Conclusion.*** The proposed system implements a face recognition system based on PCA and SVM methods through MATLAB. In experiments using the ORL face database as the training set and test set, the PCA-SVM method's face recognition achieved the best accuracy of 94 % through cross-validation during the SVM training process, and in the test on the test set The recognition rate is 85.5 %. The function implemented by this system is only the face recognition function. The complete face recognition process also includes the face detection part. If occlusion, posture transformation, etc. are involved, the recognition

method may still need to be adjusted.

## *References*

*1. Face recognition based on PCA algorithm / D. Yubo [et al.] // Proceedings of the 2009 China Instrumentation and Measurement and Control Technology Conference. – 2009.*

*2. Hasan, B. M. S. A review of principal component analysis algorithm for dimensionality reduction / B. M. S. Hasan, A. M. Abdulazeez // Journal of Soft Computing and Data Mining. – 2021. – Vol. 2 (1). – P. 20–30.*

*3. Mavroforakis, M. E. A geometric approach to support vector machine (SVM) classification / M. E. Mavroforakis, S. Theodoridis // IEEE transactions on neural networks. – 2006. – Vol. 17 (3). – P. 671–682.*

*4. Han S. Parameter selection in SVM with RBF kernel function / S. Han, C. Qubo, H. Meng // IEEE World Automation Congress. – 2012. P. 1–4.*

*5. Chang C.C. LIBSVM: a library for support vector machines / C. C. Chang, C. J. Lin // ACM transactions on intelligent systems and technology (TIST). – 2011. – Vol. 2 (3). – P. 1–27.*

УДК 528.854

## СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ НА ОСНОВЕ АНАЛИЗА ГЛАВНЫХ КОМПОНЕНТОВ И МЕТОДА ОПОРНЫХ ВЕКТОРОВ

*Ван Кайюй*

*магистрант группы 267311*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Бойправ О.В. – кандидат технических наук, доцент кафедры ЗИ*

**Аннотация**. Анализ главных компонентов – это широко используемая технология извлечения признаков при распознавании лиц. Она позволяет уменьшить размерность анализируемых данных при сохранении их характеристик. В частности, при использовании этого метода можно уменьшить размеры анализируемых изображений лиц и за счет этого эффективно уменьшить количество функций, необходимых для анализа, и упростить модель и сложность этого процесса. Применение метода опорных векторов в распознавании лиц основано на возможности эффективно находить с его использованием границы решений в пространстве признаков и различать разные категории (т. е. лица разных людей). В статье представлен реализованный с помощью MATLAB метод распознавания лиц, основанный на сочетании анализа главных компонентов и метода опорных векторов.

**Ключевые слова:** распознавание лиц, анализ главных компонент, метод опорных векторов, MATLAB.

УДК 004.415.53

## VINDOCTOR – СРЕДСТВО ИЗОЛИРОВАННОГО ЗАПУСКА ПРИЛОЖЕНИЙ

*Винокуров А.А., Доценко Е.В.*

*Национальный детский технопарк, г. Минск, Республика Беларусь*

*Научные руководители: Белоусова Е.С.– кандидат технических наук, доцент кафедры ЗИ; Мальцев В.Л. – заведующий лаборатории «Информационная безопасность» Национального детского технопарка*

**Аннотация.** В материалах доклада представлены результаты разработки средства изолированного запуска приложений VinDoctor. На основе изучения общей схемы работы современных SandBox и анализа их достоинств и недостатков был разработан алгоритм работы и пользовательский интерфейс средства изолированного запуска приложений VinDoctor. Тестирование разработанного средства показало, что VinDoctor не оказывает влияния на работу всей

операционной системы в целом по сравнению с существующими аналогами.

**Ключевые слова:** SandBox, средство изолированного запуска, вредоносные файлы, съемный носитель

***Введение.*** Средство изолированного запуска приложений (Sandbox, песочница) – это выделенная аппаратная или аппаратно-программная среда для исполнения файлов программ. Такая технология применяется, как правило, для эмуляции работы подозрительного программного кода в изолированной среде с целью снижения вероятности нарушения работы продуктивных систем.

Общая схема работы SandBox включает следующие этапы:

1 Начало работы. Запуск, инициализация окружения, проверка доступности системных ресурсов.

2 Изоляция процессов. Создание изолированного контейнера, ограничение доступа к фалойвой системе.

3 Контроль доступа. Определение политик контроля доступа для управления действиями приложения.

4 Мониторинг. Отслеживание активности приложения в реальном времени, регистрация попыток доступа к ресурсам и изменениям в системе.

5 Обнаружение и предотвращение угроз. Реализация механизмов обнаружения вредоносных действий в SandBox.

6 Завершение работы. Остановка и завершение изолированного окружения.

Таким образом, использование средства изолированного запуска приложений позволяет выявить неизвестные типы кибератак на основании поведенческого анализа вредоносного программного обеспечения.

Сегодня на рынке Sandbox производители предлагают несколько видов реализации средств изолированного запуска приложений: решение на базе аппаратной платформы или решение на базе облачного сервиса. Сравнительный анализ современных Sandbox (Comodo Free Antivirus, 360 Total Security) показал, что они являются неэффективными при проверке вредоносных файлов на внешних съемных носителях, содержащих неизвестные сигнатуры и используемые для реализации кибератак типа zero-day. Так, например, Comodo Free Antivirus вообще не определил на съемных носителях вредоносные файлы, а 360 Total Security определяет только сигнатурные вирусы, но при этом пропускает вредоносные файлы, посредством которых нарушитель может получить доступ к операционной систему и управлять ее элементами. Поэтому на основе проведенного анализа существующих SandBox решений было сформулировано предложение разработать новое средство изолированного запуска, в котором не будет всех представленных выше недостатков, которое будет способно выявлять вредоносные файлы разных видов.

***Основная часть.*** Для реализации средства изолированного запуска приложений VinDoctor был разработан алгоритм работы программы (рисунок 1).

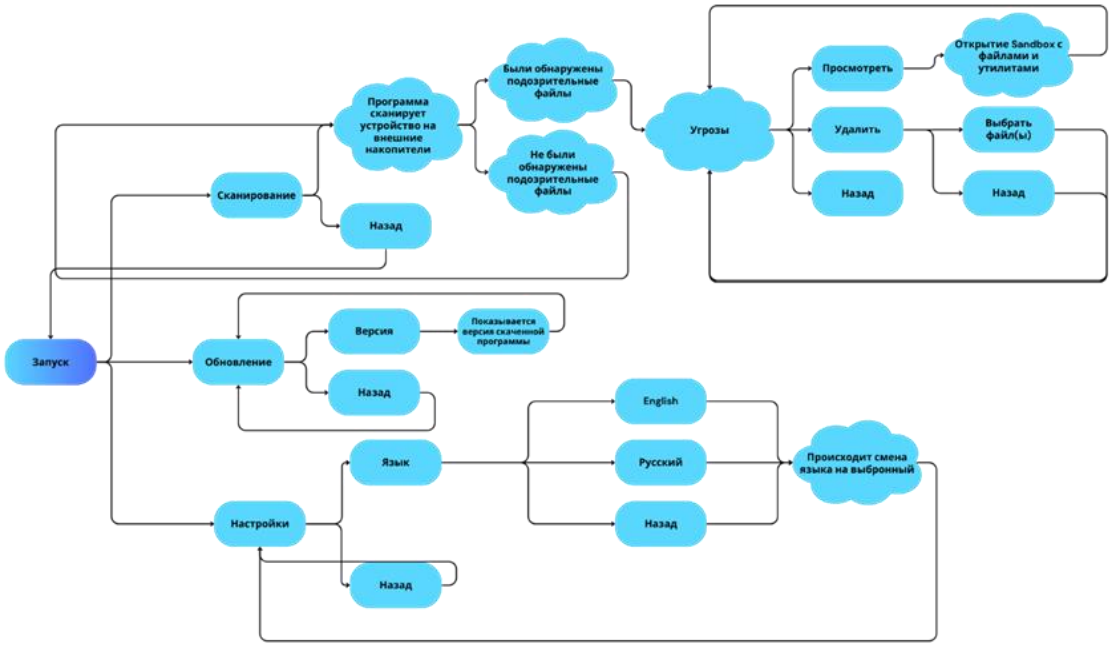



Рисунок 1 – Алгоритм работы средства изолированного запуска приложений VinDoctor

С помощью языка программирования Java (JDK21) был создан эргономичный пользовательский интерфейс средства изолированного запуска приложений VinDoctor, представленный на рисунке 2. Сканер для внешних накопителей был написан на языке программирование Python 3.9.5.

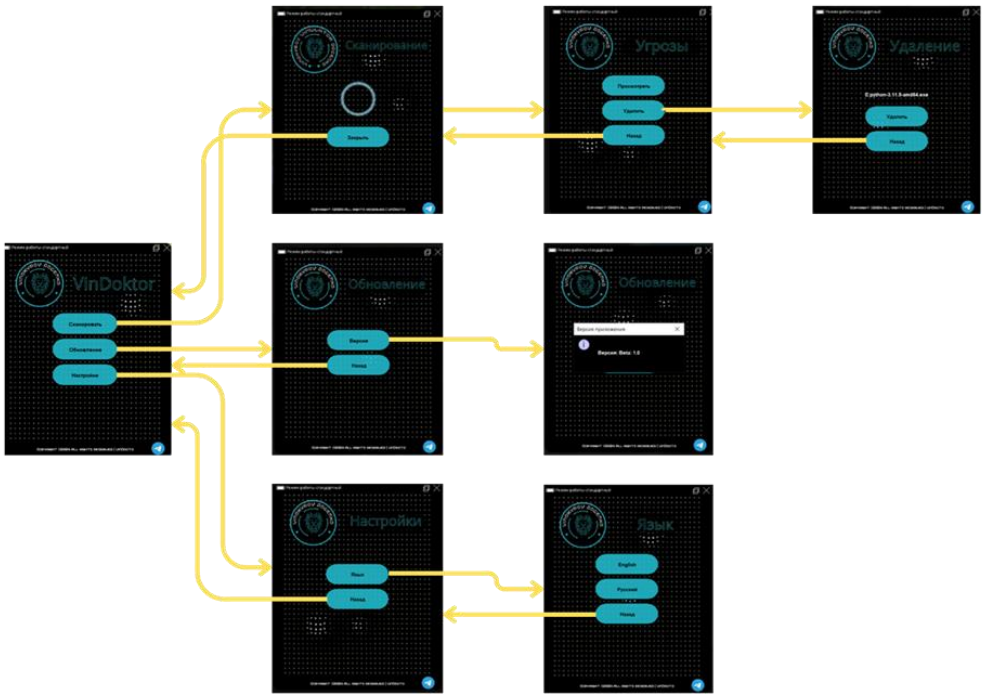



Рисунок 2 – Пользовательский интерфейс средства изолированного запуска приложений VinDoctor

Для проведения тестирования программного решения был разработан код на языке Python 3.9.5. Цель тестирования заключалась в систематическом измерения нагрузки на центральный процессор (ЦП), оперативную память и диск при работе со средством изолированного запуска приложений. При проведении тестирования пользователь активно взаимодействовал с программой VinDoctor, используя все её

возможности, а именно: изменял настройки программы, осуществлял сканирование внешнего носителя с вредоносным файлом и др.

***Заключение.*** В результате тестирования было установлено, что при сканировании внешнего накопителя с вредоносным файлом программой VinDoctor незначительно увеличивается нагрузка на ЦП. Получено, что средняя нагрузка на ЦП составляет 8,27 %, максимальная – 24,9 %, что говорит о том, что разработанное средство изолированного запуска приложений VinDoctor не оказывает влияние на работу всей операционной системы в целом по сравнению с существующими аналогами.

### *Список литературы*

*1. Терехов, С.Технология Sandbox как средство обеспечения кибербезопасности электронных государственных услуг / С. Терехов, Д. Шмырев // CONNECT. Мир информационных технологий. – № 9, 2017. – С. 106–109.*

*2. Антивирусные песочницы [Электронный ресурс]. – Режим доступа : https://habr.com/ru/articles/105581/– Дата доступа : 11.02.2024.*

UDC 004.415.53

## VINDOCTOR – ISOLATION LAUNCHING APPLICATIONS INSTRUMENT

*Vinokurov A.A., Docenko E.V.*

*National Children's Technopark, Minsk, Republic of Belarus*

*Belousova E.S. – PhD (Tech.), associate professor at the information security department;*
*Maltsau V.L. – Head of the information security laboratory at National Children's Technopark'*

**Annotation**. The results of developing for Isolation Launching Applications Instrument VinDoctor was presented in this article. The operating algorithm and user interface for the VinDoctor isolated application launcher were developed based on a studying of the general operating scheme of modern SandBoxes and an analysis of their advantages and disadvantages. Testing of the developed instrument VinDoctor showed that it does not affect the operating system in comparison to analogues.

**Keywords:** SandBox, Isolation Launching Applications Instrument, malicious files, flash memory card

УДК 004.777

## ПРОГРАММНЫЙ МОДУЛЬ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЕСТРЕ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

*Боровец Н.О.*

*гр. 367241*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Пулко Т.А. – канд. техн.наук, доцент*

**Аннотация.** Данная статья представляет обзор программного модуля, который будет разработан для обнаружения угроз информационной безопасности в реестре операционных систем семейства Windows. Модуль специализируется на обнаружении нежелательного подключения мобильных телефонов и незарегистрированных USB-накопителей в локальной сети организации, которые могут представлять серьезную угрозу для безопасности информации. Анализ основных проблем безопасности, связанные с такими устройствами, и предлагают решение в виде программного модуля, основанного на мониторинге реестра

Windows и анализе идентификационных данных подключенных устройств.

**Ключевые слова:** программный модуль, локальная вычислительная сеть, операционные системы семейства Windows, администратор, язык Python.

***Введение.*** В современном цифровом мире, где информационные технологии играют ключевую роль в деятельности организаций, обеспечение безопасности информации становится неотъемлемой задачей для любого предприятия. Особенно актуальным остается обеспечение защиты от внутренних угроз, таких как нежелательное подключение мобильных устройств и USB-накопителей к корпоративным сетям. Именно здесь встает задача разработки эффективных инструментов для обнаружения и предотвращения подобных угроз.

Одним из наиболее распространенных средств хранения конфиденциальной информации и настроек операционной системы Windows является ее реестр. Именно в этом ключевом компоненте системы скрыты потенциальные угрозы, связанные с нежелательным доступом и внесением изменений. В связи с этим возникает необходимость в разработке программного модуля, способного надежно обнаруживать угрозы информационной безопасности в реестре операционных систем семейства Windows.

***Основная часть.*** Целью разработки программного модуля является предоставление администраторам информации о подключенных устройствах, проверка их легитимности и обеспечение безопасности информационной среды организации.

Работа модуля будет иметь следующие особенности, он может работать как в ручном режиме, т.е администратор запускает модуль вручную через интерфейс или командную строку. Модуль начинает свою работу по анализу реестра Windows и сбору информации о подключенных устройствах и сетевых параметрах. Модуль сканирует реестр Windows на наличие записей о подключенных устройствах и сетевых настройках компьютера. После завершения анализа, модуль извлекает необходимую информацию о времени подключения мобильных телефонов и USB-накопителей, а также о сетевых параметрах компьютера, таких как IP-адрес и MAC-адрес, его имени в локальной сети организации. Полученная информация представляется администратору в удобном формате, возможно, через интерфейс программы или вывод в консоль. В зависимости от настроек модуля, администратор может выполнять дополнительные действия, такие как сохранение результатов в файл.

Также модуль может работать, как и в автоматическом режиме совместно с установленным антивирусном программным обеспечением на предприятии (к примеру, Kaspersky Endpoint Security), где создается задача на основании которой модуль запускается на всех компьютерах организации, где установлен антивирус.

Текстовое описание диаграммы вариантов использования модуля обнаружения угроз в реестре Windows:

- Администратор устанавливает и настраивает модуль;
- Администратор определяет параметры мониторинга реестра;
- Администратор настраивает журналирование действий модуля;
- Модуль мониторит реестр Windows на наличие новых записей о подключенных устройствах;
- Модуль анализирует идентификационные данные новых устройств;
- Модуль проверяет права доступа к подключенным устройствам;
- Модуль анализирует активность подключенных устройств;
- Модуль сравнивает идентификационные данные с зарегистрированными устройствами;

- Модуль ведет журнал действий для последующего анализа.

Для реализации поставленных целей принято решение об использовании в работе языка программирования Python. Данное решение обусловлено тем, что данный язык программирования легкий в освоении с простым и понятным синтаксисом. Это позволяет в перспективе упростить процесс сопровождения итогового решения, в случае смены разработчика.

***Заключение.*** Разработка и внедрение программных модулей для обнаружения угроз информационной безопасности в реестре Windows является важным шагом для обеспечения безопасности информации в современном бизнесе. Эти модули обеспечивают непрерывный мониторинг системы, анализируют активность и идентифицируют потенциальные угрозы, что позволяет оперативно реагировать на возможные инциденты и минимизировать риски для организации. Данный программный модуль разрабатывается на языке программирования Python.

### *Список литературы*

*1. Климов Александр, Чеботарев Игорь Реестр Windows – 2002-2012. Справочные материалы – 325с.*
*2. Денис Колисниченко Секреты, настройка и оптимизация реестра Windows – Санкт-Петербур 2010г. – 320с*
*3. Язык программирования Python : учеб.-метод. пособие / Д. Ю. Косицин. – Минск: БГУ, 2019. – 136с.*

UDC 004.777

## SOFTWARE MODULE FOR DETECTING INFORMATION SECURITY THREATS IN THE REGISTRY OF OPERATING SYSTEMS OF THE WINDOWS FAMILY

*Borovets N.O.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Pulko T.A. – Ph.D. technical sciences, associate professor*

**Annotation**. This article provides an overview of a software module that will be developed to detect information security threats in the registry of Windows operating systems. The module specializes in detecting unwanted connections of mobile phones and unregistered USB drives on the enterprise local network, which can pose a serious threat to information security. They analyze the main security problems associated with such devices and offer a solution in the form of a software module based on monitoring the Windows registry and analyzing the identification data of connected devices.

**Keywords:** software module, local area network, Windows operating systems, administrator, Python language.

УДК 004.777

## ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

*Габриелева Е. Г.*

*гр.274003*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Шаронова Е. И. – ведущий инженер-программист ОСТО ЦИИР*

**Аннотация.** В настоящее время защита информации в автоматизированных системах обработки информации является критически важной, так как множество данных хранится и обрабатывается в электронной форме, и их утечка или

компрометация может иметь серьёзные последствия. В данной статье рассматриваются основные угрозы кибербезопасности, методы по их преодолению и защите информации.

**Ключевые слова:** защита информации, автоматизированные системы обработки информации, шифрование

***Введение.*** В современном мире защита информации в автоматизированных системах обработки информации (АСОИ) является важным вопросом, так как АСОИ содержат большое количество конфиденциальных данных. Преимущества таких автоматизированных систем включают увеличение эффективности работы: автоматизация позволяет выполнять задачи быстрее и точнее, по сравнению с ручным вводом и обработкой информации. Автоматизация помогает устранять ошибки, связанные с человеческим фактором, такие как опечатки или неверное внесение данных, что улучшает качество и надёжность информации. Данная система также позволяет снизить затраты на ручную обработку данных и на документооборот. В целом, автоматизированные системы обработки информации помогают улучшить эффективность и надёжность работы, ускорить процессы и снизить риски ошибок, они способствуют улучшению принятия решений и координации работы в организации [1].

Однако наряду с вышеперечисленными преимуществами существует перечень проблем, возникающих в связи с увеличением объёмов информации и возрастающими угрозами в сфере кибербезопасности. Именно поэтому обеспечение надёжной защиты информации становится жизненно важным и особенно актуальным.

***Основная часть.*** Все угрозы в автоматизированных системах обработки информации, как показано на рисунке 1, делятся на непреднамеренные и преднамеренные. Первые чаще всего связаны с факторами внешней среды, а вторые – с незаконными действиями злоумышленников. Преднамеренные угрозы являются куда более опасными, чем непреднамеренные, так как данные могут быть не только уничтожены, но ещё и захвачены злоумышленниками.

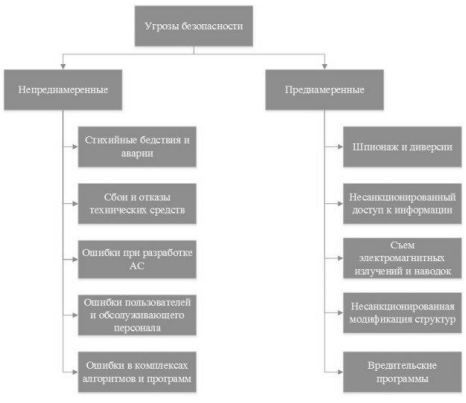



Рисунок 1 – Угрозы кибербезопасности

Далее подробнее рассмотрим самые распространённые угрозы кибербезопасности:

1. Атака на конфиденциальность: нападающие могут пытаться получить несанкционированный доступ к конфиденциальным данным;

2. Атаки на целостность: злоумышленники могут изменять или подделывать данные в автоматизированных системах;

3. Атака на доступность: целью таких атак является нарушение функционирования автоматизированных систем, чтобы лишить их пользователей доступа к сервисам или ресурсам;

4. Вирусы и вредоносные программы: атакующие могут внедрять вирусы и другие вредоносные программы в автоматизированные системы для получения контроля над ними или для нанесения вреда.;

5. Атака типа «отказ в обслуживании» (DDoS): злоумышленники могут использовать бот-сети, чтобы создать огромное количество запросов на сервер, перегружая его и вызывая отказ в обслуживании для легитимных пользователей, что может привести к временной недоступности системы или сервиса;

6. Сетевая атака: взломщики могут попытаться получить доступ в автоматизированные системы через сетевые уязвимости. Это может включать перехват данных, подделку пакетов или взлом сетевых устройств [2].

Все виды перечисленных угроз влекут за собой потерю или утечку данных, финансовые потери или нарушение работы систем. Это может нанести серьёзный ущерб бизнесу или привести к неправильным решениям, основанным на искажённых данных. Поэтому необходимо принимать ряд мер по защите автоматизированных систем.

Выстраивая систему защиты информации в автоматизированных информационных системах корпорации, IT-специалист может использовать различные методы, одновременное применение которых позволяет решать поставленные задачи. Они делятся на следующие подгруппы:

1. Защита данных от утраты в результате аварий или сбоя оборудования;

2. Контроль возможности физического доступа к аппаратуре, панелям управления и сетям, в результате которого возможно повреждение оборудования, хищение информации, намеренное создание аварийных или нештатных ситуаций, установка закладных устройств, позволяющих считывать звуковые и электромагнитные волны;

3. Аутентификация пользователей, программ, съёмных носителей информации;

4. Криптография: использование шифрования данных и цифровых подписей для обеспечения целостности и подлинности данных;

5. Защита сетей и связанных с ними ресурсов от несанкционированного доступа, что включает в себя использование сетевых файерволов, шифрования сетевого трафика, обнаружение вторжений;

6. Аудит и контроль: регулярное проведение аудитов системы для выявления возможных уязвимостей и слабых мест, а также постоянный контроль и мониторинг доступа к информации и действий пользователей;

7. Резервное копирование и восстановление в случае потери или повреждения [3].

Все эти меры должны быть комбинированы и подстроены под конкретные требования и характеристики автоматизированной системы обработки информации для наилучшего обеспечения защиты информации.

Рассмотрим один из надёжных способов защиты информации – её шифрование. Шифрование данных – это преобразование информации, делающее её нечитаемой для посторонних. Существует два основных вида шифрования: симметричное и асимметричное.

Симметричное шифрование для шифрования и дешифрования данных использует один и тот же криптографический ключ. Такой метод прост в работе и понимании, техническая нагрузка на оборудование невелика, и таким образом обеспечивается высокая скорость и надёжность шифрования. К недостаткам

относится сложность обмена ключами: при успешном перехвате ключа злоумышленник получит неограниченный доступ к зашифрованной информации. Advanced Encryption Standard (AES) – это симметричный алгоритм шифрования, использующий ключевое преобразование для защиты данных. Он обеспечивает высокую степень безопасности и эффективность.

Асимметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей: открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и проверки электронной подписи. Закрытый (приватный) ключ применяется для подписания и расшифровки данных, зашифрованных открытым ключом. RSA (алгоритм шифрования с открытым ключом) - это асимметричный алгоритм, который широко используется для шифрования обмена ключей и цифровой подписи [4].

Вне зависимости от выбранного вида шифрования, ни один из них не является гарантом стопроцентной безопасности. Поэтому нужно помнить, что любой подход нужно комбинировать с другими средствами информационной защиты.

***Заключение.*** Данная статья поможет читателям понять, какие меры необходимы для обеспечения безопасности информации в АСОИ, и научит применять соответствующие методы по её защите.

### *Список литературы*

*1. Сергеев, М. К. Автоматизированные системы обработки информации и управления // Актуальные исследования. – 2023. – №24 (154). – Ч.I. С. 58–63.*

*2. . Иванов, К. К. Угрозы безопасности информации в автоматизированных системах / К. К. Иванов, Р. Н. Юрченко, А. С. Ярмонов. — Текст: непосредственный // Молодой ученый. – 2016. – №29 (133). – С. 20–22.*

*3. Сайт компании Smart-Soft [Электронный ресурс] / Защита информации в автоматизированных системах. – 2020. – Режим доступа: https://www.smart-soft.ru/blog. – Дата доступа: 13.10.2023.*

*4. Сайт компании Индид [Электронный ресурс] / Шифрование. – 2022. – Режим доступа: https://indeed-company.ru/blog/shifrovanie/. – Дата доступа: 13.10.2023.*

UDC 004.777

## INFORMATION SECURITY IN AUTOMATED INFORMATION PROCESSING SYSTEMS

*Gabrieleva E. G.*

*gr.274003*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Sharonova E. I. – Senior Engineer-Programmer at OSTO CIIR*

**Annotation**. Currently, information security in automated information processing systems is critically important, as a vast amount of data is stored and processed in electronic form, and their leakage or compromise can have serious consequences. This article examines the main cyber threats, methods to overcome them, and information security measures.

**Keywords:** information security, automated information processing systems, encryption

УДК 004.777

# СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ

*Габрусь Е.В.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации, профессор*

**Аннотация.** В материалах доклада рассматривается разработка полномасштабной системы управления информационной безопасностью, которая выполняет функции комплексного управления, мониторинга и аудита информационной безопасности. Представлена система управления информационной безопасностью, основанная на принципах конфигурационного управления.

**Ключевые слова:** управление, архитектура системы

***Введение.*** В настоящее время практически ни одна организация не обходится без использования IT-технологий. Данные, обрабатываемые в информационных системах, могут иметь высокую ценность для компании. В таких случаях становится неприемлемым нарушение тех или иных характеристик безопасности (конфиденциальности, целостности и доступности) критичной информации, поскольку это может привести не только к серьезному ущербу, но и поставить под сомнение дальнейшее существование организации. В связи
с этим появляется необходимость в обеспечении защиты информации, обрабатываемой компанией.

Безусловно, необходимо использовать комплексный подход, содержащий в себе как применение организационных мер, так и использование технических (в том числе программных и аппаратно-программных) средств защиты информации.

***Основная часть.*** Основным способом обеспечения непрерывной деятельности предприятия является организация отказоустойчивости бизнес-процессов, производственных процессов, экономической и управленческой сферы. Однако в связи с ростом автоматизации задач, решаемых в рамках деятельности предприятия, остро стоит вопрос об обеспечении сохранности конфиденциальной информации, коммерческой и государственной тайны.
На ряду с применением специализированных средств противодействия кражи информационных ресурсов (далее – ИР) могут быть использованы система управления информационной безопасностью (далее – СУИБ) или система мониторинга защищённости информации (далее – СМИ). Ежегодно данные отчётов ведущих компаний об утечках информации и их последствиях: частичное или полное приостановление деятельности предприятий, огромные финансовые потери, говорят о необходимости не только обеспечения информационной безопасности (далее – ИБ), восстановлении информации после сбоя работы систем, но и об обеспечении комплексного управления ИБ.

Таким образом средняя утечка данных (количество данных на один случай) составила 2,93 миллиона записей, что на 35,2% меньше, чем в 2021 году (4,52 миллиона записей). Скорее всего, реальный «вес» одной утечки оказался выше, так как доля случаев, когда количество утекших записей была неизвестной, в 2022 году составила 58,8%. Однако, в 2021 году доля таких инцидентов была еще выше – 63,2%. Резкий рост количества утечек данных в последние годы главным образом

был спровоцирован беспрецедентным увеличением активности внешних злоумышленников, в том числе гибридных атак. Отчет компании InfoWatch по распределению утечек информации в мире по вектору воздействия за период 2017-2022 годы, с учетом неопределенных (то есть когда источник утечки определить не представляется возможным), приведен на рисунке 1.

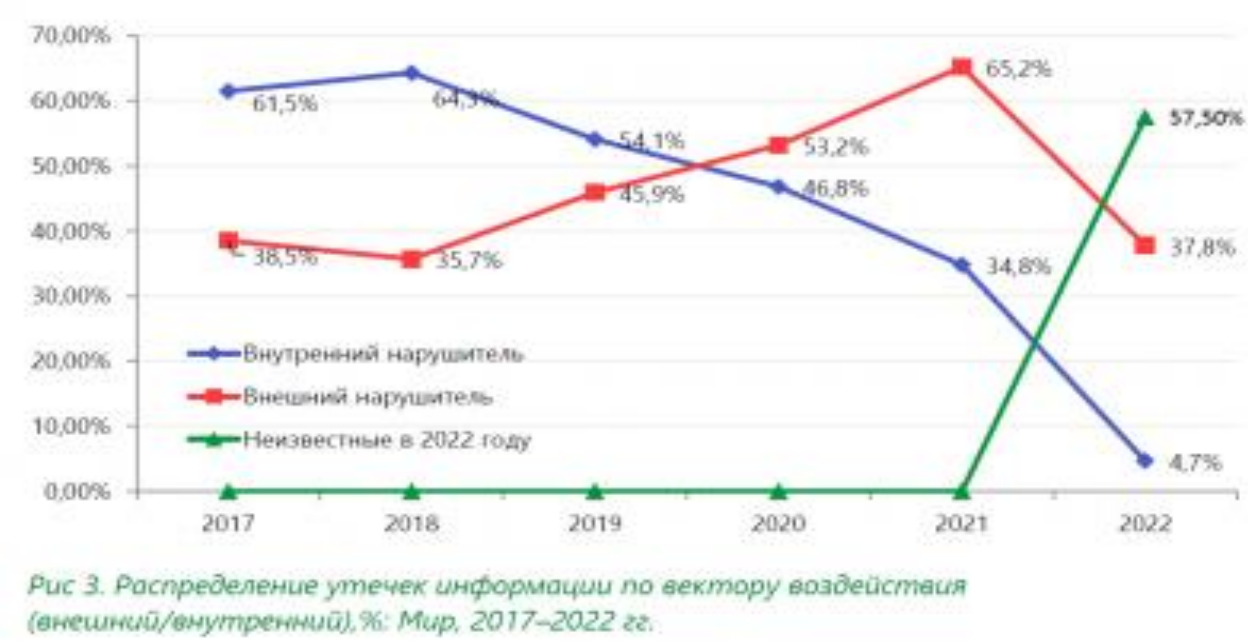



Рисунок 1 – Результаты исследования утечек информации компанией InfoWatch

Можно сделать вывод, что, не смотря на усовершенствование методик по защите информации, улучшение качества систем защиты информации (далее – СЗИ), хакерские навыки по осуществлению взлома СЗИ и выводу из строя защищаемых информационных систем позволяют достигнуть им своей цели: хищения критически важных ИР. При высокой численности утечек конфиденциальной информации, последствия для предприятий критические: невозможность найти виновного в краже информации, финансовые потери, рост социальной инженерии. По данным Zecurion Analytics за 2014 год, максимальный ущерб от одного инцидента ИБ в российских компаниях составил 30 миллионов долларов, средний ущерб в мире от одной утечки– 25 миллионов долларов. Из информации, представленной выше, следует, что кражи и утечки ИР увеличиваются, а убытки, нанесенные предприятиям, растут. Анализ показал, что применение СУИБ и СМИ позволяет снизить риски нарушения ИБ и оказать противодействие несанкционированному доступу к информации. Однако часто сложная реализация таких систем приводит к трудностям, возникающим при внедрении и использовании механизмов управления. Таким образом, СУИБ и СМИ должны обладать гибким механизмом администрирования. Современные СУИБ решают специализированную задачу, а не совокупность задач, это не позволяет использовать технологию комплексного управления. Для проектирования и реализации СУИБ предприятия, специалистами используется определенный метод управления: кибернетический (основан на принципах кибернетики и модели «черного ящика»), организационный (утвержденная политика ИБ и система внутренних документов, регламентирующих основные положения ИБ), процессный подход (непрерывность функционирования управленческих процессов), оптимизационный (поиск и применение оптимальных функций управления). Для

достижения эффективного управления ИБ, необходимо применять комплексный подход, представляющий собой совокупность методов управления, описанных выше. В качестве исследуемой проблемы предложена СУИБ, архитектура которой представлена на рисунке 2.

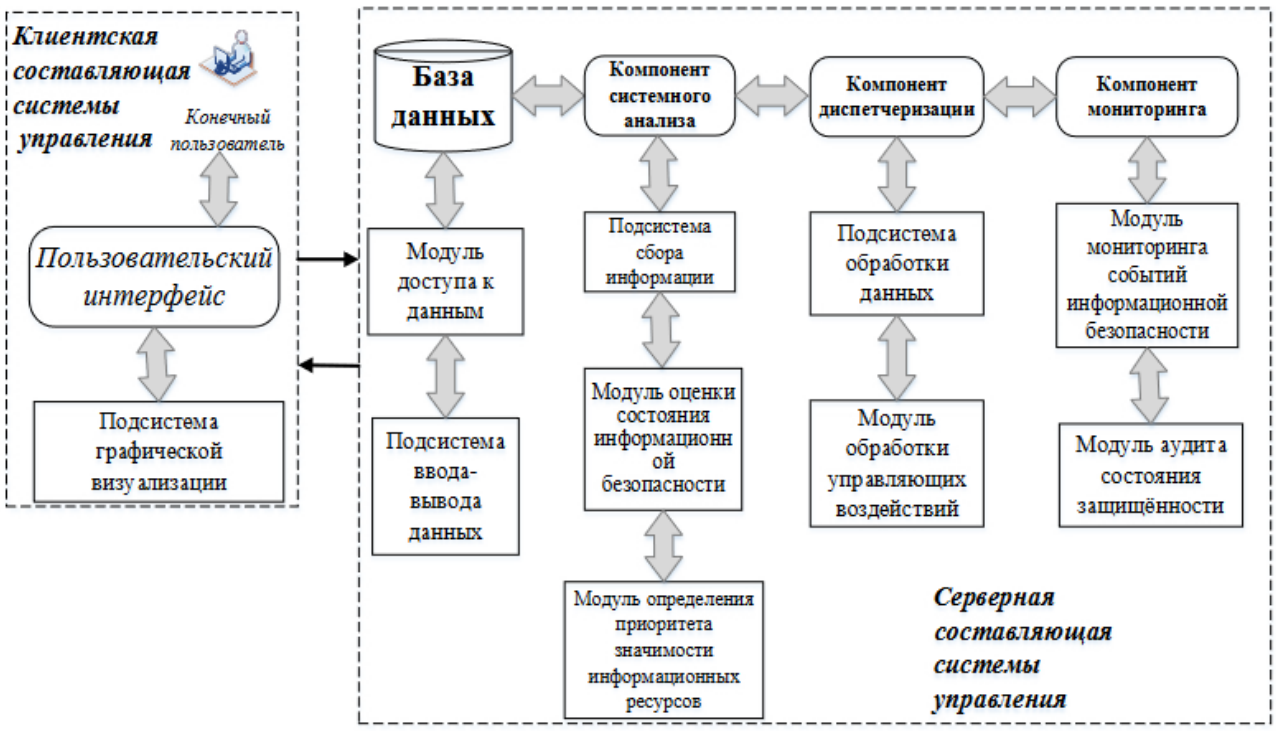



Рисунок 2 – Архитектура системы управления информационной безопасностью предприятия

Так как СЗИ распределенные и многозадачные, при разработке СУИБ будет использоваться концепция конфигурационного управления. Запланированная к разработке СУИБ представляет собой клиент-серверную систему. Клиентская часть позволяет взаимодействовать пользователю (специалисту по ИБ) с СУИБ по средствам пользовательского интерфейса. Для наглядного отображения функций управления в СУИБ заложена подсистема графической визуализации. Серверная часть включает в себя базу данных, компонент системного анализа, компонент диспетчеризации и компонент мониторинга. СУИБ объединяет функционирование четырех подсистем и шести модулей. Отличие запланированной к разработке СУИБ от ранее предложенных заключается в том, что набор конфигураций, позволяет сформировать систему многоуровневого управления.

***Заключение.*** Таким образом разработка и внедрения СУИБ и информационных технологий неразрывно связаны со стандартизацией процессов их управления, созданием нормативной, методической и регламентирующей базы. Кроме того, СУИБ отвечает за планирование, исполнение, контроль и техническое обслуживание всей инфраструктуры безопасности. Эффективность системы ИБ и труда администраторов средств ИБ будет чрезвычайно низкой при отсутствии средств сбора, анализа, хранения информации о состоянии системы ИБ, централизованного управления всеми ее составляющими. Дело в том, что каждое средство защиты реализует некоторую составляющую политики безопасности, которая на уровне подсистем задается набором параметров и требований.

### *Список литературы*

*1. Панасенко А.А. Конфиденциальные данные продолжают утекать. [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Threats_Analysis/Sensitive_data_continue_leak – Дата доступа: 15.02.2024.*

*2. Zecurion Analytics. Утечки конфиденциальной информации [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf – Дата доступа: 15.02.2024.*

*3. Сердюк Н.Н. Архитектура информационно-аналитической системы управления безопасностью производства. / Н.Н. Сердюк // Автоматизированные системы управления и приборы, 2014, № 167.*

*4. Козунова С.С. Информационная система управления информационной безопасностью организации // Наука и Мир. 2016. Т. 1. № 4(32), 59-60 с.*

*5. Козунова С.С., Бабенко А.А. Автоматизация управления инвестициями в информационную безопасность предприятия //Вестник компьютерных и информационных технологий, 2015, № 3 (129), 38-44 с.*


UDC 004.777

## INFORMATION SYSTEMS SECURITY MANAGEMENT SYSTEM

*Habrus Y.V.*

*gr.367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Borbotko T.V. – Dr. of Sci. (Tech.),* head of the department of information security, *professor*

**Annotation**. The report discusses the development of a full-scale information security management system, which performs the functions of integrated management, monitoring and audit of information security. An information security management system based on the principles of configuration management is presented.

**Keywords:** management, system architecture

УДК 537.87:539.216

## КОНСТРУКЦИИ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ГОФРИРОВАННОЙ МЕТАЛЛИЗИРОВАННОЙ ПОЛИМЕРНОЙ ПЛЕНКИ

*Гладинов А.Д.*

*аспирант кафедры защиты информации*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Богуш В.А. – доктор физико-математических наук, профессор*

**Аннотация.** В докладе приведены результаты исследования взаимодействия электромагнитного излучения СВЧ-диапазона с тонкопленочными экранами в виде гофрированной металлизированной полимерной пленки. Эти результаты включают в себя закономерности изменения значений коэффициентов отражения и передачи электромагнитного излучения таких экранов в зависимости от высоты гофра.

**Ключевые слова:** экранирование электромагнитного излучения, отражение, передача

***Введение.*** Электромагнитное излучение (ЭМИ) повсеместно окружает человека во всех сферах его деятельности и оказывает влияние как на него самого, так и на окружающие его на работе и в быту изделия электронной техники (ИЭТ). Основные области применения электромагнитных экранов приведены на рисунке 1 [1].

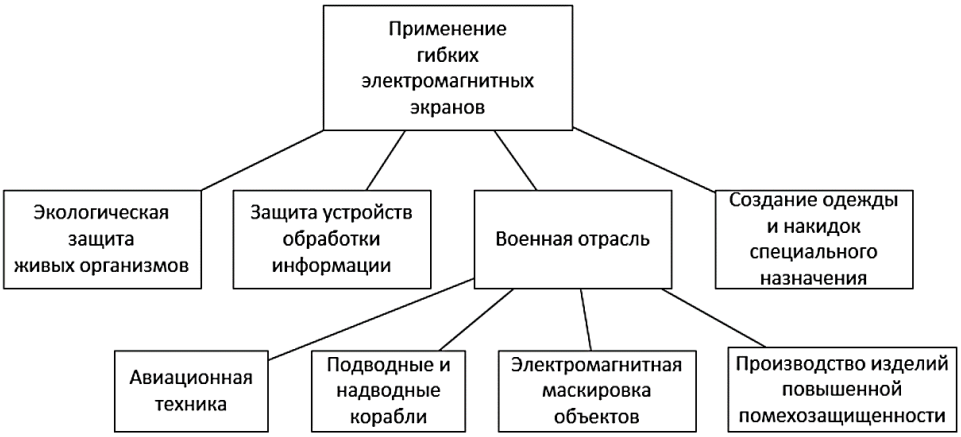



Рисунок 1 – Основные области применения электромагнитных экранов

Перспективным направлением защиты от ЭМИ является совершенствование конструкций и технологии изготовления экранов ЭМИ. Кроме того, для повышения эффективности экранирования необходимы исследования и поиск новых материалов, конструкций и технологий их изготовления. Применение полимерных материалов в качестве основы для экранов ЭМИ позволит снизить их массу, тем самым расширит возможности их использования при защите от ЭМИ.

***Основная часть.*** Для изготовления экранов ЭМИ была выбрана многослойная пленка на полиэтиленовой основе Kotar IZOFOLIX [2]. Данная пленка имеет толщину 105 мкм и представляет многослойную структуру, на один из внутренних слоев которой нанесена металлизация Al толщиной 150 нм. Общий вид пленки приведен на рисунке 2.

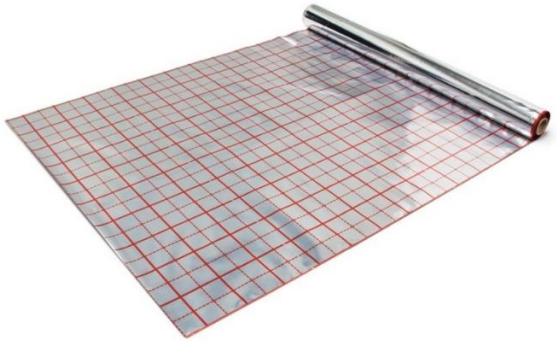
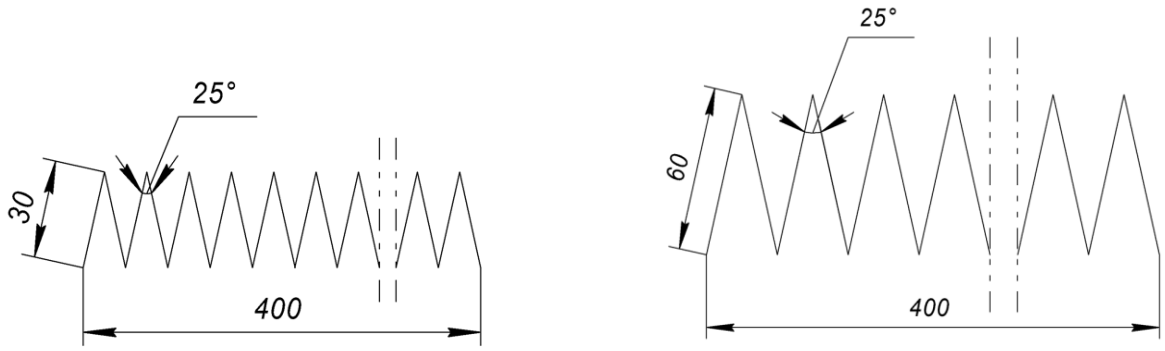


Рисунок 2 – Общий вид пленки Kotar IZOFOLIX

Экраны ЭМИ изготавливались путем гофрирования указанной пленки, которое заключалось в складывании ее в виде «гармошки» с разной высотой. Для исследований были выбраны высоты гофра, равные 30, 60 и 90 мм, обусловленные кратностью длине электромагнитной волны в гигагерцовом диапазоне частотных измерений. Размеры экранов составляли 300×400 мм. Схема электромагнитных экранов с высотой гофров 30 и 60 мм и углом при вершине 25° представлена на рисунке 3.




*a* *b*

Рисунок 3 – Схема гофрированного электромагнитного экрана с высотой (*a* – 30 мм, *b* – 60 мм)

Измерение значений коэффициентов отражения и передачи изготовленных экранов ЭМИ проводилось в диапазоне частот 2,0…17 ГГц. При исследованиях использовался измерительный модуль коэффициентов передачи и отражения SNA 0.01–18. Все измерения проводились в 2 этапа. На первом этапе проводилась калибровка установки для измерений в заданном диапазоне частот. На втором этапе выполнялись измерения коэффициентов отражения и передачи.

По результатам проведенных измерений без использования металлического отражателя установлено, что в диапазоне частот от 2…17 ГГц (рисунок 4), значения коэффициентов отражения ЭМИ экрана (с высотой гофра 30 мм изменяется в диапазоне значений от – 0,3 дБ до – 7 дБ, для гофра высотой 60 мм — в диапазоне от – 0,1 дБ до – 14 дБ и для гофра высотой 90 мм — в диапазоне от – 0,5 дБ до – 14 дБ. При этом наблюдается характерное резонансное увеличение коэффициента отражения в диапазоне частот 5…8 ГГц, а также 11…14 ГГц при всех высотах гофр.

По результатам проведенных измерений с использованием металлического отражателя установлено, что в диапазоне частот от 2…17 ГГц (рисунок 5) значения коэффициентов отражения экранов с высотой гофра 30 мм изменяется в пределах от – 0,1 дБ до 11 дБ, а экранов с высотой гофра 60 и 90 мм – соответственно в пределах от – 0,1 до – 12 дБ и от – 1 до – 16 дБ. Также наблюдается увеличение коэффициента отражения в диапазонах частот 3…5 ГГц, 7…9 ГГц и 13…16 ГГц.

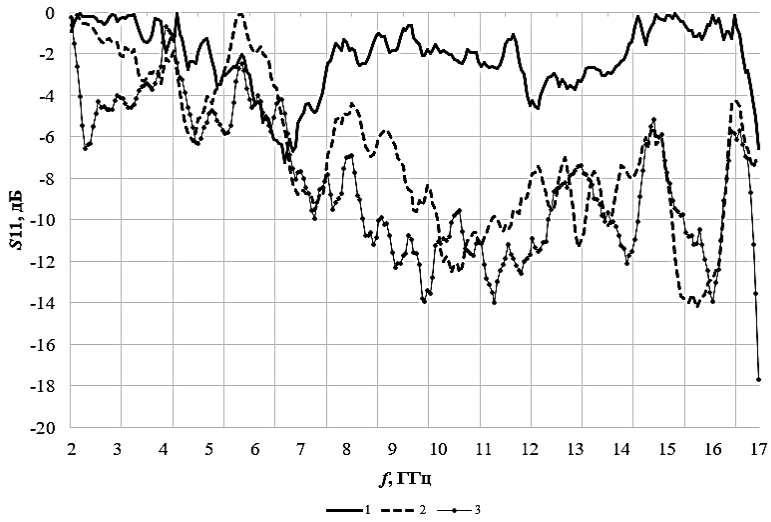



Рисунок 4 – Частотные зависимости коэффициента отражения ЭМИ в диапазоне частот 2,0…17 ГГц (без металла)
Высота гофра, мм: 1 – 30, 2 – 60, 3 – 90

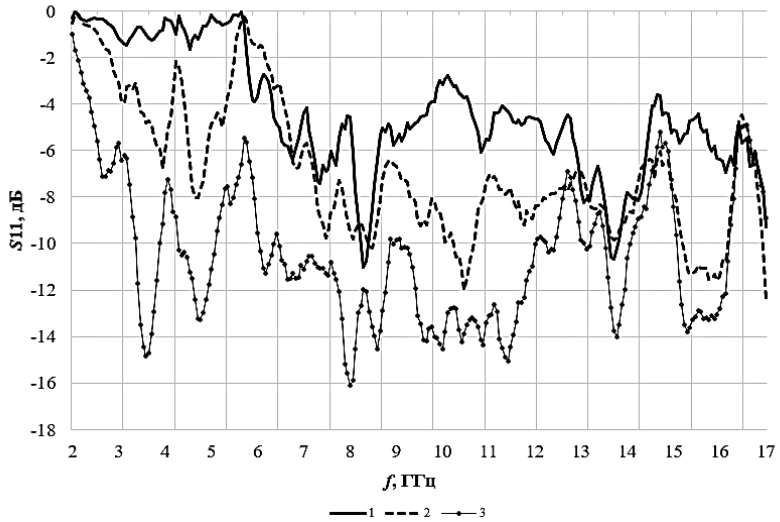



Рисунок 5 – Частотные зависимости коэффициента отражения ЭМИ в диапазоне частот 2,0…17 ГГц (с металлом). Высота гофра, мм: 1 – 30, 2 – 60, 3 – 90

По результатам измерений коэффициента передачи в диапазоне частот 2…17 ГГц (рисунок 6) было установлено, что его значения изменяется в диапазоне от – 40 до – 18 дБ. Сравнение значений коэффициентов передачи экранов ЭМИ с выстой гофра 30, 60 и 90 мм показало, что изменение высоты гофра не оказывает существенного влияния на величину коэффициента передачи.

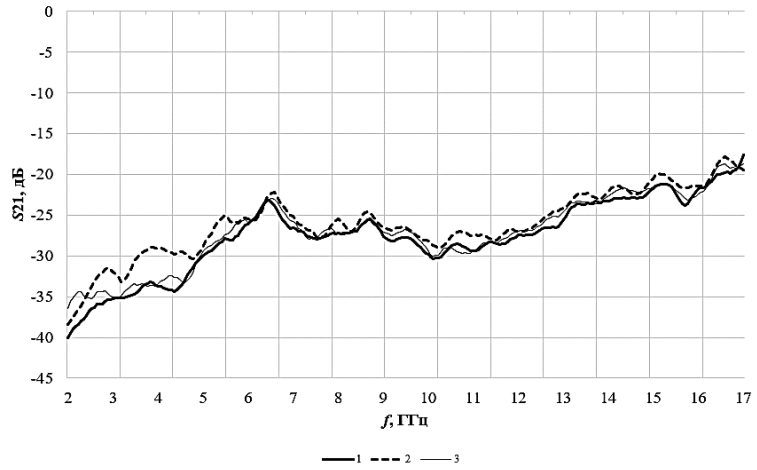



Рисунок 6 – Частотные зависимости коэффициента передачи ЭМИ в диапазоне частот 2,0…17 ГГц. Высота гофра, мм: 1 – 30, 2 – 60, 3 – 90

***Заключение.*** На основе полученных результатов можно сделать вывод о том, что гофрирование экрана ЭМИ из многослойной пленки на полиэтиленовой основе Kotar IZOFOLIX оказывает влияние на величину его коэффициента отражения электромагнитного излучения в диапазоне частот 2…17 ГГц. Установлено, что при увеличении высоты гофра с 30 до 90 мм коэффициент отражения ЭМИ возрастает в 2 раза (измерения без металла) и в 1,45 раза (измерения с металлом). Данное увеличение связано с увеличением числа переотражений электромагнитного излучения от боковых поверхностей гофра. Показано, что гофрирование экрана не оказывает значительного влияния на значения его коэффициента передачи ЭМИ.

## *Список литературы*

*1. Абасов, Р. К. Применение углеродных материалов в экранировании электромагнитных полей / Р. К. Абасов // Политический молодежный журнал. – 2016. – № 5. – С. 1 – 7.*

*2. Изоляционная фольга IZOFOLIX [Электронный ресурс] – Режим доступа : https://www.kotar.pl/ru/oferta/folie-izolacyjne/108-folia-izolacyjna-izofolix-rus. – Дата доступа : 14.02.2024*

UDC 537.87:539.216

## DESIGNS OF ELECTROMAGNETIC SHIELDS BASED ON CORRUGATED METALLIZED POLYMER FILM

*Gladinov A.D.*

*Postgraduate student of Information Protection Department*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Bogush V.A. – Doctor of Sciences (Physical and Mathematical), Professor*

**Annotation**. The report presents the results of study of microwave electromagnetic radiation interaction with thin-film shields in the form of corrugated metallized polymer film. These results include patterns of changes in the values of electromagnetic radiation reflection and transmission coefficients of such shields depending on the height of the corrugation.

**Keywords:** electromagnetic radiation shielding, reflection, transmission

УДК 004.056:004.7

## МЕТОДИКА КОНФИГУРАЦИИ КОНТРОЛЛЕРА ДОМЕНА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ

*Григорян О.П., Пискунова Е.С.*

*гр.161401*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белоусова Е.С. – кандидат технических наук, доцент кафедры ЗИ*

**Аннотация.** В материалах доклада рассматривается конфигурация контроллера домена на основе Active Directory, которое позволяет централизованно управлять пользователями, группами и компьютерами в сети. Реализация данной службы позволяет администраторам эффективно управлять безопасностью в сети, определяя права доступа пользователей к различным ресурсам

**Ключевые слова:** обеспечение безопасности, Active Directory, контроллеры доменов

***Введение.*** С увеличением числа угроз кибербезопасности и развитием цифровых технологий обеспечение безопасности информации и сетей становится все более критически важным для организаций, поскольку утечка конфиденциальных данных или нарушения в работе сети могут повлечь серьезные последствия. Одним из фундаментальных элементов инфраструктуры сети в среде Windows Server является Active Directory, который обеспечивает централизованное управление и высокий уровень информационной безопасности сети.

Active Directory – это служба каталогов, которая используется для управления ресурсами в локальной сети организации. Другими словами, Active Directory – это центральная база данных, в которой хранится информация о пользователях, группах, компьютерах и других сетевых устройствах. Active Directory предоставляет службы аутентификации и авторизации, позволяя пользователям аутентифицироваться на устройствах и получать доступ к ресурсам в соответствии с их правами. Основными элементами структуры управления сети являются домены,

контроллеры доменов, деревья и леса доменов. Домены – это логические группы объектов, контроллеры доменов хранят информацию и управляют доступом к ресурсам, а деревья и леса доменов представляют собой иерархические структуры, объединяющие связанные домены и деревья в единую систему управления. В рамках сети, использующей Active Directory, серверы DHCP (Dynamic Host Configuration Protocol) и DNS (Domain Name System) играют важную роль в обеспечении бесперебойной работы сети. Сервер DHCP предназначен для автоматического назначения IP-адресов устройствам в сети, что упрощает доступ к сетевым ресурсам, в то время как сервер DNS отвечает за разрешение имен узлов в сети в IP-адреса, обеспечивая правильную адресацию и доступ к ресурсам.

Проведение научной работы по данной теме на практике позволит выявить оптимальные стратегии и методы обеспечения безопасности с использованием Active Directory. Это поможет организациям повысить уровень защиты своих данных и сетевой инфраструктуры, что является крайне актуальным в наше время.

***Основная часть.*** Для реализации службы Active Directory в роли администратора используется виртуальная машина с серверной операционной системой Windows Server, а в роли пользователя – виртуальная машина с операционной системой Windows 10.

Для первоначальной конфигурации контроллера необходимо создать домен и обеспечить связь между администратором и пользователем. Для организации вычислительной сети установлены Active Directory Domain Service (AD DS), DHCP-сервер и DNS-сервер. На рисунке 1 изображена панель мониторинга всех установленных серверов.

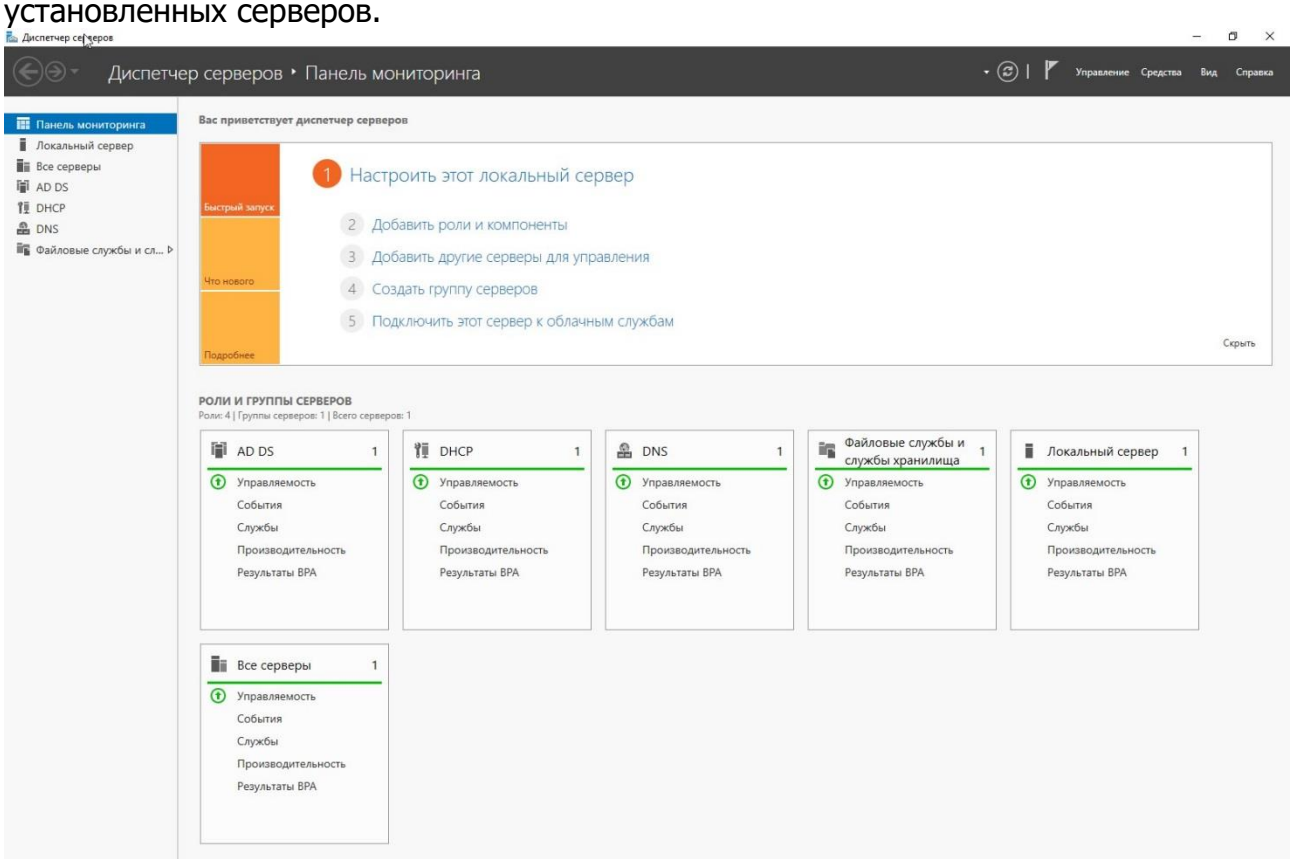



Рисунок 1 – Панель мониторинга установленных серверов

Следующий шаг настройки – добавление пользователей и разграничение их прав. На рисунке 2 представлена начальная страница входа в систему пользователя, где указан уже настроенный домен GP.

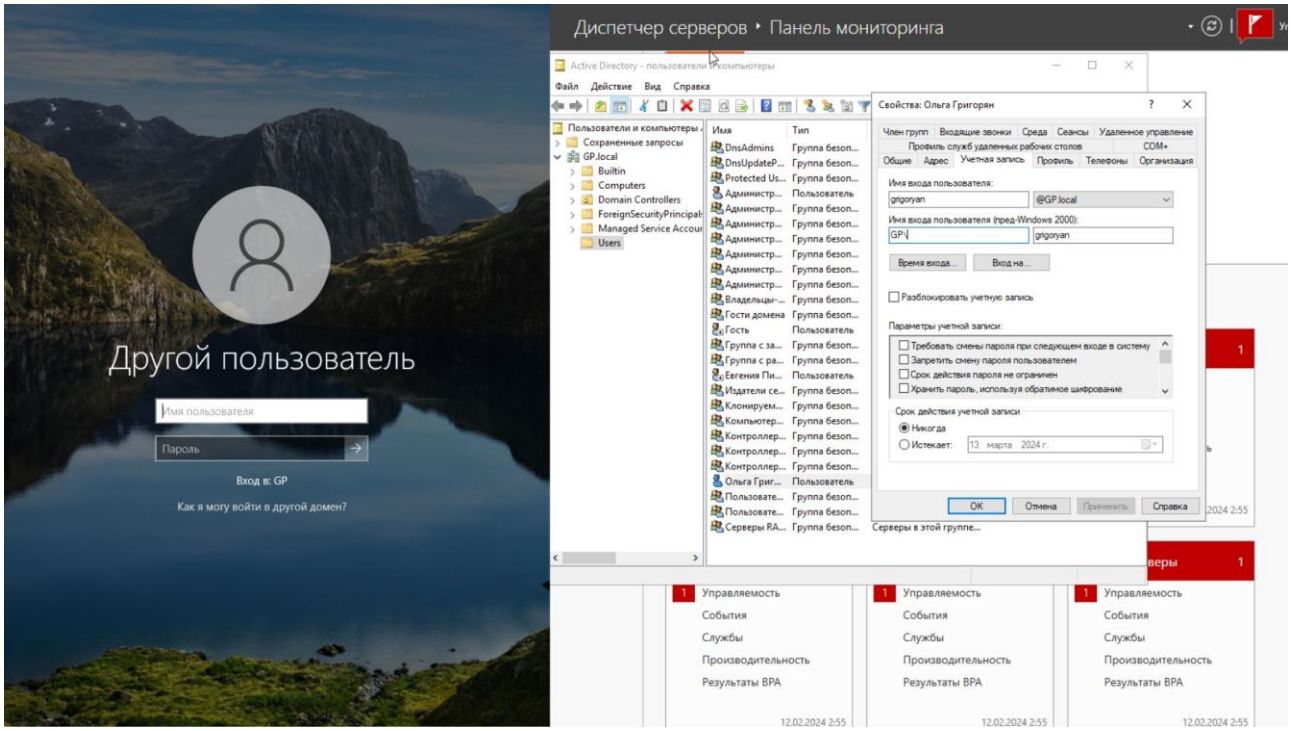



Рисунок 2 – Вход пользователя в домен

Также необходимо настроить раздачу IP-адресов по протоколу DHCP. На рисунке 3 отображен результат работы сервера.

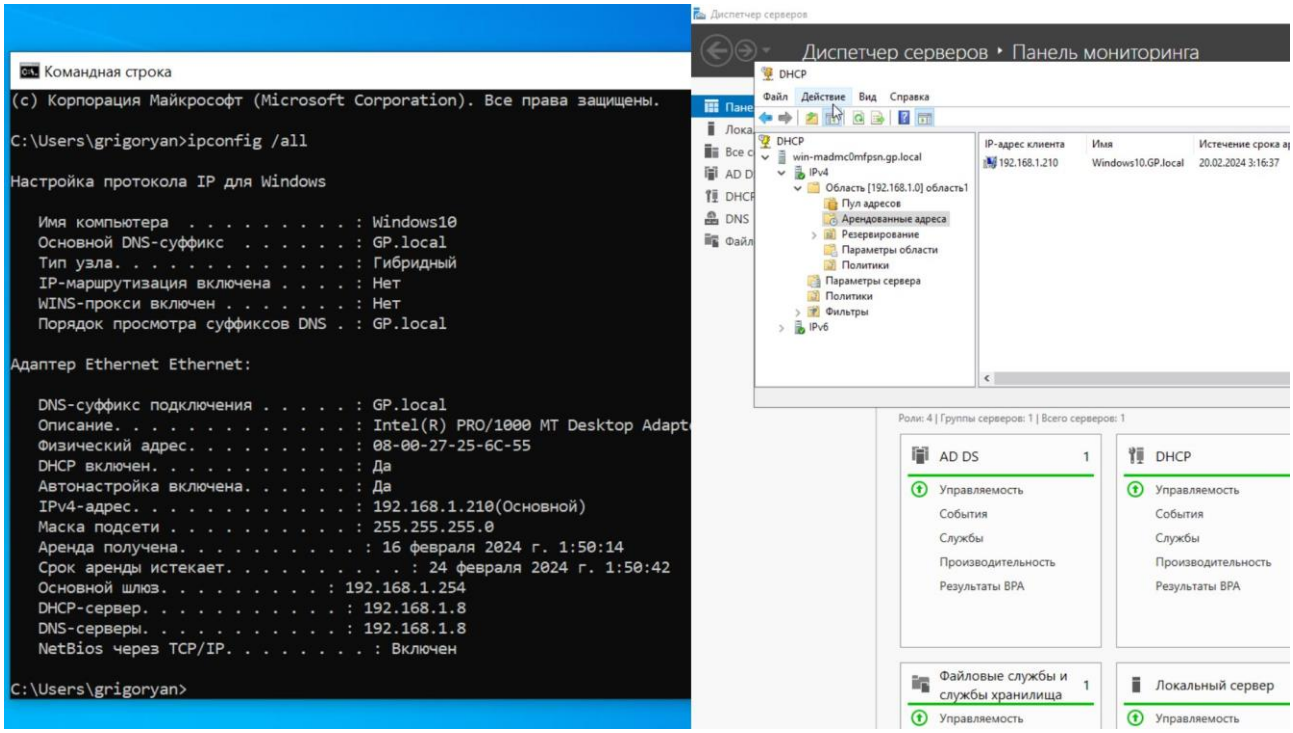



Рисунок 3 – Результат работы DHCP-сервера

***Заключение.*** Применение методики конфигурации позволит повысить уровень безопасности локальной сети и защитить информационные ресурсы организации от угроз и атак. В дальнейшем планируется внедрение различных политик безопасности сети, а также добавление иных операционных систем в домен, что позволит

улучшить управление пользователями и ресурсами сети.

### *Список литературы*

*6. Active Directory и LDAP [Электронный ресурс]. – ISPsystem – 2023. – Режим доступа: https://www.ispsystem.ru/news/active-directory-ldap/. – Дата доступа: 16.02.2024.*

UDC 004.056:004.7

## DOMAIN CONTROLLER CONFIGURATION METHODOLOGY FOR SECURING THE LOCAL NETWORK

*Grigoryan O.P., Piskunova E.S.*

*gr.161401*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Belousova E.S. – PhD (Tech.), associate professor at the information security department*

**Annotation** The article discusses the configuration of a domain controller based on Active Directory, which allows centralized management of users, groups and computers in the network. The implementation of this service allows administrators to effectively manage security in the network by defining user access rights to various resources

**Keywords:** security assurance, Active Directory, domain controllers

УДК 004.056.53

## СИСТЕМА ОБНАРУЖЕНИЯ ПЕРВОНАЧАЛЬНОГО ДОСТУПА НАРУШИТЕЛЯ В ИНФОРМАЦИОННУЮ СИСТЕМУ

*Дедков В.Н.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации*

**Аннотация.** В материалах доклада рассматриваются основные принципы работы, архитектуры и технологии, задачи и цели систем обнаружения вторжений (IPS) и предотвращения вторжений (IDS).

**Ключевые слова**: системы обнаружения вторжений (IPS) и предотвращения вторжений (IDS).

***Введение.*** Система обнаружения первоначального доступа нарушителя в информационную систему является важным компонентом защиты цифровой инфраструктуры организации, в ходе чего анализируется принцип работы и функциональные возможности такой системы, которая предназначена для обнаружения попыток несанкционированного доступа к информационной системе на ранних стадиях. В данном докладе обсуждаются методы и алгоритмы, используемые в таких системах, включая учет поведенческих аномалий, анализ сетевого трафика и обнаружение атак на основе сигнатур. Также приводятся примеры практического применения таких систем и их роль в обеспечении безопасности информационной инфраструктуры организации. Подчеркивается важность постоянного мониторинга и

обновления таких систем, чтобы быть эффективными в обнаружении новых и продвинутых методов атаки.

Система обнаружения первоначального доступа нарушителя в информационную систему (анализатор, IDS) – это инструмент, предназначенный для выявления и реагирования на попытки несанкционированного доступа к компьютерным сетям и информации.

Задачей такой системы является обнаружение и анализ сетевого трафика и его сравнение с предопределенными правилами и шаблонами. При обнаружении подозрительной активности система сигнализирует об инциденте и принимает меры по его блокированию или реагированию на него.

Основная цель системы обнаружения первоначального доступа – предотвращение вторжений, а также своевременное выявление и устранение уязвимостей в информационной системе. Она способна обнаруживать различные виды атак, включая внедрение вредоносного кода, сканирование портов, подбор паролей и другие методы несанкционированного доступа к системе.

Плюсы использования системы обнаружения первоначального доступа включают:

- Возможность обнаружения и блокирования атак на ранних стадиях, помогая предотвратить ущерб и негативные последствия для организации.
- Повышение уровня безопасности и защиты системы путем обнаружения новых и неизвестных атак, которые могут обойти традиционные средства защиты.
- Улучшение возможностей реагирования на инциденты безопасности и проведение детального анализа произошедших событий.
- Сокращение времени, затрачиваемого на обнаружение и реагирование на нарушения безопасности.

Однако, следует учесть, что система обнаружения первоначального доступа не является панацеей для всех угроз и уязвимостей. Ее эффективность может быть ограничена, особенно в случае новых и неизвестных угроз. Поэтому, для полноценной защиты информационной системы, рекомендуется комбинировать ее использование с другими методами и средствами безопасности.

***Основная часть.*** Рассмотрим системы IPS и IDS.

IDS расшифровывается как Intrusion Detection System — система обнаружения вторжений. IPS, или Intrusion Prevention System, — система предотвращения вторжений. По сравнению с традиционными средствами защиты — антивирусами, спам-фильтрами, файерволами — IDS/IPS обеспечивают гораздо более высокий уровень защиты сети.

Антивирус анализирует файлы, спам-фильтр анализирует письма, файервол — соединения по IP. IDS/IPS анализируют данные и сетевое поведение. Продолжая аналогию с хранителями правопорядка, файервол, почтовые фильтры и антивирус — это рядовые сотрудники, работающие «в поле», а системы обнаружения и предотвращения вторжений — это старшие по рангу офицеры, которые работают в отделении. Рассмотрим эти системы подробнее.

### Архитектура и технология IDS.

Принцип работы IDS заключается в определении угроз на основании анализа трафика, но дальнейшие действия остаются за администратором. Системы IDS делят на типы по месту установки и принципу действия.

### Виды IDS по месту установки.

Два самых распространенных вида IDS по месту установки:

- Network Intrusion Detection System (NIDS);
- Host-based Intrusion Detection System (HIDS).

Первая работает на уровне сети, а вторая — только на уровне отдельно взятого хоста.

### Сетевые системы обнаружения вторжения (NIDS).

Технология NIDS дает возможность установить систему в стратегически важных местах сети и анализировать входящий/исходящий трафик всех устройств сети. NIDS анализируют трафик на глубоком уровне, «заглядывая» в каждый пакет с канального уровня до уровня приложений.

NIDS отличается от межсетевого экрана, или файервола. Файервол фиксирует только атаки, поступающие снаружи сети, в то время как NIDS способна обнаружить и внутреннюю угрозу.

Сетевые системы обнаружения вторжений контролируют всю сеть, что позволяет не тратиться на дополнительные решения. Но есть недостаток: NIDS отслеживают весь сетевой трафик, потребляя большое количество ресурсов. Чем больше объем трафика, тем выше потребность в ресурсах CPU и RAM. Это приводит к заметным задержкам обмена данными и снижению скорости работы сети. Большой объем информации также может «ошеломить» NIDS, вынудив систему пропускать некоторые пакеты, что делает сеть уязвимой.

### Хостовая система обнаружения вторжений (HIDS).

Альтернатива сетевым системам — хостовые. Такие системы устанавливаются на один хост внутри сети и защищают только его. HIDS также анализируют все входящие и исходящие пакеты, но только для одного устройства. Система HIDS работает по принципу создания снапшотов файлов: делает снимок текущей версии и сравнивает его с предыдущей, тем самым выявляя возможные угрозы. HIDS лучше устанавливать на критически важные машины в сети, которые редко меняют конфигурацию.

### Другие разновидности IDS по месту установки.

Кроме NIDS и HIDS, доступны также PIDS (Perimeter Intrusion Detection Systems), которые охраняют не всю сеть, а только границы и сигнализируют об их нарушении.

Еще одна разновидность — VMIDS (Virtual Machine-based Intrusion Detection Systems). Это разновидность систем обнаружения угрозы на основе технологий виртуализации. Такая IDS позволяет обойтись без развертывания системы обнаружения на отдельном устройстве. Достаточно развернуть защиту на виртуальной машине, которая будет отслеживать любую подозрительную активность.

### Виды IDS по принципу действия.

Все системы обнаружения атак IDS работают по одному принципу — поиск угрозы путем анализа трафика. Отличия кроются в самом процессе анализа. Существует три основных вида: сигнатурные, основанные на аномалиях и основанные на правилах.

### Сигнатурные IDS.

IDS этой разновидности работают по схожему с антивирусным программным обеспечением принципу. Они анализируют сигнатуры и сопоставляют их с базой, которая должна постоянно обновляться для обеспечения корректной работы. Соответственно, в этом заключается главный недостаток сигнатурных IDS: если по каким-то причинам база недоступна, сеть становится уязвимой. Также если атака новая и ее сигнатура неизвестна, есть риск того, что угроза не будет обнаружена.

Сигнатурные IDS способны отслеживать шаблоны или состояния. Шаблоны — это те сигнатуры, которые хранятся в постоянно обновляемой базе. Состояния — это любые действия внутри системы.

Начальное состояние системы — нормальная работа, отсутствие атаки. После успешной атаки система переходит в скомпрометированное состояние, то есть заражение прошло успешно. Каждое действие (например, установка соединения по протоколу, не соответствующему политике безопасности компании, активизация ПО и т.д.) способно изменить состояние. Поэтому сигнатурные IDS отслеживают не действия, а состояние системы.

Как можно понять из описания выше, NIDS чаще отслеживают шаблоны, а HIDS — в основном состояния.

### IDS, основанные на аномалиях.

Данная разновидность IDS по принципу работы в чем-то схожа с отслеживанием состояний, только имеет больший охват.

IDS, основанные на аномалиях, используют машинное обучение. Для правильной работы таких систем обнаружения угроз необходим пробный период обучения. Администраторам рекомендуется в течение первых нескольких месяцев полностью отключить сигналы тревоги, чтобы система обучалась. После тестового периода она готова к работе.

Система анализирует работу сети в текущий момент, сравнивает с аналогичным периодом и выявляет аномалии. Аномалии делятся на три категории:

- Статистические;
- аномалии протоколов;
- аномалии трафика.

Статистические аномалии выявляются, когда система IDS составляет профиль штатной активности (объем входящего/исходящего трафика, запускаемые приложения и т.д.) и сравнивает его с текущим профилем. Например, для компании характерен рост трафика по будним дням на 90%. Если трафик вдруг возрастет не на 90%, а на 500%, то система оповестит об угрозе.

Для выявления аномалий протоколов IDS-система анализирует коммуникационные протоколы, их связи с пользователями, приложениями и составляет профили. Например, веб-сервер должен работать на порту 80 для HTTP и 443 для HTTPS. Если для передачи информации по HTTP или HTTPS будет использоваться другой порт, IDS пришлет уведомление.

Также IDS способны выявлять аномалии, любую небезопасную или даже угрожающую активность в сетевом трафике. Рассмотрим, к примеру, случай DoS-атаки. Если попытаться провести такую атаку «в лоб», ее распознает и остановит даже файервол. Креативные злоумышленники могут рассылать пакеты с разных адресов (DDoS), что уже сложнее выявить. Технологии IDS анализируют сетевой трафик и заблаговременно предотвращают подобные атаки.

***Заключение.*** В ходе данного доклада была рассмотрена проблема обнаружения первоначального доступа нарушителя в информационную систему. Были изучены различные методы и подходы к обнаружению таких угроз, а также рассмотрены основные принципы функционирования систем обнаружения.

Эффективное обнаружение первоначального доступа нарушителя требует комплексного подхода, включающего в себя как технические средства, так и процессы мониторинга и анализа данных. Кроме того, важным фактором является обновление и совершенствование систем обнаружения в соответствии с появляющимися угрозами.

Обнаружение первоначального доступа нарушителя в информационную систему является критически важным этапом в обеспечении безопасности данных и защите от кибератак. Развитие и совершенствование средств обнаружения является необходимым шагом для эффективной защиты информационных ресурсов.

Несмотря на сложность задачи обнаружения первоначального доступа нарушителя, современные технологии и методики позволяют создавать более надежные и эффективные системы обнаружения. Дальнейшие исследования и разработки в этой области могут значительно улучшить уровень безопасности информационных систем.

## *Список литературы*

*1. IDS / IPS (Intrusion Detection and Prevention System) [Электронный ресурс]. –Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/ids-ips/ - Дата доступа: 14.02.2024.*

*2. Cybersecurity and Technology Controls [Электронный ресурс]. –Режим доступа: https://www.mitre.org/publications/technical-papers/cybersecurity-and-technology-controls Дата доступа: 16.02.2024.*

***3. IPS / IDS системы. Обнаружение и предотвращение вторжений [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/obnaruzhenie-i-predotvrashchenie-vtorzheniy/ Дата доступа: 16.02.2024.***

UDC 004.056.53

## SYSTEM ZUR ERKENNUNG DES ERSTZUGRIFFS VON EINDRINGLINGEN IN EIN INFORMATIONSSYSTEM

*Dedkov V.N.*

*gr.367241*

*Belarussische Staatliche Universität für Informatik und Radioelektronik, Minsk, Republik Belarus*

*Wissenschaftlicher Leiter: Borbotko T.V. - Doktor der Technischen Wissenschaften, Leiter des Lehrstuhls für Informationssicherheit*

**Zusammenfassung.** Der Bericht behandelt die grundlegenden Arbeitsprinzipien, Architekturen und Technologien, Aufgaben und Ziele von Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).

**Schlüsselwörter:** Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).

УДК 069.271.2 – 021.131:044.056.5

## МАКЕТ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ PNETLAB ДЛЯ ИЗУЧЕНИЯ КИБЕРАТАКИ ARP-SPOOFING

*Иванов А.П., Кисель А.В.*

*гр.161402*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белоусова Е.С. – доцент кафедры ЗИ, кандидат технических наук, доцент.*

**Аннотация.** В материалах доклада представлены результаты анализа уязвимости ARP-протокола и реализация кибератаки ARP-spoofing в смоделированной локальной сети в виртуальной лаборатории PnetLAB. Предлагается разработанный макет виртуальной лаборатории использовать для развития знаний и навыков у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

**Ключевые слова:** сетевые кибератаки, ARP-spoofing, PnetLab

***Введение.*** ARP (Address Resolution Protocol) был разработан Лораном Джонсоном в начале 1980-х годов с целью решения проблемы сопоставления IP-адресов узлов с их физическими MAC-адресами в компьютерных сетях. Протокол был впервые определен в RFC 826 в 1982 году. Он стал ключевым элементом современных компьютерных сетей, обеспечивая эффективную коммуникацию и обмен данными между устройствами в локальных сетях.

Актуальность проблемы сетевых атак, таких как ARP-spoofing, становится все более критичной в условиях большого использования локальных сетей в различных сферах жизни. ARP-spoofing это кибератака, основанная на влиянии на передачу ARP-кадров. В ходе кибератаки нарушитель сканирует сеть и подменяет MAC-адреса. Это позволяет ему подделывать и перенаправлять сетевой трафик, что приводит к серьезным последствиям, таким как перехват информации, ее подмена или нарушение нормального функционирования сети.

Цель данной научной работы заключается в разработке эффективных методов защиты от кибератак на основе изучения сценариев ARP-spoofing. Результаты этого

исследования могут стать основой для разработки политик безопасности и обеспечить устойчивость к подобным угрозам в локальных сетях.

***Основная часть.*** Для изучения принципов передачи ARP-кадров и уязвимостей ARP-протокола была создана локальная сеть в виртуальной лаборатории PnetLab, которая предоставляет возможности проектирования локальных сетей на базе устройств различных производителей в режиме реального времени.

Построенная виртуальная лаборатория в PnetLab приведена на рисунке 1. В нее входит следующее оборудование:

– шлюз подключения к внешней сети (Network);
– маршрутизатор Cisco c7200 (Router);
– коммутатор Cisco IOS L2 (Switch);
– компьютер нарушителя с ОС Linux (Ubuntu);
– компьютер жертвы с ОС Linux (Ubuntu_victim);
– компьютер с ограниченной ОС (VPC).

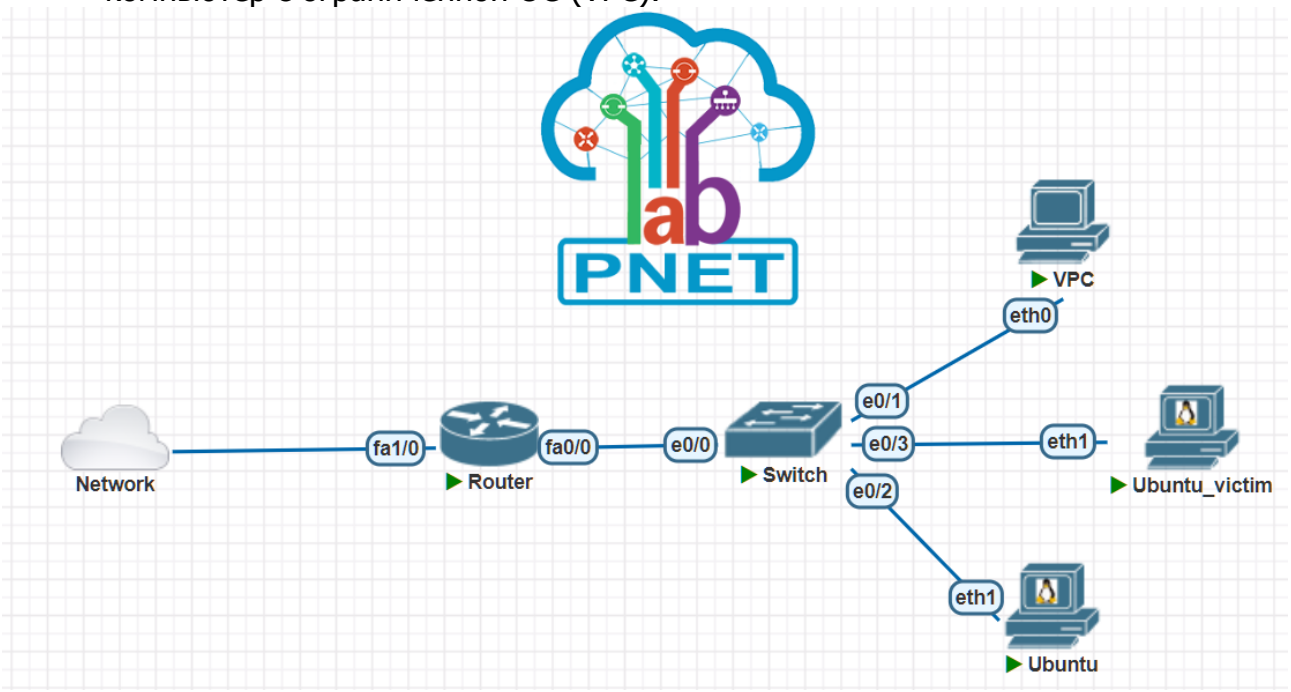



Рисунок 1 – Топология локальной сети в виртуальной лаборатории PnetLab

На основе изучения принципа передачи ARP-кадров были выявлены несколько уязвимостей. В связи с тем, что ARP-запрос содержит широковещательный MAC-адрес, то такой ARP-кадр может получить любое устройство в широковещательном сегменте. Поэтому возникает один из вариантов кибератаки – постоянная отправка ARP-кадров с модифицированным MAC-адресом. Устройство Ubuntu_victim получает ARP-ответ от устройства нарушителя. Далее происходит перенаправление трафика на устройство нарушителя. Второй вариант атаки – реализация кибератаки «человек-посередине» с помощью подмены MAC-адреса порта маршрутизатора на MAC-адрес устройства-нарушителя в таблице ARP Ubuntu_victim. Было принято решение изучения второго варианта реализации кибератаки ARP-spoofing.

В топологии топология локальной сети в виртуальной лаборатории PnetLab (рисунок 1) устройство Ubuntu_victim (MAC-адрес 50:00:00:24:00:01) получило по DHCP IP-адрес 192.168.50.4/24, а устройство Ubuntu (MAC-адрес 50:00:00:37:00:01) – 192.168.50.2/24.

Далее на устройстве Ubuntu был установлен инструмент arp-scan для обнаружения IP- и MAC-адреса всех устройств в локальной сети с помощью команды:

*admin@Ubuntu:~$ sudo apt install arp-scan –interface=eth1 --localnet*

В результате нарушитель получает информацию о MAC- и IP-адресах всех устройств. Располагая полученной информацией, нарушитель реализует кибератаку ARP-spoofing с помощью команды:

*root@Ubuntu:/home/admin#* arpspoof -i eth0 -t 192.168.50.4 192.168.50.1

На рисунке 2 представлена ARP-таблица на устройстве Ubuntu_victim до и после реализации команды arpspoof.

```
admin@Ubuntu_victim:~$ arp -a
? (192.168.50.2) at 50:00:00:37:00:01
? (10.177.0.1) at 02:42:1a:82:c8:78 [e
? (192.168.50.1) at ca:21:14:b6:00:00
```

а

```
admin@Ubuntu_victim:~$ arp -a
? (192.168.50.2) at 50:00:00:37:00:01
? (10.177.0.1) at 02:42:1a:82:c8:78 [e
? (192.168.50.1) at 50:00:00:37:00:01
```

б

Рисунок 2 – Содержимое ARP-таблицы на устройстве Ubuntu_victim до (а) и после (б) реализации кибератаки ARP-spoofing

Таким образом, можно сделать вывод, что была проведена успешная замена MAC-адреса маршрутизатора на физический адрес устройства нарушителя. Для проверки перенаправления трафика использовалась программа Wireshark (рисунок 3).

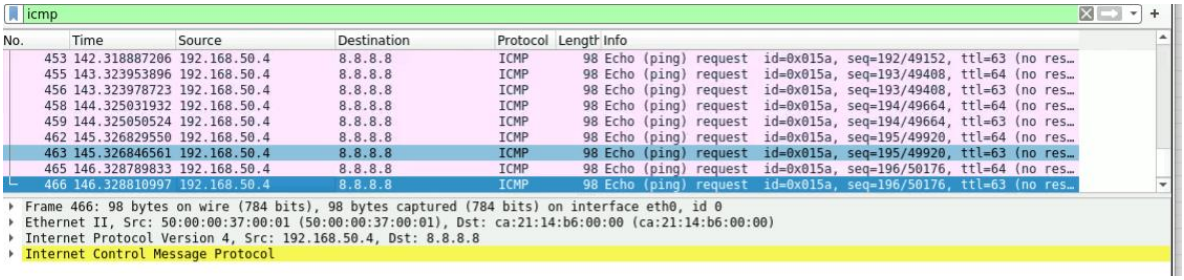



Рисунок 3 – Анализ трафика Wireshark

На рисунке 3 видно, что трафик, идущий от устройства Ubuntu_victim (IP-адрес 192.168.50.4/24) перенаправлен на устройство с MAC-адресом 50:00:00:37:00:01, что соответствует устройству нарушителя Ubuntu.

На основе полученных результатов, можно сделать вывод о том, что несмотря на актуальность и значимость протокола ARP в современных локальных сетях он легко может быть использован для реализации кибератак и перенаправления трафика. Поэтому следует использовать необходимые средства защиты на сетевом оборудовании.

Возможны несколько вариантов защиты от атаки ARP-spoofing:

1. Статические ARP-таблицы.
2. Защита коммутатора. Большинство управляемых коммутаторов оснащены функциями предотвращения кибератак ARP Poisoning, динамической проверки ARP (Dynamic ARP Inspection, DAI).

***Заключение.*** На основе проведенных исследований предлагается реализовать макет виртуальной лаборатории на основе платформы PnetLab для изучения уязвимостей ARP-протокола, реализации кибератаки ARP-spoofing, конфигурации функций предотвращения кибератак. Такой макет позволит развивать знания и навыки у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

## *Список литературы*

*7. Бабин С. А. Инструментарий хакера. / Бабин С. А. – Санкт-Петербург, 2014. – 240 с.*

*8. Отравление ARP: что это такое и как предотвратить ARP-спуфинг [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/varonis/articles/562144/. – Дата доступа: 02.02.2024.*

UDC 069.271.2 – 021.131:044.056.5

## THE LAYOUT OF THE NETLAB VIRTUAL LABORATORY TO STUDY THE ARP-SPOOFING CYBERATTACK

*Ivanov A.P., Kisel A.V.*

*gr.161402*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Belousova E.S. – PhD (Tech.), associate professor at the information security department*

**Annotation**. The report presents the results of an analysis of the vulnerability of the ARP protocol and the implementation of the ARP-spoofing cyberattack in a simulated LAN in the virtual laboratory PnetLAB. It is proposed to use the developed layout of the virtual laboratory to develop knowledge and skills among students of various specialties, including 1-98 01 02 "Information security in telecommunications".

**Keywords:** network attacks, ARP-spoofing, PnetLab.

УДК 004.777

## АНАЛИЗ И ХАРАКТЕРИЗАЦИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

*Кедик П.Р.*

*гр. 367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Врублевский И.А. – кандидат технических наук, доцент кафедры ЗИ*

**Аннотация.** Доклад рассматривает различные методы и средства, которые могут быть использованы для несанкционированного доступа к каналам передачи конфиденциальной информации. Приводится обзор основных причин и последствий утечек информации, акцентируется внимание на значимости предотвращения и обнаружения таких утечек для защиты конфиденциальности данных. Описываются различные технические каналы утечки информации.

**Ключевые слова:** утечка информации, технические каналы, средства вычислительной техники

***Введение.*** В современном мире все больше информации обрабатывается с помощью персональных электронно-вычислительных машин (ПЭВМ) и осуществляется электронный документооборот. Как следствие, это вызывает необходимость уделять особое внимание защите информации, обрабатываемой на ПЭВМ. Это связано с тем, что физические процессы, проходящие в технических устройствах при обработке информации, создают в окружающем пространстве побочные электромагнитные, акустические и другие излучения. Подобные излучения могут обнаруживаться на довольно значительных расстояниях и, следовательно, использоваться злоумышленниками, пытающимися получить доступ к конфиденциальной информации.

Источник информативного сигнала, техническое средство, осуществляющее перехват информации и физическая среда, в которой распространяется информативный сигнал, называется техническим каналом утечки информации. Поэтому, утечка информации по техническим каналам – это неконтролируемое

распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

Цель данного доклада представить системный обзор современных технических каналов утечки информации. Проведенный анализ технических каналов утечки информации поможет сформировать понимание угрозы и принять соответствующие меры для защиты информации.

***Основная часть.*** Технические каналы утечки информации принято делить на следующие типы (рисунок 1):

– оптические каналы – электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра. Основой визуально-оптического канала является оптическое излучение или свет. Визуально-оптическое наблюдение является наиболее известным, достаточно простым, широко распространенным методом разведки. В настоящее время для перехвата информации по визуально-оптическим каналам используются фото- и видеокамеры;

– акустические каналы – распространение звуковых колебаний в любом звукопроводящем материале. Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы;

– электрические каналы – напряжения и токи в различных токопроводящих коммуникациях. Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных и сторонних электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Подобные непредусмотренные связи называют паразитными связями и наводками, которые приводят к образованию электрических каналов утечки информации;

– радиоканалы – электромагнитные излучения радиодиапазона. Относятся к наиболее опасным и широко распространенным каналам утечки информации. Анализ физической природы многочисленных преобразователей и излучателей позволяет утверждать, что источниками опасного сигнала являются элементы, узлы и проводники технических средств, а также радио- и электронная аппаратура. Каждый источник опасного сигнала при определенных условиях может образовывать канал утечки информации, а, следовательно, каждая электронная система, содержащая в себе совокупность элементов, узлов и проводников, обладает некоторым множеством каналов утечки.

По природе образования технические каналы утечки информации можно разделить на естественные и специально создаваемые (рисунок 2). Естественные каналы утечки информации образуются за счет ПЭМИ, возникающих при обработке информации в средствах вычислительной техники (СВТ) (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания СВТ, соединительных линиях вспомогательных технических средств и систем и посторонних проводниках (электрические каналы утечки информации). К специально создаваемым каналам утечки информации относятся каналы, создаваемые путем внедрения в СВТ электронных устройств перехвата информации (закладных устройств) и путем высокочастотного навязывания СВТ[1].


Рисунок 1 – Классификация технических каналов утечки информации


Рисунок 2 – Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники

***Заключение.***

Таким образом, анализ современных технических каналов утечки информации

позволяет понять, какие методы и технологии могут быть использованы для доступа к каналам передачи конфиденциальных данных. Результаты проведенного анализа позволяет разработчикам и организациям принять соответствующие меры по предотвращению утечки информации и защите конфиденциальности. В тоже время, следует отметить, что технические методы не могут полностью гарантировать защиту от утечки информации. Поэтому без должного обучения и осведомленности сотрудников, существует риск, что конфиденциальные данные могут быть утрачены или скомпрометированы. Вот почему важным шагом в обеспечении безопасности информации является усиление обучения и осведомленности сотрудников относительно потенциальных угроз и правил обращения с конфиденциальными данными. Следовательно, понимание и использование современных методов и технологий для предотвращения утечки информации является важным компонентом в обеспечении конфиденциальности и безопасности данных в наших цифровых средах

### *Список литературы*

*1. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие. / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.*

*9. Зайцев А.П., Шелупанов Р.В., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации. / Зайцев А.П., Шелупанов Р.В., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. – Москва, 2009. – 508 с.*

UDC 004.777

## ANALYSIS AND CHARACTERIZATION OF INFORMATION LEAKAGE TECHNICAL CHANNELS

*Kedzik P.R.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vrublevsky I.A. – candidate of technical sciences, associate professor at the department of information security*

**Annotation**. The report examines various methods and means that can be used for unauthorized access to channels transmitting confidential information. An overview of the main causes and consequences of information leaks is provided, with an emphasis on the importance of prevention and detection of such leaks to protect data confidentiality. Various technical channels for information leakage are described.

**Keywords:** information leakage, technical channels, computing facilities.

УДК 004.777

## СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ К ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА БАЗЕ УПРАВЛЯЕМЫХ КОММУТАТОРОВ HUAWEI И CISCO.

*Кривко Д.Н.*

*гр. 367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Пулко Т.А. – канд. техн.наук, доцент*

**Аннотация.** В материалах доклада рассматриваются шаги разработки алгоритма,

направленного на управление коммутационным оборудованием производителей Cisco и Huawei. Итогом данной работы должна стать централизованная система, позволяющая оптимизировать рабочий процесс администратора сети в области предоставления доступа к локальной сети, а также направленная на повышение общего уровня информационной безопасности в применяемом сегменте.

**Ключевые слова:** локальная вычислительная сеть, алгоритм управления доступом, коммутатор, маршрутизация, Access Control List, язык Python.

***Введение.*** Расширение локальных вычислительных сетей, а также их регулярное усложнение за счет реализации новейших методов обеспечения информационной безопасности зачастую приводит к тому, что в рамках одной локальной вычислительно сети используются передовые коммутаторы различных вендоров. Данный факт в значительной степени усложняет работу специалистов ответственных за администрирование сети, поскольку различные производители в своих решениях не всегда используют единые подходы к их реализации. Чем сложнее и разнообразнее становится диапазон применяемых команд управления сетевым оборудованием, тем выше шанс ошибки со стороны администратора, что в свою очередь может негативно сказаться как на информационной безопасности данной сети, так и на её функционировании в целом. Создание систем позволяющих решать подобного рода проблемы является востребованной, поскольку с их помощью с администратора снимается функция непосредственного ввода команд управления, что позволяет в большей степени сконцентрировать внимание на более актуальных вопросах. Целью данной работы является написание алгоритма управления доступом к локальной вычислительной сети, позволяющего идентифицировать сетевое коммутационное оборудование производителей Cisco и Huawei, с применением необходимого набора команд, характерных каждому из производителей.

***Основная часть.*** Для разработки итогового алгоритма необходимо разобрать пул команд управления коммутаторов Cisco и Huawei, с целью определения закономерностей их применения, а также отличительных особенностей их синтаксиса. Получив данную информацию, необходимо описать логику работы алгоритма, уделив внимание вопросу идентификации оборудования, а также последовательности действий по генерированию команд управления. Только после этого можно будет приступать к кодированию данного алгоритма с использованием языка программирования и созданию централизованной системы управления доступом к локальной вычислительной сети. На данном этапе необходимо реализовать следующий набор функций:

– централизованная система учета IP-адресов используемых в ЛВС;
– поиск по системе учета, в соответствии с известными параметрами;
– разграничение доступа к системе централизованного управлений по паролю;
– введение логирования всех действий, выполняемых посредством системы централизованного управления;
– автоматическое определения вендора коммутационного оборудования в ЛВС до момента исполнения отдельных команд;
– автоматическое выполнение команд, необходимых для управления доступом к ЛВС;
– реализация автоматического определения mac-адреса для каждого ip-адреса активного оборудования, используемого в ЛВС;
– реализация функционала, позволяющего производить разрешения/ограничение прохождения трафика по ЛВС для конкретных ip-адресов посредством статической маршрутизации, а также используя ACL-листы;
– реализация функционала отвязки/привязки mac-адреса к конкретному ip-адресу;
– наладить взаимодействие с сервером антивирусного обеспечения, с целью отображения наиболее актуальной информации, относящейся к антивирусной защите для конкретного ip-адреса;
– автоматическая синхронизация вносимой информации в систему учета с системой учета вышестоящей организации.

Для решения поставленных задач необходимо определиться с пошаговым алгоритмом взаимодействия всех взаимосвязанных элементов: базы данных, коммутационного оборудования, системы антивирусной защиты.

На начальных этапах разработки необходимо описать структуру базы данных, с целью максимальной оптимизации данных которые потребуются для дальнейшей работы, избегая избыточности данных, которые не должны дублироваться, а при необходимости, из одних данных получать другие уже непосредственно в процессе работы программы, без постоянного их хранения.

Для реализации поставленных целей принято решение об использовании в работе языка программирования Python. Данное решение обусловлено тем, что данный язык программирования легкий в освоении с простым и понятным синтаксисом. Это позволяет в перспективе упростить процесс сопровождения итогового решения, в случае смены разработчика. Также Python имеет одну из самых больших библиотек, включая библиотеки для работы с сетевыми протоколами, такими как urllib3, telnetlib, pynetbox и т. д.

Библиотеки значительно облегчают разработку сетевых приложений и управление сетевыми устройствами, они могут использоваться для управления различными сетевыми устройствами, включая маршрутизаторы, коммутаторы, межсетевые экраны, серверы и т. д., а также могут быть использованы для мониторинга сетевой активности, анализа данных и создания пользовательских интерфейсов, предоставляет возможности для автоматизации управления. Он может использоваться для написания сценариев, которые выполняют повторяющиеся задачи. Это позволяет администратора сети сэкономить время и улучшить эффективность своей работы.

Была разработана схема взаимодействия сетевых сервисов, которая наглядно показывает процесс взаимодействия между отдельными сетевыми сервисами, работа которых направлена на обеспечение отдельных элементов информационной безопасности. Объединение их в одну единую систему позволит в значительней степени повысить оперативность принятия решений в области защиты информации, а также упростит процесс управления доступом к локальной вычислительно сети (рисунок 1).

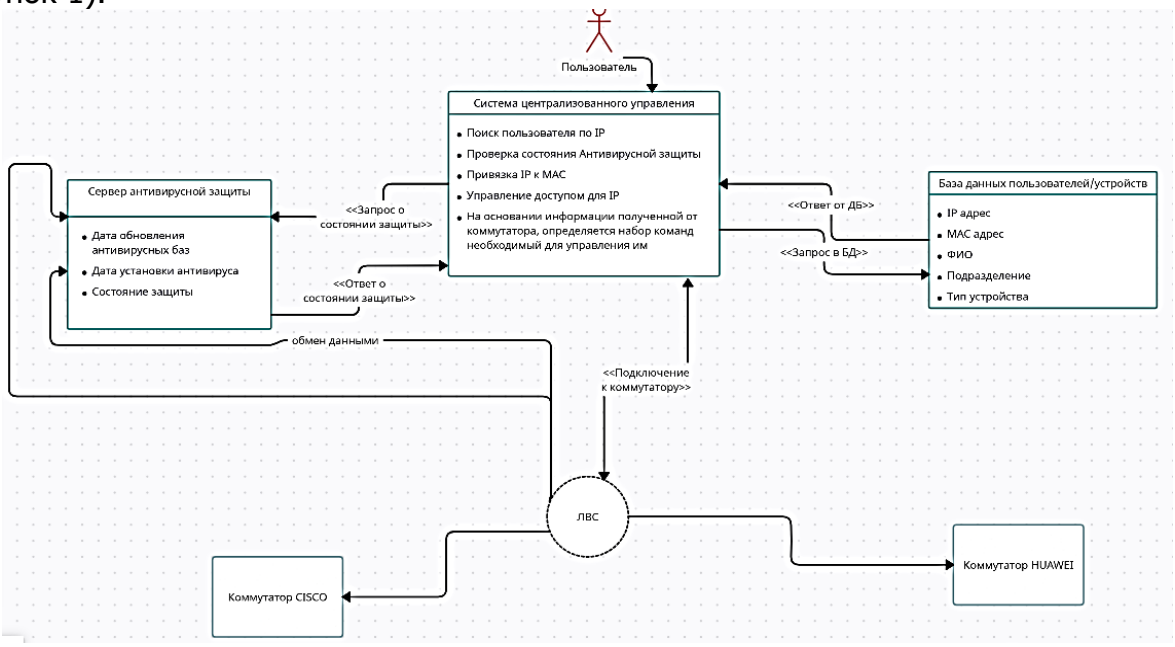



Рисунок 1 – Общая схема взаимодействия сетевых сервисов

***Заключение.*** Использование разработанной системы централизованного управления доступом к локальной вычислительной сети позволит повысить эффективность работы специалистов ответственных за организацию информационной безопасности, в рамках предоставления доступа к ресурсам локальной вычислительной сети веленого сегмента, а также более оперативно реагировать на возникающие угрозы.

Данная система разрабатывается на языке программирования Python, что в перспективе позволит более оперативно внедрять необходимые изменения в систему, а также позволит расширять её конечный функционал.

## *Список литературы*

*1. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство – 2008. – 994 с.*

*2. Бэрри Пол Изучаем программирование на Python. – Эксмо, 2020. – 624 с.*
*3. Жан Вальран Парех Шьям Коммуникационные сети. Краткое введение - ДМК Пресс, 2023.- 268с.*

UDC 004.777

## WEB APPLICATION FOR THE FOR MEMORIZING SPECIAL INFORMATION USING THE LEITNER METHOD

*Krivko D.N.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Pulko T.A. – Ph.D. technical sciences, associate professor*

**Annotation**. The report discusses the steps of developing an algorithm aimed at managing switching equipment from Cisco and Huawei manufacturers. The result of this work should be a centralized system that allows optimizing the network administrator's workflow in the area of providing access to the local network, and also aimed at increasing the overall level of information security in the applied segment.

**Keywords:** local area network, access control algorithm, switch, routing, Access Control List, Python language

УДК 004.774

## УЯЗВИМОСТЬ HTTP/2 RAPID RESET

*Лифанов К.В., Рощупкин Н.А.*

*гр. 161401*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белоусова Е.С.– кандидат технических наук, доцент кафедры ЗИ*

**Аннотация.** В материалах доклада представлены результаты исследования уязвимости протокола HTTP/2 (CVE-2023-44487), изучены и реализованы механизмы реализации DoS- и DDos-кибератак, в частности Rapid Reset Attack, на виртуальном макете, состоящем из веб-сервера и устройства нарушителя. Предложены методы ликвидации уязвимости веб-сервера, поддерживающим соединения по протоколу HTTP/2.

**Ключевые слова:** HTTP/2, CVE-2023-44487, DDoS, Nginx, Rapid Reset Attack

***Введение.*** HTTP/2 – протокол, разработанный рабочей группой Hypertext Transfer Protocol working group. В мае 2015 года спецификация HTTP/2 была опубликована как RFC 7540. HTTP/2 был создан для решения проблемы увеличения временной задержки при передаче данных по протоколу HTTP/1. По статистике на данный момент протоколом HTTP/2 пользуются более 50% всех веб-ресурсов. Основными составляющими HTTP/2 стали фреймы (Frames) и потоки (Streams). В HTTP/2 есть функция мультиплексирования: все потоки посылаются в едином TCP соединении. Также в HTTP/2 есть специальный тип фреймов RST_STREAM, позволяющий прерывать определенный поток. Перечисленные функции HTTP/2 позволяет открыть несколько одновременных потоков в одном TCP соединении. Отмена потока реализуется посредством отправки RST_STREAM. Преимуществом такого соединения является то, что от клиента и сервера не требуется согласования

отмены, она возможна в одностороннем порядке. Несмотря на преимущества новых функций протокола HTTP/2, у них есть уязвимости, одна из них CVE-2023-44487. Данная уязвимость является актуальной, так как для ее реализации не требуются значительные ресурсы.

CVE-2023-44487 – это уязвимость функции отправки фрейма RST_STREAM и функции мультиплексирования потоков протокола HTTP/2, которая может быть эксплуатирована путем открытия клиентом большого количества потоков одновременно, что приводит к ожиданию ответа от сервера на каждый поток запроса, при этом клиент немедленно отменяет каждый запрос. Таким образом, могут быть совершены DoS или DDoS кибератаки, в том числе Rapid Reset Attack, представленные на рисунке 1.

***Основная часть.*** Для исследования уязвимости протокола HTTP/2 был создан макет, который включал в себя следующие виртуальные машины:

1 Веб-сервер на основе оперативной системе GNU/Linux Ubuntu Server 22.04 (ОЗУ 2 Гбайта, 1 vCPU).

2 Устройство потенциального нарушителя, с аналогичной ОС и равное по вычислительной мощности с сервером для корректности и наглядности сравнения.

Для работы веб-сервера было выбрано одно из самых распространенных ПО Nginx, за счет открытого исходного кода, удобству установки и конфигурации. Для использования протокола HTTP/2 необходима поддержка шифрования TLS посредством SSL-сертификатов, за счет чего осуществляется использование протокола HTTPS. Поэтому на веб-сервере были созданы самоподписанные SSL-сертификаты и произведена соответствующая конфигурация Nginx. Далее в конфигурационном файле веб-сервера в разделе «server» указывается строка «listen 443 ssl http2», которая включает поддержку HTTP/2.

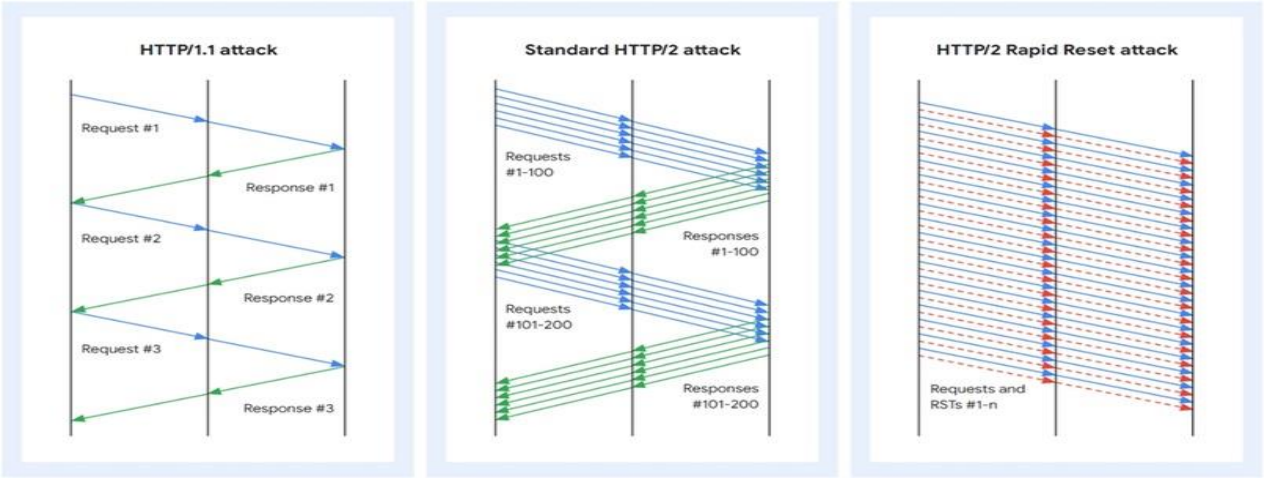



Рисунок 1 – Механизмы реализации DoS и DDoS кибератак с использованием различных версий протокола HTTP

Для реализации DoS кибератаки использовалась утилита, написанная на языке Go «rapidresetclient», позволяющая реализовать исследуемую кибератаку. Для контроля работы утилиты и просмотра отправляемых пакетов была использована программа «Wireshark», которая позволяет отследить количество, частоту и содержание HTTP-запросов.

Учитывая использование протокола HTTPS и его функции шифрования, для просмотра содержания пакетов было необходимо отредактировать исходный код «rapidresetclient» для сохранения генерируемых ключей шифрования при установлении HTTPS-соединения и дальнейшего использования их для расшифровки пакетов. Как показано на рисунке 2, утилита исправно отправляет GET-запросы и

запросы с флагом RST_STREAM поочередно, используя протокол HTTP/2, что и является реализацией Rapid Reset Attack.

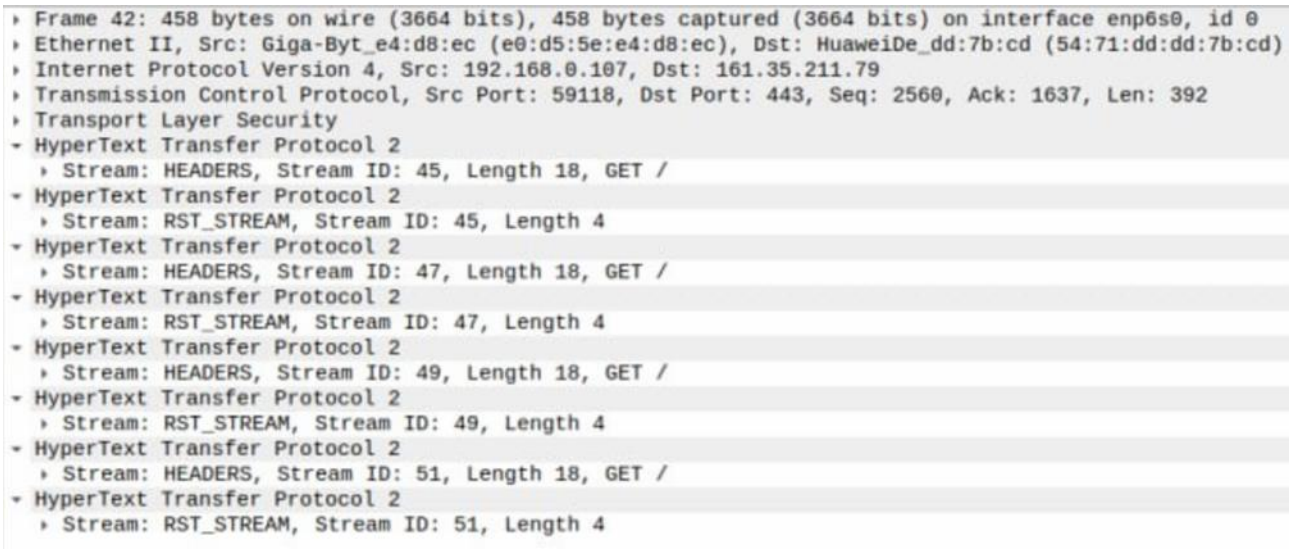



Рисунок 2 – Результат анализа пакетов с помощью Wireshark в ходе проведения Rapid Reset Attack

Для сравнения эффективности кибератак была произведена классическая DoS кибератака на протокол HTTP/1.1 с поддержкой HTTPS. Результаты сравнения двух кибератак представлены в таблице 1. В таблице 1 приводится значение «load average», которое отображает среднюю нагрузку системы, где «0» означает отсутствие нагрузки, «1» - отсутствие запаса производительности для 1-ядерного компьютера, а если значение больше, чем количество ядер процессора, значит система значительно перегружена и процессы ожидают своей очереди на исполнение.

Таблица 1 – Сравнение нагрузки при реализации Rapid Reset Attack и классической HTTP/1.1 кибератаке

| Тип кибератаки | Кол-во запросов в секунду | Степень нагрузки процессора на сервере, % | Значение «load average» на сервере | Степень нагрузки процессора на устройстве нарушителя, % | Значение «load average» на устройстве нарушителя |
|---|---|---|---|---|---|
| HTTP/2 Rapid Reset Attack | 8125 | 85–90 | 0,95–1,05 | 0,75–0,8 | 0,90 |
| HTTP/1.1 DoS | 234 | 84–86 | 0,60–0,65 | 86-90 | 44,5–48,0 |

***Заключение.*** Результаты сравнения реализации Rapid Reset Attack и классической DoS кибератаке показали, что с точки зрения требований к вычислительной способности устройства нарушителя, кибератака на HTTP/2 намного эффективнее.

На основе изучения механизмов реализации DoS кибератак на веб-сервера, поддерживающие соединение по протоколу HTTP/2, были предложены способы ликвидации уязвимости CVE-2023-44487:

1 Ограничение количества открытых соединений и количества одновременно открытых потоков в рамках одного соединения.

2 Переход на HTTP/3.

3 Своевременное обновление серверного программного обеспечения.

Необходимо отметить, что первый способ не применим к сервисам, обрабатывающим большое количество пользователей одновременно. Также существуют коммерческие решения от Cloudflare и других организаций, предоставляющих услуги в области кибербезопасности.

### *Список литературы*

1. *CVE-2023-44487 [Электронный ресурс]. – Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487. – Дата доступа : 05.02.2024.*

*2. Создание самоподписанного SSL-сертификата для Nginx [Электронный ресурс]. – Режим доступа: https://www.8host.com/blog/sozdanie-samopodpisannogo-ssl-sertifikata-dlya-nginx-v-ubuntu-18-04/. – Дата доступа : 05.02.2024.*

*3. Tool for testing mitigations and exposure to Rapid Reset DDoS [Электронный ресурс]. – Режим доступа : https://github.com/secengjeff/rapidresetclient. – Дата доступа : 05.02.2024.*

*4. Best DDoS Attack Script Python3, Attack With 56 Methods [Электронный ресурс]. – Режим доступа : https://github.com/MatrixTM/MHDDoS. – Дата доступа : 05.02.2024.*

UDC 004.774

## THE HTTP/2 RAPID RESET VULNERABILITY

*Lifanov K.V., Roschupkin N.A.*

*gr. 161401*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Belousova E.S. – PhD (Tech.), associate professor at the department of information security*

**Annotation**. The HTTP/2 vulnerability (CVE-2023-44487) research was presented in this article. Mechanisms for implementing DoS and DDos cyber attacks, in particular Rapid Reset Attack, have been studied and implemented on a virtual model consisting of a web server and an intruder device. Methods for eliminating vulnerabilities of a web server that supports connections via the HTTP/2 protocol have been proposed.

**Keywords:** HTTP/2, CVE-2023-44487, DoS, DDoS, Nginx, Rapid Reset Attack

УДК 004.056.53

# ФИШИНГ КАК ПРОБЛЕМА СОВРЕМЕННОГО ОБЩЕСТВА

*Долгая А.С., Майорова Е.А.*
*гр. 361402*
*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Пухир Г.А. — старший преподаватель кафедры защиты информации*

**Аннотация.** В материалах статьи рассматривается такой вид интернет-мошенничества как фишинг, его типы, основные методы борьбы с ними. Защита от фишинга в приоритете ставит информированность пользователей о таком виде атаки с целью исключения человеческого фактора.

**Ключевые слова:** фишинг, программное обеспечение, защита информации

***Введение.*** В современном мире стремительно происходит процесс цифровизации. Как результат, все сферы жизни подверглись изменениям. Даже преступления теперь совершаются посредством сети Интернет. Одним из самых распространённых примеров можно назвать фишинг. Фишинг (phishing) (выуживание идентификаторов) – способ получения идентификаторов пользователя информационных систем нарушителем, который основан на предоставлении пользователю такой информации и создании нарушителем таких

условий ее восприятия, при которых пользователь примет ошибочное решение и в результате чего выполнит некоторое действие, которое является выгодным нарушителю.

***Основная часть.*** Проблема фишинга крайне актуальна среди обычных пользователей, активно использующих информационные технологии в бытовой сфере. К примеру, в 2023 году почти половина (43%) всех успешных атак на организации были проведены с использованием социальной инженерии[1] (79% из них осуществлялись через электронную почту, СМС-сообщения, социальные сети и мессенджеры).

Существуют следующие виды фишинга:

- Почтовый — сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат, вложения в виде файла или гипертекстовой ссылки на файл, загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя;
- Онлайновый — сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат, вложения в виде файла или гипертекстовой ссылки на файл, загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя;
- Целенаправленный — (спиарфишинг, spear - гарпун) - сообщения, которые формирует нарушитель, передаются посредством электронной почты. Их текст адресован конкретному человеку, так как нарушитель до составления такого сообщения смог получить доступ к персональным данным этого человека;
- Вишинг — реализуется с помощью средств IP (IP –internet protocol) телефонии (мессенджеры) – это позволяет скрыть адрес нарушителя и управлять действиями человека с помощью речи.

Целенаправленный фишинг является самым опасным, так как полученные заранее данные о жертве вызывают у нее доверие. Чтобы противостоять фишингу важно знать как он работает. Цепочка событий при реализации фишинговой атаки может быть рассмотрена на примере широко известной модели атаки Cyber-Kill Chain [статья «The Industrial Control System Cyber-Kill Chain» авторства Майкла Дж. Ассанта и Роберта М. Ли]. Сценарий, по которому работает злоумышленник, включает в себя сбор информации об атакуемом объекте, внедрение в систему (например, загрузка и установка вредоносного программного обеспечения) и активация вредоносных действий.

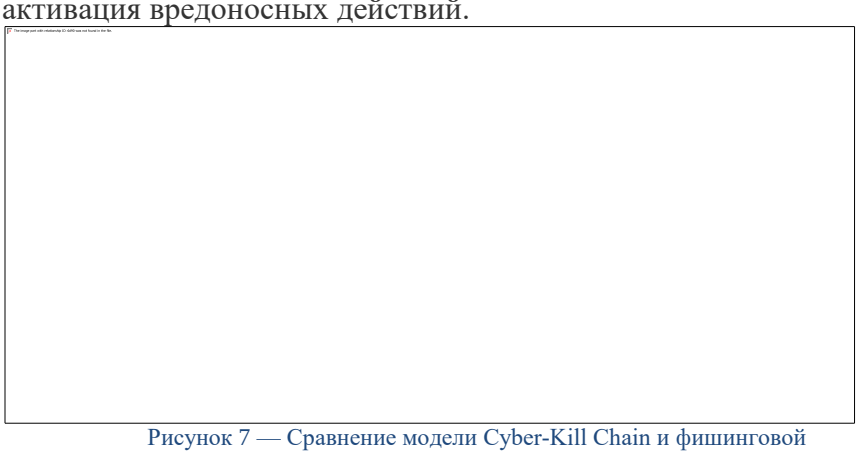


Рисунок 7 — Сравнение модели Cyber-Kill Chain и фишинговой

На рисунке 1 мы можем видеть сравнение модели атаки Cyber-Kill Chain и фишинговой атаки. Они происходят по сходному принципу. Как и Cyber-Kill Chain, фишинговая цепочка начинается с подготовки нарушителя (сбор контактов, подготовка инфраструктур), затем нарушитель воздействует на эмоциональное состояние жертвы и

[1] **Социальная инженерия** - метод управления действиями пользователя информационной системы, основанный на введении его в эмоциональное состояние таким образом, чтобы нейтрализовать его критическое мышление на то время, когда он будет совершать выгодное действие под управлением нарушителя

предпринимает некоторые действия для получения его идентификаторов (обман, клик, ввод данных). Успешная реализация этих пунктов неизбежно приводит к реализации атаки (кража данных, действие).

Для защиты от подобного рода атак существуют разные подходы, позволяющие разорвать цепочку событий, запущенных злоумышленником. При этом, чем раньше будет обнаружена угроза, тем эффективнее можно противостоять фишингу. Чтобы не стать жертвой фишинга, зачастую, достаточно сохранять критическое мышление и уметь распознавать подозрительные сообщения и ссылки. Это как раз и позволит на первых этапах остановить развитие опасных для конфиденциальной информации пользователя событий.

Другой подход использует автоматизированные системы, анализирующие содержимое файлов, почтовых писем и другого контента, который может содержать вредоносный код или ссылку на него. Также существуют программное обеспечение, предназначенное для защиты от фишинга. Среди прочих, можно выделить отдельные примеры таких программ [https://1csoft.ru/catalog/programmy-dlya-zashchity-ot-fishinga]:

- Dallas Lock — сертифицированная система защиты конфиденциальной и секретной (до уровня совершенно секретно включительно) информации от несанкционированного доступа накладного типа в персональных компьютерах с ОС семейства Windows. Обеспечивает: защиту от руткитов, защиту от фишинга, защиту USB-устройств, DLP-системы, защиту от утечки данных, межсетевой экран.
- NANO Антивирус Pro — надежный и удобный продукт от российского разработчика, предназначенный для защиты персонального компьютера под управлением операционной системы Windows от всех типов вредоносных программ – шифровальщиков, блокировщиков экрана, банковских троянских программ, потенциально нежелательных программ, рекламных программ, программ-шпионов и т.д. Специализируется именно на защите от фишинга.
- PRO32 Ultimate Security — комплексное решение премиум-класса для информационной безопасности. Обеспечивает защиту устройств Windows и Android от современных киберугроз и вредоносных программ, включает функции резервного копирования и восстановления для предотвращения потери данных.
- Антивирус Касперского для файловых серверов — эффективно защищает файловые серверы, работающие под управлением Microsoft Windows, Linux и Novell NetWare, от всех видов вредоносных программ. Антивирусная защита сетевых хранилищ общего доступа очень важна, поскольку один-единственный зараженный файл на сервере может стать источником заражения всех компьютеров вашей корпоративной сети. Современные требования к решениям для защиты файловых серверов включают стабильность работы продукта и эффективное использование системных ресурсов.

***Заключение.*** Как мы видим, в современном обществе созданы благоприятные условия для защиты от фишинга. Технологии кибератак совершенствуются, как и методы борьбы с ними. Тогда как психология человека заложена природой, поэтому главной проблемой остается лишь неосведомленность людей о методах противодействиях ему. Нарушители постоянно создают новые способы обмана, поэтому необходимо регулярно повышать уровень информированности людей.

### *Список литературы:*


1. *1Soft. Программы для защиты от фишинга [Электронный ресурс]. — Режим доступа : https://1csoft.ru/catalog/programmy-dlya-zashchity-ot-fishinga. — Дата доступа : 28.02.2024.*
2. *Международный журнал прикладных и фундаментальных исследований. Анализ проблемы фишинга в цифровом пространстве [Электронный ресурс]. — Режим доступа : https://applied-research.ru/ru/article/view?id=13594. Дата доступа: 28.02.2024*
3. *Positive technologies. Тренды фишинговых атак на организации в 2022-2023 годах [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/#id10. Дата доступа : 29.02.2024*
4. *M. J. Assante, R. M. Lee. The Industrial Control System Cyber Kill Chain / M. J. Assante, R. M. Lee. — SANS Institute, 2015. — 2 с.*

UDC 004.056.53

# PHISHING AS A PROBLEM OF MODERN SOCIETY

*Dolgaya A.S., Mayorova Y.A.*
*gr. 361402*

*Belarusian State University of Informatics and Radioelectronics,*
*Minsk, Republic of Belarus*

*Puhir H.A. — Senior Lecturer of the Department of Information Protection*

**Annotation.** In the materials of the article is considered this kind of Internet fraud as phishing, its types, the main methods of dealing with them. Protection against phishing prioritizes users' awareness of this type of attack to eliminate the human factor.

**Keywords:** phishing, software, information protection

УДК 004.056

# МЕТОДИКА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ БГУИР

*Матюшкин С.И.*

*гр. 267241*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Петров С.Н. – кандидат технических наук, доцент*

**Аннотация.** В материалах доклада рассматриваются результаты анализа уязвимостей программных продуктов, использованных при реализации интегрированной информационной системы БГУИР. Уязвимости в информационной системе могут привести к несанкционированному доступу к конфиденциальной информации, ее утечке или изменению. Анализ уязвимостей играет ключевую роль в обеспечении безопасности информационной системы.

**Ключевые слова:** ИИС БГУИР, уязвимости, CVE, модель угроз

***Введение.*** Интегрированная информационная система (ИИС) БГУИР ориентирована на автоматизацию учебных процессов и облегчение взаимодействия сотрудников и студентов. Использование ИИС позволяет упростить учет информации о студентах, учебных группах, учебных планах специальностей. В рамках ИИС функционирует подсистема «Студенты», в которой хранятся и обрабатываются персональные данные студентов. Согласно закону Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», оператор обязан обеспечивать защиту персональных данных в процессе их обработки. Оператор обязан принимать правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных. Обнаружение уязвимостей подсистемы «Студенты» ИИС БГУИР направлено на достижение этой цели.

***Основная часть.*** Интегрированная информационная система БГУИР содержит следующие разделы: Расписание; Расписание кафедры; Подразделения; Студенты; Рейтинг; Перечень дисциплин; Телефонный справочник; Техподдержка [1].

Подсистема «Студенты» ИИС БГУИР содержит следующие разделы: Личный кабинет; Список сотрудников; Контингент; Журнал текущей успеваемости; Отчеты; Словари; Планы; Учебная нагрузка; Учебный процесс [2].

Подсистема «Кабинет сотрудника» ИИС БГУИР содержит следующие разделы: Журнал успеваемости; Объявления; Личная страница; Должности; Настройки [3].

При реализации ИИС БГУИР используются следующие технологии:

Angular. Это открытая и свободная платформа для разработки веб-приложений, написанная на языке TypeScript, разрабатываемая командой из компании Google, а также сообществом разработчиков из различных компаний [4]. В ИИС применяется для формирования интерфейса пользователя.

Spring Framework. Это универсальный фреймворк с открытым исходным кодом для Java-платформы от компании VMware [5]. В ИИС используется при реализации логики работы системы.

Docker. Это программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации от компании Docker Inc. Позволяет «упаковать» приложение со всем его окружением и зависимостями в контейнер, который может быть развернут на любой Linux-системе с поддержкой контрольных групп в ядре, а также предоставляет набор команд для управления этими контейнерами [6]. В ИИС применяется для контейнеризации Angular и Spring Framework.

PostgreSQL. Это свободная объектно-реляционная система управления базами данных (СУБД) [7]. В ИИС используется для хранения данных системы.

Nginx. Это веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах от компании NGINX Inc [8]. В ИИС применяется в качестве реверс-прокси для отделения пользователей от среды выполнения.

Одной из основный угроз информационной безопасности для интегрированной информационной системы БГУИР является угроза утечки конфиденциальной информации, например, персональных данных студентов. Также вероятной угрозой может быть нарушение доступности информационных сервисов вследствие проведения атаки типа «отказ в обслуживании» (DoS, DDoS). Зачастую отказ в обслуживании является одним из начальных звеньев цепочки действий нарушителя, приводящей к несанкционированному доступу к конфиденциальной информации и как следствие ее утечке.

Угроза может быть реализована через уязвимости в программных продуктах, аппаратном обеспечении или недостаточно защищенные базы данных.

CVE (Common Vulnerabilities and Exposures) – это база данных, которая содержит информацию о различных уязвимостях в программном обеспечении и других компонентах информационных систем [9]. Использование CVE позволяет определить потенциальные угрозы для информационной системы, а также оценить их серьезность и возможные последствия.

Процесс использования CVE включает в себя определение уязвимостей в качестве первого шага. Используя CVE, можно идентифицировать уязвимости, которые могут быть использованы нарушителями для получения несанкционированного доступа к системе или утечки конфиденциальной информации [10].

Поиск уязвимостей в базе CVE по запросу «Angularjs» показал 8 уязвимостей за период времени с 2019 по 2024 годы: CVE-2023-26118; CVE-2023-26117; CVE-2023-26116; CVE-2022-25869; CVE-2022-25844; CVE-2020-7676; CVE-2019-14863; CVE-2019-10768.

Последняя на сегодняшний день уязвимость CVE-2023-26118. Версии пакета

angular, начиная с 1.4.9 по 1.8.3, уязвимы к Regular Expression Denial of Service (ReDoS) через элемент <input type="url"> из-за использования небезопасного регулярного выражения в функциональности input[url]. Эксплуатация этой уязвимости возможна с помощью больших продуманных входных данных, что может привести к «катастрофическому возврату», ситуации при которой регулярное выражение «подвешивает» интерпретатор и потребляет 100% ресурсов процессора. Такая уязвимость относится к категории «отказ в обслуживании». Согласно рейтингу CVSS, воздействие уязвимости на доступность низкая.

Поиск уязвимостей в базе CVE по запросу «Postgresql» показал 154 уязвимости за период времени с 2002 по 2024 годы, из них 17 уязвимостей с рейтингом CVSS выше 9 (критические уязвимости). Уязвимость CVE-2024-24213, опубликованная 8 февраля 2024, имеет рейтинг 9.8 и относится к категории Sql Injection. Имеет высокое влияние на конфиденциальность, доступность и целостность. Supabase PostgreSQL v15.1 (on x86_64-pc-linux-gnu) содержит уязвимость для внедрения SQL через компонент /pg_meta/default/query.

Поиск уязвимостей в базе CVE по запросу «Spring Framework» показал 16 уязвимости за период времени с 2020 по 2024 годы, из них 3 уязвимости с рейтингом CVSS 8 и выше (критические уязвимости). Уязвимость CVE-2022-22965, опубликованная 1 апреля 2022, имеет рейтинг 9.8 с вероятностью использования 97.46% и связана с удаленным выполнением кода. Последняя уязвимость CVE-2024-22233, связанная с тем, что специально созданные HTTP-запросы могут вызвать отказ в обслуживании (DoS), опубликована 22 января 2024.

Поиск уязвимостей в базе CVE по запросу «NGINX» показал 7 уязвимости за период времени с 2022 по 2024 годы. Уязвимость CVE-2023-44487, опубликованная 10 октября 2023, имеет вероятность использования 70.59% относится к категории «Отказ в обслуживании» и связана с тем, что отмена запроса может быстро сбросить многие потоки. Эта уязвимость активно использовалась с августа по октябрь 2023.

Использование различных средств и библиотек сторонних разработчиков, особенно популярных и с открытым исходным кодом приводит к тому, что в них злоумышленниками активно ищутся и эксплуатируются уязвимости, которые могут устраняться разработчиками в течение длительного периода. Кроме этого, возникает дополнительная сложность из-за того, что после обновления средства или библиотеки, особенно если это контейнеризировано, может возникнуть несовместимость с действующим проектом и информационная система перестанет полностью или частично выполнять свои функции. Причем определение необходимых изменений в коде проекта для корректной работы может занять много времени или быть вообще невозможна. Отказ же от обновлений приводит к высокой уязвимости. Создание «тестовой» копии проекта, на которой можно было бы отлаживать изменения, крайне сложно и малоэффективно из-за невозможности создания нагрузочных условий.

***Заключение.*** Проведен анализ уязвимостей программных продуктов, использованных при реализации интегрированной информационной системы БГУИР, с помощью открытой базы данных уязвимостей CVE. Рассмотрены примеры критичных или распространенных уязвимостей. Более полный анализ уязвимостей непосредственно ИИС БГУИР, возможен с применением сканеров уязвимостей, что возможно лишь с разрешения владельца информационной системы.

### *Список литературы*

*1. ИИС «БГУИР: Университет» [Электронный ресурс]. – Режим доступа: https://iis.bsuir.by – Дата доступа: 15.02.2024.*

2. «Студенты» ИИС БГУИР [Электронный ресурс]. – Режим доступа: https://students.bsuir.by – Дата доступа: 15.02.2024.
3. Кабинет сотрудника ИИС БГУИР [Электронный ресурс]. – Режим доступа: https://account.bsuir.by/personal-page – Дата доступа: 15.02.2024.
4. Angular. The web development framework for building the future [Электронный ресурс]. – Режим доступа: https://angular.io – Дата доступа: 18.02.2024.
5. Spring by VMware [Электронный ресурс]. – Режим доступа: https://spring.io – Дата доступа: 18.02.2024.
6. Docker: Accelerated Container Application Development [Электронный ресурс]. – Режим доступа: https://www.docker.com – Дата доступа: 18.02.2024.
7. PostgreSQL: The world's most advanced open source database [Электронный ресурс]. – Режим доступа: https://www.postgresql.org/ – Дата доступа: 18.02.2024.
8. nginx documentation [Электронный ресурс]. – Режим доступа: https://nginx.org/en/docs/ – Дата доступа: 18.02.2024.
9. Common Vulnerabilities and Exposures [Электронный ресурс]. – Режим доступа https://ru.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures – Дата доступа: 18.02.2024.
10. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Электронный ресурс]. – Режим доступа https://www.cvedetails.com – Дата доступа: 18.02.2024.

UDC 004.056

## METHODOLOGY FOR DETECTING VULNERABILITIES IN THE INTEGRATED INFORMATION SYSTEM OF BSUIR

*Matyushkin S.I.*

*gr. 267241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Petrov S.N., PhD, associate professor*

**Annotation**. The materials of the report discuss the results of the analysis of vulnerabilities of software products used in the implementation of the integrated information system of BSUIR. Vulnerabilities in an information system can lead to unauthorized access to confidential information, its inaccessibility or modification. Vulnerability analysis plays a key role in ensuring the security of an information system.

**Keywords:** IIS BSUIR, vulnerabilities, CVE, threat model

УДК 349.373

# О НОРМАТИВНО-ПРАВОВОМ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ ОБЩЕГО СРЕДНЕГО ОБРАЗОВАНИЯ

*Нестерович Ю.Н., магистрант гр. 267241*
*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Листопад Н. И. – доктор технических наук, профессор, заведующий кафедры ИРТ*

**Аннотация.** Рассматриваются вопросы нормативно-правового обеспечения информационной безопасности, позволяющие обосновать необходимость формирования модели информационной безопасности учреждений общего среднего образования в контексте цифровой трансформации.

**Ключевые слова:** информационная безопасность, информационно-образовательная среда, общее среднее образование, правовое обеспечение.

***Введение.*** В современных условиях всеобщей информатизации и цифровой трансформации усиливаются угрозы национальной безопасности в информационной сфере. Формирование эффективного механизма обеспечения информационной безопасности требует разработки модели информационной безопасности и учреждений общего среднего

образования с целью защиты данных, а также прогноза, предотвращения последствий любых неблагоприятных воздействий, которые могут нанести ущерб информационно-образовательной среде.

***Основная часть.*** Информационная безопасность выступает важнейшей составляющей национальной безопасности и необходимым условием реализации стратегического национального приоритета и общегосударственной задачи – формирование в Республике Беларусь информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и прогрессивного развития. Информационная безопасность определяется как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

Одним из важнейших составляющих обеспечения информационной безопасности является нормативно-правовое обеспечение. В Республике Беларусь формируются правовые основы обеспечения информационной безопасности. Так, информационные отношения в целом регламентированы Законом «Об информации, информатизации и защите информации» от 10.11.2008 № 455-З [2].

В целях обеспечения реализации государственной политики в области информационной безопасности постановлением Совета Безопасности Республики Беларусь утверждена Концепция информационной безопасности Республики Беларусь от 18.03.2019 г., № 1 (далее – Концепция) [1]. Концепция обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере [1].

Становление информационного общества охватывает все сферы деятельности человека, в том числе и сферу образования, и основано на внедрении компьютерной техники и использовании сети Интернет в учреждениях образования. В настоящее время перед системой образования стоит необходимость по совершенствованию всех образовательных процессов путем внедрения цифровых технологий, что в свою очередь обусловливает необходимость анализировать ситуацию и формировать методы и способы обеспечения информационной безопасности. Отметим, что создание системы информационной безопасности в соответствии с современными требованиями предусмотрено Государственной программой «Образование и молодежная политика» на 2021-2025 годы» (подпрограмма 11 «Обеспечение функционирования высшего образования») в качестве одного из векторов, обеспечивающих достижение высокого уровня информатизации системы образования [3].

Расширение спектра средств передачи информации и доступа к ним обучающихся, увеличение различных форм дистанционного обучения влечет появление новых рисков, угроз и актуализирует проблему обеспечения информационной безопасности в учреждениях общего среднего образования. Вопрос информационной безопасности общих средних учебных заведений является достаточно новым и недостаточно исследованным.

Безусловно, учреждения общего среднего образования не могут оставаться в стороне от глобального процесса информатизации и цифровизации, одним из направлений которого выступает формирование безопасной информационной образовательной среды учреждения образования.

Каждое учреждение общего среднего образования должно формировать систему информационно-образовательной среды, которая качественно влияет на образовательный процесс. При этом, систему безопасной информационной образовательной среды формирует как безопасная информационная образовательная среда самого учреждения общего среднего образования, так и безопасная информационная среда участников образовательного процесса и прежде всего, обучающихся.

Таким образом, в контексте обеспечения информационной безопасности в условиях цифровой трансформации, представляется актуальным дальнейшее исследование проблем обеспечения информационной безопасности учреждений общего среднего образования.

Считаем необходимым разработать модель обеспечения информационной безопасности учреждений общего среднего образования, включающую субъекты, угрозы, меры обеспечения безопасности. Формируя модель обеспечения информационной безопасности учреждений общего среднего образования необходимо учитывать, что образовательный процесс в первую очередь, касается уязвимых, наименее защищенных участников образовательного процесса – обучающихся. Поэтому система информационной безопасности учреждений общего среднего образования должна быть направлена не только на сохранность баз данных, содержащих конфиденциальные сведения, но и гарантировать невозможность доступа в учреждения образования любой информации, предполагающей негативное воздействие на сознание обучающихся в учебных заведениях общего среднего образования.

***Заключение.*** С учетом изложенного считаем, что доминирующим свойством формирующейся информационно-образовательной среды учреждений общего среднего образования в современных условиях является безопасность, которая выражается в: безопасности личной информации участников образовательного процесса; безопасности ресурсов информационной образовательной среды; безопасности учреждения общего среднего образования при взаимодействии с информационной образовательной средой.

### *Список использованных источников:*

[1] *О концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.*

[2] *Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 ноября 2008 г. № 455-З (ред. от 10.10.2022) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.*

[3] *О государственной программе «Образование и молодежная политика» на 2021-2025 годы [Электронный ресурс]: постановление Совета Министров Респ. Беларусь, 19 января 2021 г., № 57 (ред. от 12.12. 2023 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.*

UDC 349.373

## ON REGULATORY AND LEGAL ENSURANCE OF INFORMATION SECURITY OF GENERAL SECONDARY EDUCATION INSTITUTIONS

*Nesterovich Yu.N.,*

*gr. 267241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Listopad N.I. — Doctor of Sciences (Technical.), Professor, head of information radioengineering department*

**Annotation**. The issues of regulatory and legal support for information security are considered, making it possible to justify the need to formulate an information security model for general secondary education institutions in the context of digital transformation.

**Keywords:** information security, information and educational environment, general secondary education, legal support.

УДК 621.391

# АНАЛИЗ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

*Пакуш П.А.*

*гр. 367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Врублевский И.А. –кандидат технических наук, доцент кафедры ЗИ*

**Аннотация.** В материалах доклада представлен анализ методов и средств защиты речевой информации. Сделан вывод, что для защиты речевой информации от утечки по техническим каналам на объектах информационной деятельности, где циркулирует информация с ограниченным доступом, необходимо проводить комплекс технической защиты информации, которой представляет собой совокупность организационных, инженерных и технических мероприятий и средств.

**Ключевые слова:** защита речевой информации, акустический, виброакустический канал

***Введение.*** Защита сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере является основной задачей информационной безопасности. Актуальность задач защиты речевой информации от утечки по акустическим и виброакустическим каналам связана с речевой деятельностью человека и поэтому занимает важное место в области безопасности информации. В тоже время ряд факторов, влияющих на эффективность защиты речевой информации, зачастую остается за пределами внимания при организации системы информационной безопасности объектов, разработке и производстве средств защиты речевой информации, их практическом применении. С целью нахождения оптимальных решений для защиты от рисков потери информации проведен анализ методов и средств защиты речевой информации и показана их важность для систем защиты информации.

***Основная часть.*** Методы и средства защиты речевой информации от утечки по акустическому и виброакустическому каналам основаны на уменьшении отношения «сигнал/шум». При этом различают пассивные и активные методы[1].

Пассивные методы направлены на уменьшение уровня информативного сигнала за счет улучшения звуко- и виброизоляции инженерных конструкций и установки фильтрующих устройств в проводных коммуникациях.

Активные методы основаны на увеличении уровня шума по отношению к естественному (фоновому) и реализуются с помощью технических средств, основу которых составляют различные генераторы шума. Также для этих целей используется акустическая маскировка (рисунок 1). Мероприятия акустической маскировки позволяют обеспечить следующие функции: неузнаваемость голоса диктора; существенное снижение неразборчивости речи диктора; скрыть факт передачи речевой информации[2].

Активные методы защиты речевой информации чаще всего используют так называемые «белый», «розовый» и «речеподобный» шумы (рисунок 2), (графики 1, 2, 3 соответственно), различающиеся формой огибающей спектра. Целесообразность использования того или иного вида помех определяется многими факторами (в частности преследуемыми целями: маскирование, имитация, обеспечение максимальной комфортности переговоров и т.п.). Следует отметить, что для обеспечения минимума интегрального уровня помех, наиболее эффективной является речеподобная помеха.

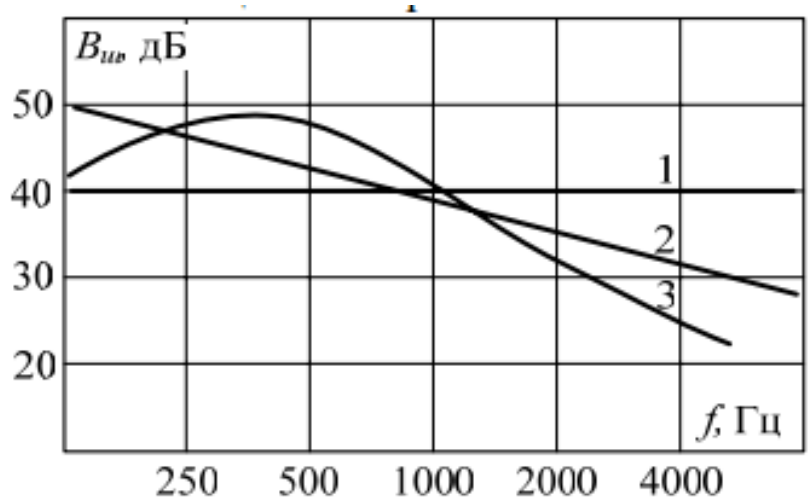
Технические средства защиты при проведении конфиденциальных переговоров, с точки зрения защиты речевой информации можно разделить на две группы: средства защиты помещений и средства защиты собственно речевой информации.

К первой группе аппаратура постановки помехи на границе защищаемого помещения («вдоль» ограждающих конструкций) относятся – генераторы акустического и виброакустического шума. Ко второй группе – аппаратура акустического зашумления, располагающаяся в непосредственной близости от места нахождения участников переговоров.

В первом случае при достаточно комфортных условиях для находящихся в помещении людей не гарантируется защита речевой информации по всему объему помещения (например, от утечки за счет скрытно установленных внутри помещения специальных технических средств (СТС) типа радиомикрофонов, диктофонов и т.п.). Поэтому, требуются дополнительные организационно-технические меры по выявлению и/или блокированию таких СТС.

Во втором случае вероятность утечки речевой информации за счет любых СТС, содержащих микрофоны, близка к нулю. Но в этом случае возникает проблема обеспечения комфортности переговоров, поскольку участники находятся под непосредственным воздействием акустического шума.


Рисунок 1 – Классификация методов акустической маскировки




1 – «белый» шум
2 – «розовый» шум
3 – «речеподобный» шум

Рисунок 2 – Виды шумов

***Заключение.***

Показано, что в своем первоначальном виде речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. Различного рода преобразователи акустических и вибрационных колебаний являются вторичными источниками. Это такие как: громкоговорители, телефоны, микрофоны, акселерометры и т.д. Технические каналы утечки речевой информации в зависимости от среды распространения сигналов и способов их перехвата, можно разделить на следующие типы: акустические, вибрационные (виброакустические), акустоэлектрические, оптоэлектронные и параметрические. Для защиты речевой информации от утечки по техническим каналам на объектах информационной деятельности, где циркулирует информация с ограниченным доступом, необходимо проводить комплекс технической защиты информации, которой представляет собой совокупность организационных, инженерных и технических мероприятий и средств.

## *Список литературы*

*1. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.*

*2. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие /В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с*

*3. Рева, И. Л. О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам / И. Л. Рева, В. А. Трушин, А. В. Иванов // Специальная техника. –2016. – № 6. – С. 29–35с.*

UDC 621.391

## ANALYSIS OF METHODS AND MEANS OF PROTECTING SPEECH INFORMATION

*Pakush P.A.*

*group 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vrublevsky I.A. – Candidate of Technical Sciences, Associate Professor of the Department of Information Security*

**Annotation**. The report contains an analysis of methods and means of protecting speech information. It is concluded that in order to protect speech information from leakage through technical channels at information activity facilities where information with limited access circulates, a complex of technical information protection is created, which is a set of organizational, engineering and technical measures and means.

**Keywords:** speech information protection, acoustic, vibroacoustic channel

УДК 004.056

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ СИСТЕМЫ ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

*Петров А.Д.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Петров С.Н. – кандидат технических наук, доцент кафедры защиты информации*

**Аннотация.** В материалах доклада рассматривается методика разработки политики информационной безопасности в учреждениях системы высшего образования Республики Беларусь с учетом требований Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. №66.

**Ключевые слова:** политика информационной безопасности, информационная безопасность

***Введение.*** Политика информационной безопасности играет ключевую роль в обеспечении защиты информационных активов организации. Она позволяет определить основные направления и приоритеты в области информационной безопасности, установить ответственность и обязанности сотрудников.

Политика информационной безопасности позволяет разработать эффективные меры по предотвращению, обнаружению и реагированию на угрозы информационной безопасности

Руководящие документы оказывают значительное влияние на содержание политики информационной безопасности. Они определяют требования и стандарты, которым должна соответствовать система информационной безопасности организации. Указ Президента Республики Беларусь №449 от 9 декабря 2019 года «О совершенствовании государственного регулирования в области защиты информации» [1] является примером такого документа и устанавливает ряд требований и принципов для обеспечения безопасности информационных систем и обработки информации. О мерах по реализации Указа Президента Республики

Беларусь от 9 декабря 2019 года №449 подробно описано в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. №66 [2].

***Основная часть.*** Согласно пункта 9 главы 2 положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено политика информационной безопасности организаций должна содержать:

– цели и принципы защиты информации в организации;

– перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, а также отдельно стоящих электронных вычислительных машин, используемых в организации и принадлежащих ей на праве собственности или ином законном основании, с указанием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации;

– обязанности пользователей информационной системы;

– порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации.

Основными целями политики информационной безопасности учреждений системы высшего образования являются:

– сохранение конфиденциальности критичных информационных ресурсов;

– обеспечение непрерывности доступа к информационным ресурсам учреждений системы высшего образования;

– защита целостности информации с целью поддержания возможности учреждений системы высшего образования по оказанию услуг высокого качества и принятию эффективных управленческих решений;

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами учреждений системы высшего образования;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

– предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

Основными задачами политики информационной безопасности учреждений системы высшего образования являются:

– разработка требований по обеспечению информационной безопасности;

– контроль выполнения установленных требований по обеспечению информационной безопасности;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;

– разработка нормативных документов для обеспечения информационной безопасности учреждений информационной безопасности;

– выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности учреждений высшего образования;

– организация антивирусной защиты информационных ресурсов учреждений системы высшего образования;

– защита информации учреждений системы высшего образования от несанкционированного доступа и утечки по техническим каналам связи;

– организация периодической проверки соблюдения информационной

безопасности с последующим представлением отчета по результатам указанной проверки ректору учреждения высшего образования.

Политика информационной безопасности образовательных учреждений направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшения рисков и снижения потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников образовательного учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора, хранения, обработки, предоставления и распространения информации и обеспечение и бесперебойного процесса деятельности.

Наибольшими возможностями для нанесения ущерба обладает собственный персонал учреждений системы высшего образования.

Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Стратегия обеспечения информационной безопасности высших образовательных учреждений заключается в использовании заранее отработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму потери от технических аварий и ошибочных действий сотрудников высших учебных учреждений.

Основными принципами обеспечения информационной безопасности:

– постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов учреждений высшего образования;

– своевременное обнаружение проблем, корректировка моделей угроз и нарушителя;

– персонификация и разделение ролей и ответственности между сотрудниками.

Объектами защиты с точки зрения информационной безопасности являются:

– информационный процесс профессиональной деятельности;

– информационные активы учреждений высшего образования.

Защищаемая информация делится на следующие виды:

– информация по финансово-экономической деятельности учреждений высшего образования;

– персональные данные – личные сведения о человеке, с помощью которых его можно идентифицировать согласно Закона Республики Беларусь от 7 мая 2021 года №99-З «О защите персональных данных»;

– другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования».

Управление информационной безопасностью учреждений системы высшего образования включает в себя:

– разработку и поддержание в актуальном состоянии Политики информационной безопасности;

– разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;

– обеспечение бесперебойного функционирования комплекса средств информационной безопасности;

– осуществление контроля (мониторинга) функционирования системы информационной безопасности;

– оценку рисков, связанных с нарушения информационной безопасности.

***Заключение.*** Политика информационной безопасности является основным документом организации по обеспечению и организации информационной безопасности. Соблюдение требований политики информационной безопасности позволяет минимизировать риски и угрозы информационной безопасности в процессе обучения абитуриентов и работы сотрудников учреждений высшего образования.

## *Список литературы*

*1. Указ Президента Республики Беларусь от 9 декабря 2019 года № 449 «О совершенствовании государственного регулирования в области защиты информации» – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by*

*2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 года № 449» – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by*

UDC 004.056

## INFORMATION SECURITY POLICY IN INSTITUTIONS OF THE HIGHER EDUCATION SYSTEM OF THE REPUBLIC OF BELARUS

*Petrov A.D.*

*gr.367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Petrov S.N. – PhD, associate professor of the Information Security Department*

**Annotation**. The materials of the report discuss the methodology for developing an information security policy in institutions of the higher education system of the Republic of Belarus, taking into account the requirements of the Order of the Operational Analytical Center under the President of the Republic of Belarus dated February 20, 2020 No. 66

**Keywords:** information security policy, information security.

УДК 004.056.53

## МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ПРИМЕРЕ ТЕХНИК МОДЕЛИ MITRE ATT&CK TA0002-TA0009

*Попович А.А.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации*

**Аннотация.** В материалах доклада рассматриваются основные принципы и концепции модели MITRE ATT&CK, ее структуру, основные категории тактик и техник, а также примеры использования модели в практических задачах, что позволит углубить знания о принципах кибербезопасности и методах защиты от кибератак на примере техник модели TA0002-TA0009.

**Ключевые слова:** модели MITRE ATT&CK, техники модели TA0002-TA0009, кибербезопасность.

***Введение.*** В современном цифровом мире информационные системы играют ключевую роль в повседневной деятельности организаций и частных лиц. От электронной почты до онлайн-банкинга, мы все используем различные информационные системы для обмена информацией, проведения операций и ведения бизнеса. Однако вместе со всеми преимуществами, которые приносят нам информационные технологии, возникают и серьезные угрозы для информационной безопасности.

Информационная безопасность информационных систем становится все более актуальной темой в современном мире. Утечки конфиденциальных данных, кибератаки, вредоносное программное обеспечение - все это потенциальные угрозы, с которыми сталкиваются организации и частные лица. Поэтому обеспечение безопасности информационных систем становится приоритетной задачей для многих компаний и организаций.

В данном докладе рассмотрим модель нарушителя MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), которая представляет собой базу знаний, которая классифицирует различные тактики, техники и процессы, используемые злоумышленниками при проведении кибератак. Данная модель разработана командой MITRE для организации информационной безопасности и служит для лучшего понимания и анализа поведения нарушителей.

Модель MITRE ATT&CK включает более 250 тактик и техник, которые могут быть использованы при целенаправленных атаках на информационные системы и сети. Эти тактики и техники разделены на матрицы ATT&CK, каждая из которых описывает определенную цель и способы ее достижения.

Модель нарушителя MITRE ATT&CK помогает организациям и специалистам в области кибербезопасности лучше понять, какие методы и инструменты могут быть использованы злоумышленниками, и принять необходимые меры по защите от таких атак. Она также помогает при анализе угроз и разработке стратегии защиты для предотвращения инцидентов информационной безопасности.

***Основная часть.*** MITRE ATT&CK - это модель тактик, техник и процедур (TTP), которая описывает широкий спектр методов, которые злоумышленники могут использовать при проведении атак на компьютерные системы. Вот некоторые из основных тактик, техник и процедур, входящих в модель MITRE ATT&CK:

1. Использование программной реализации: злоумышленники используют программное обеспечение для достижения своих целей, например, установка вредоносного ПО, эксплойты и обратные двери.

2. Ложные флаги: злоумышленники могут использовать ложные сигналы или информацию, чтобы запутать защитные системы и направить внимание на другую область.

3. Кража и использование учетных данных: злоумышленники могут получить доступ к учетным данным и использовать их для несанкционированного входа в системы и сети.

4. Блокировка обнаружения: злоумышленники могут применять различные методы для предотвращения обнаружения своих операций, такие как шифрование коммуникаций, маскировка вредоносного ПО и удаление следов.

5. Управление доступом: злоумышленники могут получить несанкционированный доступ к системам и сетям, используя уязвимости в процессах аутентификации и авторизации.

6. Подкармливание и обнаружение информации: злоумышленники могут

манипулировать, фальсифицировать или удалять информацию, чтобы затруднить обнаружение своей активности и следов.

7. Установка задержки и персистентности: злоумышленники могут устанавливать механизмы задержки и персистентности, чтобы продолжать свою активность после инициации атаки.

Это только некоторые из тактик, техник и процедур, рассматриваемых в модели MITRE ATT&CK. Понимание этих методов может помочь в защите компьютерных систем и сетей от атак и повысить уровень безопасности.

В рамках MITRE ATT&CK различаются различные техники, обозначенные уникальными идентификаторами. В рамках данного доклада рассмотрим техники модели TA0002-TA0009, способы их обнаружения и противодействия.

1. TA0002 - Сканирование сети:

- Обнаружение: Мониторинг сетевого трафика для обнаружения повышенной активности сканирования, особенно если замечены необычные или неподдерживаемые порты или протоколы.

2. TA0003 - Оскорбительная подготовка:

- Обнаружение: Следить за необычными или подозрительными операциями создания и попытками запуска исполняемых файлов на компьютерах в сети.

3. TA0004 - Доставка вредоносного ПО:

- Обнаружение: Использование антивирусных программ и инструментов для обнаружения вредоносных программ при доставке на конечные устройства или точки входа в сеть.

4. TA0005 - Установка вредоносного ПО:

- Обнаружение: Мониторинг активности установки программного обеспечения, особенно при обнаружении необычного или запрещенного программного обеспечения.

5. TA0006 - Запуск вредоносного ПО:

- Обнаружение: Обнаружение необычных процессов, активированных в системе, а также использование инструментов мониторинга активности процессов для обнаружения потенциально вредоносного ПО.

6. TA0007 - Получение данных:

- Обнаружение: Слежение за необычными запросами к файловым системам, базам данных или другим источникам данных, а также мониторингом активности сетевого трафика.

7. TA0008 - Коммуникации через сеть:

- Обнаружение: Использование инструментов для контроля и анализа сетевого трафика с целью обнаружения аномальной коммуникации или несанкционированной передачи данных.

8. TA0009 - Выход из системы:

- Обнаружение: Мониторинг активности пользователя, включая необычные попытки выхода из системы или переключения учетных записей, а также отслеживание активности удаленного доступа к системе [1].

Обнаружение этих техник часто осуществляется при помощи интеллектуальных систем обнаружения вторжений (IDS/IPS), анализа журналов событий, мониторинга сетевого трафика и использования специализированных инструментов для обнаружения вредоносных действий и поведения.

Противодействие техникам модели TA0002-TA0009 можно осуществлять путем следующих действий:

Обучение сотрудников: обеспечить сотрудников компании знаниями и навыками по распознаванию и предотвращению использования техник из указанных моделей.

Внедрение систем защиты: реализовать системы мониторинга и защиты, которые могут обнаружить попытки использования этих техник и предотвратить их дальнейшее применение.

Создание процедур и политик безопасности: разработать и внедрить строгие процедуры и политики безопасности, которые могут помочь предотвратить атаки при помощи указанных техник.

Систематическое обновление знаний: следить за новыми техниками и методами, которые могут быть использованы злоумышленниками, и обеспечивать периодическое обновление знаний сотрудников компании.

Сотрудничество с экспертами по кибербезопасности: в случае возникновения сомнений или необходимости принятия решения по атаке с использованием подобных техник, обращаться за помощью к специалистам в области кибербезопасности [2].

***Заключение.*** Модели MITRE ATT&CK TA0002-TA0009 представляют собой набор тактических приемов и техник, используемых злоумышленниками в рамках кибератак. Эти модели помогают аналитикам и специалистам по кибербезопасности лучше понимать и противодействовать различным угрозам и атакам. Используя модели TA0002-TA0009, компании и организации могут анализировать свои системы и сети на предмет возможных уязвимостей и улучшать свои меры защиты. Эти модели представляют собой ценный ресурс для обучения персонала по кибербезопасности, а также для разработки стратегий противодействия угрозам в сети.

В целом, модели MITRE ATT&CK TA0002-TA0009 могут значительно повысить уровень кибербезопасности организации и помочь защитить информацию и данные от потенциальных атак и угроз. Они являются важным инструментом в борьбе с киберпреступностью и поддержании безопасности в цифровой среде.

### *Список литературы*

*1. MITRE ATT&CK: A Guide to the Modern Threat Tactics [Электронный ресурс]. –Режим доступа: https://attack.mitre.org/. - Дата доступа : 15.02.2024.*

*2. Cybersecurity and Technology Controls [Электронный ресурс]. –Режим доступа: https://www.mitre.org/publications/technical-papers/cybersecurity-and-technology-controls Дата доступа : 15.02.2024.*

UDC 004.056.53

## METHODOLOGY FOR BUILDING A SYSTEM FOR MONITORING INFORMATION SECURITY EVENTS IN AN INFORMATION SYSTEM USING THE EXAMPLE OF MITRE ATT&CK MODEL TECHNIQUES TA0002-TA0009

*Popovich A.A.*

*gr.367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Borbotko T.V. – Dr. of Sci. (Tech.), Head of the Department of Information Security*

**Annotation**. The report contains the basic principles and conceptual models of MITER ATT&CK, its structure, categories of tactics and techniques, as well as examples of using models in practical tasks that allow you to use knowledge about the principles of cybersecurity and methods of protection against cyber attacks based on the main technical models TA0002-TA0009.

**Keywords:** MITRE ATT&CK models, TA0002-TA0009 models, cybersecurity.

УДК 534.2

# СИСТЕМА АКТИВНОЙ ЗАЩИТЫ КОНТРОЛИРУЕМОЙ ЗОНЫ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

*Прокошин М.И.*

*гр. 367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Врублевский И.А. – кандидат технических наук, доцент*

**Аннотация.** Рассматривается разработка системы защиты выделенного (защищаемого) помещения от утечки речевой информации по виброакустическому каналу. Разработка данной системы заключает в себе комплексный подход к обеспечению защиты речевой информации и сопряжена с применением современных технологий и методов, что поспособствует повышению уровня безопасности ведения секретных переговоров.

**Ключевые слова:** защищаемое помещение, речевая информация, активная защита, виброакустический канал.

***Введение.*** Современное информационное общество ввиду стремительного развития технологий и распространения мобильных устройств (в том числе средств акустической речевой разведки) сталкивается с возрастающей угрозой утечки конфиденциальной речевой информации через технические каналы, включая виброакустический.

Виброакустические каналы утечки информации могут быть использованы злоумышленниками для получения доступа к конфиденциальным разговорам, проводимым внутри помещений. Это может быть особенно опасно в организациях, где обсуждаются коммерческие тайны, государственные секреты или персональные данные. Это подчеркивает необходимость разработки эффективных методов защиты данных от несанкционированного доступа. В данном контексте представляется актуальной задача исследования и разработки систем защиты, способных предотвратить утечку информации через виброакустический канал.

***Основная часть.*** Прямой акустический, виброакустический, акустооптический акустоэлектрический, и акустоэлектромагнитный технические каналы представляют собой потенциальные угрозы для конфиденциальности речевой информации. Эффективные методы защиты могут быть реализованы как с применением активных технологий, так и пассивных подходов. Среди активных методов выделяют:

- виброакустическую маскировку (создание маскирующих акустических помех в воздуховодах, дверных тамбурах, ограждающих конструкциях, окнах, инженерных коммуникациях);
- линейное электромагнитное зашумление (создание низкочастотных маскирующих электромагнитных шумовых помех в соединительных линиях вспомогательных технических средств и систем (далее – ВТСС));
- подавление средств перехвата информации (подавление диктофонов в режиме записи, подавление радиозакладок, подавление средств сотовой связи, подавление сетевых закладок, подавление средств перехвата информации, подключаемых к телефонной линии).

Пассивные методы включают в себя:

- звукоизоляцию выделенных помещений (звукоизоляцию ограждающих

конструкций, дверей, окон, воздуховодов);

- установку специальных упругих виброизолирующих прокладок в трубопроводы, выходящие за пределы контролируемой зоны;
- экранирование защищаемых помещений; подавление сигналов сетевых закладок (установка фильтров нижних частот в линиях электропитания);
- подавление опасных сигналов в линиях ВТСС (установка в соединительных линиях ВТСС фильтров нижних частот);
- ограничение опасных сигналов в линиях ВТСС (установка в соединительных линиях ВТСС ограничителей сигналов малой амплитуды);
- отключение ВТСС от линии (установка в соединительных линиях ВТСС устройств защиты, отключающих преобразователи (источники) опасных сигналов от линии).

Анализ эффективности каждого из методов защиты позволит определить их применимость в различных условиях. Важно учитывать как технические аспекты, так и экономическую целесообразность применения конкретного метода.

Для того, чтобы система защиты была не только эффективной, но и экономически обоснованной, в первую очередь необходимо исследовать защищаемое помещение на наличие уязвимостей, в том числе мест возможной установки технических средств акустической речевой разведки.

На рисунке 1 изображены различные варианты возможного использования технических каналов утечки информации на примере типового объекта информатизации.

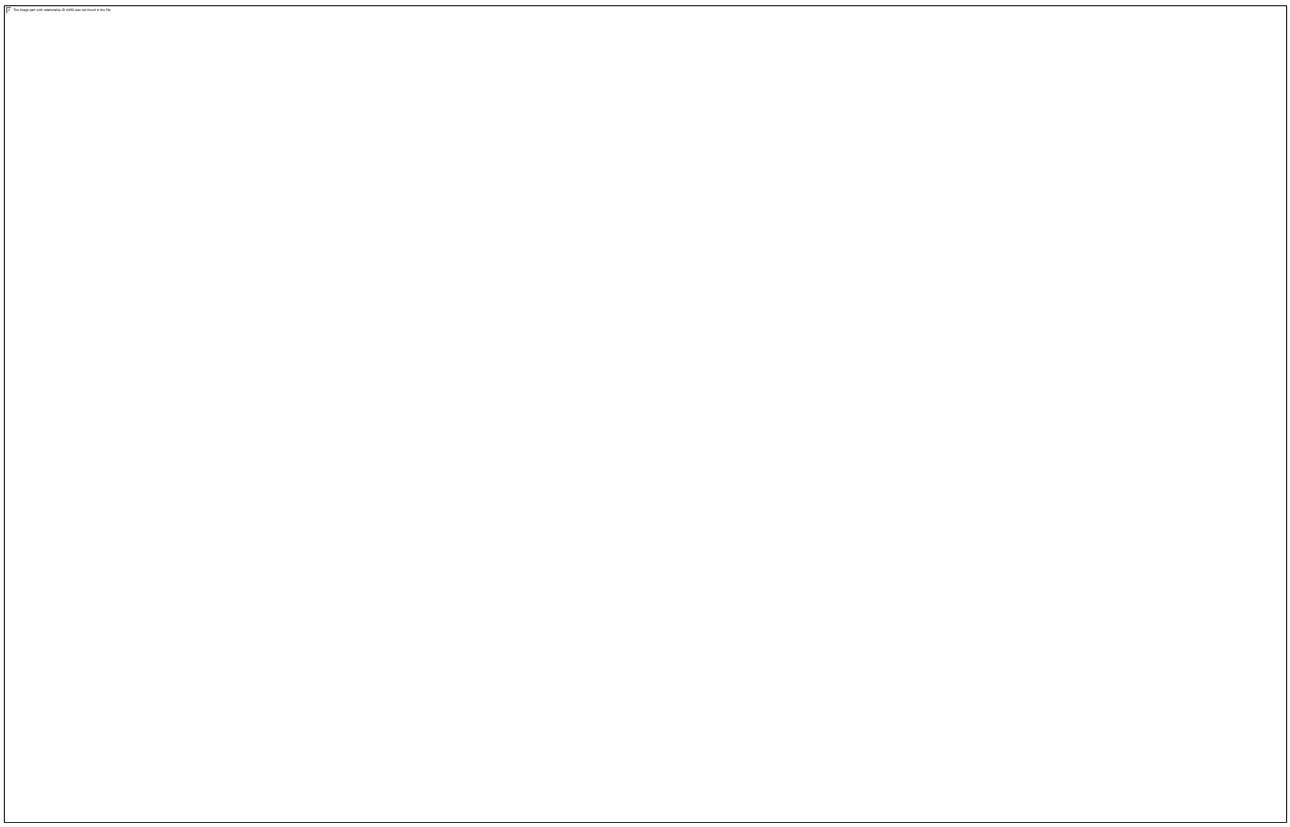


Рисунок 1 – Типовой объект информатизации

На данном примере можем отметить важность выбора и обустройства защищаемого помещения, а также необходимость использования средств активной защиты информации от утечки по техническим каналам.

Рассмотрим подробнее акустические и виброакустические каналы утечки

речевой информации.

Акустические каналы представляют собой те, по которым информация может быть перехвачена с помощью микрофонов воздушной проводимости или прослушана непосредственно человеком. Виброакустические – по которым информация может быть снята с помощью микрофонов твердой среды (виброметров, акселерометров).

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится источник речевой информации, в результате виброакустического преобразования, возникают вибрационные колебания. Средой распространения сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.).[1] Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушан, зарегистрирован на машинном носителе информации или передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному каналу передачи информации.

Наибольшую опасность представляют окна и технологические каналы с большой площадью поперечного сечения, такие, как короба коммуникаций и воздуховоды вентиляции. Если поперечные размеры короба сравнимы с длиной звуковых волн, затухание при распространении по нему звука составляет 0,01…1 дБ/м. Следующими по степени опасности являются каналы с размерами, значительно меньшими длины звуковых волн, как отверстия электропроводки, щели и трещины в строительных конструкциях, неплотности дверных и оконных проемов. В таких каналах затухание звука более значительно и находится в диапазоне 1…20 дБ/м. [1]

Общий случай работы виброакустического канала представлен структурной схемой, изображенной на рисунке 2.

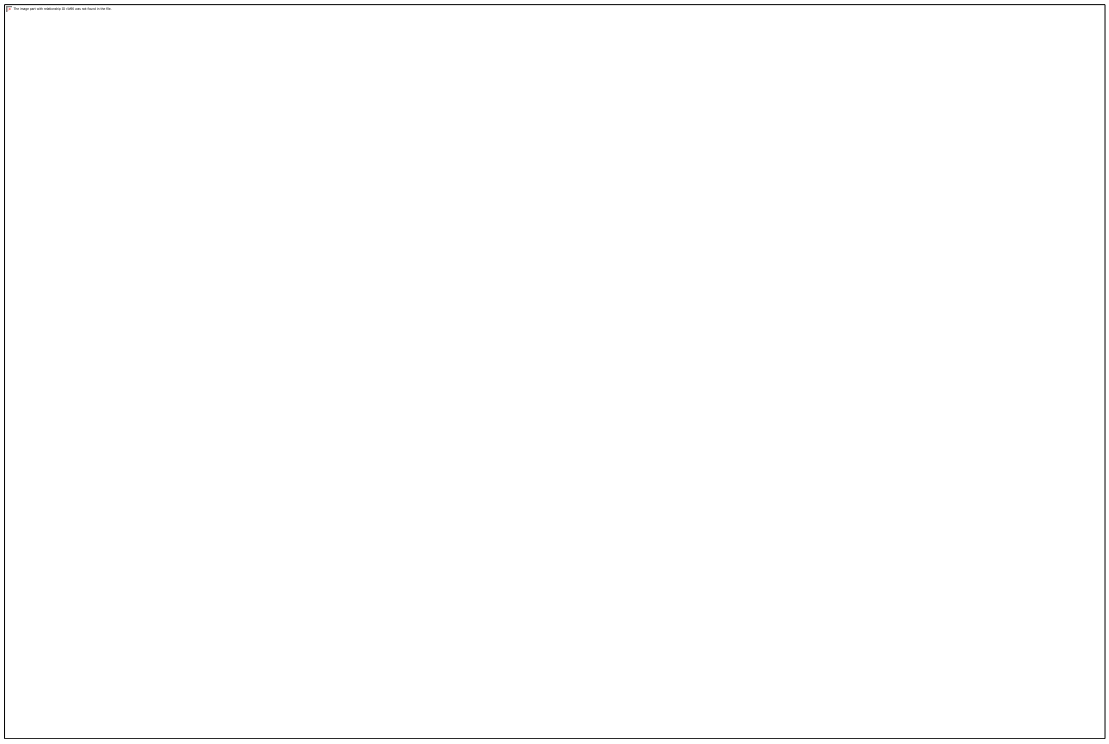


Рисунок 2 – Структурная схема прямого виброакустического канала

Таким образом, чтобы снизить коэффициент словесной разборчивости, принятый в качестве критерия защищенности речевой информации, помимо применения возможных пассивных способов защиты, необходимо принять меры ко

вводу в информационный поток достаточного уровня фоновых шумов и виброколебаний. Эффективность принятых мер будет определена экспериментально. В качестве измерительного оборудования будут использованы измерители шума и вибрации, анализатор спектра, автоматизированный программно-аппаратные комплекс.

***Заключение.*** Разработка системы активной защиты контролируемой зоны от утечки речевой информации через виброакустический канал представляет собой значимый научно-технический проект, направленный на решение проблем конфиденциальности и безопасности данных. Ключевые особенности проекта включают комплексный подход к защите информации, применение современных технологий и методов, а также анализ эффективности и применимости различных методов защиты.

Данная система будет способствовать повышению уровня безопасности циркуляции речевой информации и обеспечит надежную защиту от утечки данных через виброакустический канал.

### *Список литературы*

*1. Титов, А.А. Технические средства защиты информации. / А.А.Титов. – Томск: ТУСУР, 2010. – 194 с.*

*2. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.*

*3. Каторин, Ю. Ф. Защита информации техническими средствами: учебное пособие / Ю. Ф. Каторин, А.В. Разумовский, А.И. Спивак; – С.: Редакционно-издательский отдел НИУ ИТМО, 2012. – 417 с.*

UDC 534.2

## SYSTEM FOR ACTIVE PROTECTION OF THE CONTROLLED AREA AGAINST LEAKAGE OF VOICE INFORMATION VIA VIBROACOUSTIC CHANNEL

*Prokoshin M.I.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vrublevskiy I.A. – Cand. of Sci., Associate Professor*

**Annotation**. The materials of the report discuss the development of a system for protecting a dedicated (protected) room from leakage of speech information via a vibroacoustic channel. The development of this system includes an integrated approach to ensuring the protection of speech information and is associated with the use of modern technologies and methods, which will help increase the level of security of secret negotiations.

**Keywords:** protected room, speech information, active protection, vibroacoustic channel.

УДК 004.056.53

# АНАЛИЗ И ЗАЩИТА ОТ DDOS-АТАК В СЕТЯХ НА БАЗЕ GNS3

*Самаке Б.А.*

*гр.267241*

*Белорусский государственный университет информатики и радиоэлектроники*[1]
*г. Минск, Республика Беларусь*

*Научный руководитель: Белоусова Е.А. – кандидат технических наук*

**Аннотация.** В данной статье рассматривается один из наиболее распространенных типов атак, который является DDoS-атак, которая направлена на перегрузку серверов и сетей большим объемом сетевого трафика. В данной статье будет проведен анализ DDoS-атак и рассмотрены способы их защиты в сетях, построенных на базе симулятора сетей GNS3.

**Ключевые слова:** DDoS-атак, Hping3, wireshark, IP-адрес, локальная сеть.

***Введение.*** С динамическим развитием технологий информационной безопасности, компьютерные атаки становятся все более сложными и разрушительными. Одним из наиболее распространенных типов атак является DDoS-атаки, которые направлены на нарушение нормального трафика сервера. Они направлены на то, чтобы перегрузить устройства, службы или сеть предполагаемой цели фальшивым интернет-трафиком, сделав их недоступными для пользователей [1]. В данной статье будет проведен анализ DDoS-атак построенных на базе симулятора сетей GNS3.

Рассмотрим сценарий атаки, для выполнения DDos-атак, воспользуемся сетевым инструментом Hping3, который является утилитом командной строки для создания и отправки пользовательских пакетов TCP/IP. Это универсальный инструмент, позволяющий выполнять различные задачи. А в качестве анализатора трафика для анализа DDos-атаки воспользуемся инструментом wireshark.

Для проверки DDoS-атак необходимо было смоделировать локальную сеть. Для этого был мы воспользовались программой GNS3. Он основан на Qemu и Dynamips и является графическим интерфейсом для создания локальных сетей с использованием Qemu. В GNS3 устройства разных производителей можно добавлять самостоятельно. Также GNS3 предоставляет более точную представление в настройки оборудований [2].

На рисунке 1 представлена модель локальной сети в программном эмуляторе сети GNS3. В смоделированной сети выделено четыре виртуальные сети (VLAN),один веб сервер на котором будет произведена атака, а также оборудование который будет проводить DDos-атаку с помощью Hping3.

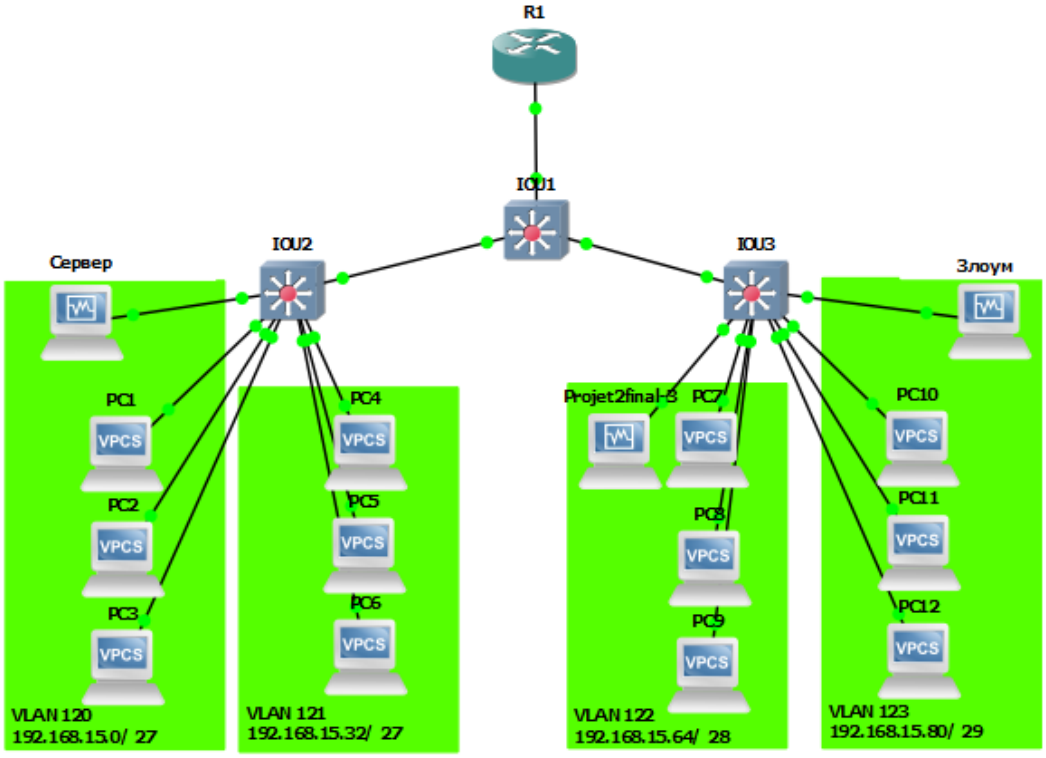



Рисунок 1 – Модель локальной сети для моделирования атаки

После построение модели, на рисунке 2 представлена команда с помощью, которого будет сгенерировано большое количество пакетов ICMP на указанный IP адрес.

```
glpi@Glpi:~$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood 192.168.15.2
[sudo] Mot de passe de glpi :
HPING 192.168.15.2 (enp0s8 192.168.15.2): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Рисунок 2 – команда для генерирование большого количества пакетов ICMP

После генерирование такого большого количество пакетов, сервер будет перегрузон этими пакетами и выйдет из строя, что приведет к невозможности другим пользователям получать доступ к серверу. Рисунок 3 покаживает аномальный трафик, который может является признаком DDoS-атаки.

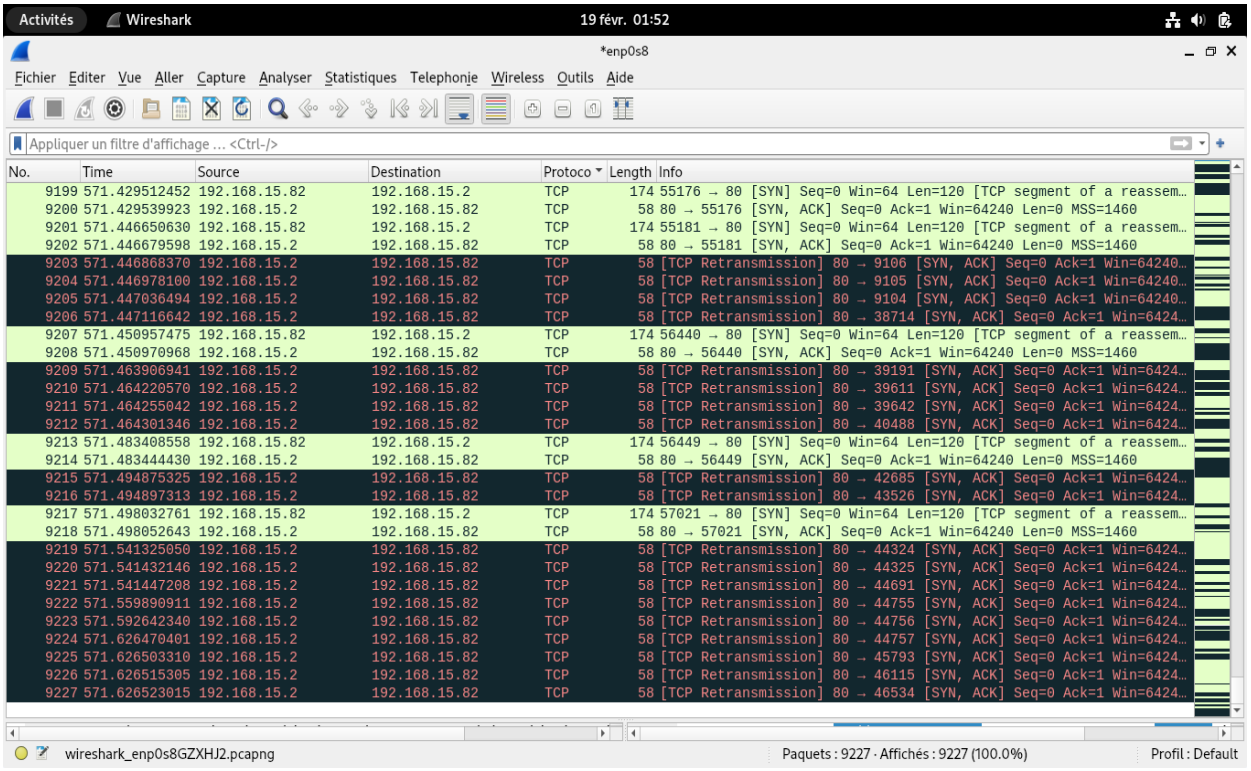



Рисунок 3 – Признак DDoS-атаки

На рисунке ниже представлен результат успешной DDoS-атаки, после которого нет доступа к серверу.


Рисунок 4 – Результат выполнение DDoS-атак

Существует несколько методов защиты от DDoS-атак, один из способов защиты - это использование механизмов обнаружения и фильтрации DDoS-трафика на уровне сети. Для этого можно использовать специализированные устройства, такие как фаерволы и IPS/IDS, которые могут распознавать и блокировать подозрительный трафик.

Другим методом защиты от DDoS-атак является распределение нагрузки на несколько серверов или узлов сети. Это позволяет снизить вероятность отказа в обслуживании в случае DDoS-атаки путем равномерного распределения нагрузки между несколькими узлами сети.

***Заключение.*** DDoS-атаки представляют серьезную угрозу для сетей и серверов, поэтому необходимы соответствующие меры защиты. На базе симулятора сетей GNS3 можно провести анализ и защиту от DDoS-атак, используя различные методы, такие как обнаружение и фильтрация трафика, распределение нагрузки и алгоритмы маршрутизации. Эти методы помогут снизить вероятность успешной DDoS-атаки и обеспечить стабильную работу сети.

***Список использованных источников:***

*1. Богомолова Л.В. КЛАССИФИКАЦИЯ DDOS-АТАК И ИХ РЕАЛИЗАЦИЯ. – Режим доступа : КЛАССИФИКАЦИЯ DDOS-АТАК И ИХ РЕАЛИЗАЦИЯ (cyberleninka.ru) . – Дата доступа : 19.02.2024.*

*2. Кулябов Д. С. Средства моделирования сетей для целей обучения– режим доступа: Средства моделирования сетей для целей обучения | Д. С. Кулябов (yamadharma.github.io). – Дата доступа: 25.03.2023.*

UDC 004.056.53

## ANALYSIS AND PROTECTION AGAINST DDOS ATTACKS IN GNS3-BASED NETWORKS

*Samake B.A.*

*gr.267241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Belousova E.S. – PhD (Tech.), associate professor at the information security department*

**Annotation** This article considers one of the most common types of attacks, which is DDoS attacks, which are aimed at overloading servers and networks with a large volume of network traffic. This article will analyze DDoS attacks and consider ways of their protection in networks built on the basis of the GNS3 network simulator.

**Keywords:** DDoS attack, Hping3, wireshark, IP address, local area network

**Annotation**. The materials of the report discuss the development of a system for protecting a dedicated (protected) room from leakage of speech information via a vibroacoustic channel. The development of this system includes an integrated approach to ensuring the protection of speech information and is associated with the use of modern technologies and methods, which will help increase the level of security of secret negotiations.

**Keywords:** protected room, speech information, active protection, vibroacoustic channel.

УДК 004.056.5

## СИСТЕМА МОНИТОРИНГА СОБЫТИЙ ИБ В ACTIVE DIRECTORY

*Смалько В.П.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Борботько Т.В. – доктор технических наук, профессор, зав. кафедры ФИБ*

**Аннотация.** Противодействию нарушителю в информационных системах основанных на

использовании контроллеров доменов обусловлено обнаружению событий информационной безопасности, возникающих в них при кибератаке. Такого рода воздействия являются разрушительными и приводят к неприемлемому ущербу. Поэтому мониторинг подобного рода событий является обязательным процессом в управлении информационной безопасностью организации.

**Ключевые слова:** события ИБ, система мониторинга, Active Directory, MITRE ATT&CK

***Введение.*** В условиях современной информационной среды одним из ключевых аспектов обеспечения безопасности корпоративных информационных систем является эффективное мониторинг и реагирование на события, связанные с информационной безопасностью. Active Directory (AD) как центральная служба управления доступом и идентификации в корпоративных сетях, подверженный различным угрозам, становится объектом повышенного внимания вопросов информационной безопасности.

Целью исследования является анализ кибератак на AD и разработка системы мониторинга событий ИБ в AD. В работе будут рассмотрены основные этапы кибератаки на AD в соответствии с MITRE ATT&CK, основные техники, используемые нарушителями, а также различные виды кибератак на AD. Затем будет представлена разработка системы мониторинга событий ИБ в AD, включая ее цели, задачи и методы в соответствии с MITRE ENGAGE.

***Основная часть.*** Каждая кибератака на Active Directory может быть разделена на несколько этапов, которые злоумышленники используют для достижения своих целей. MITRE ATT&CK Framework определяет эти этапы, предоставляя систематизированный подход к анализу кибератак и улучшению систем защиты, состоящий из тактик и техник (рисунок 1).

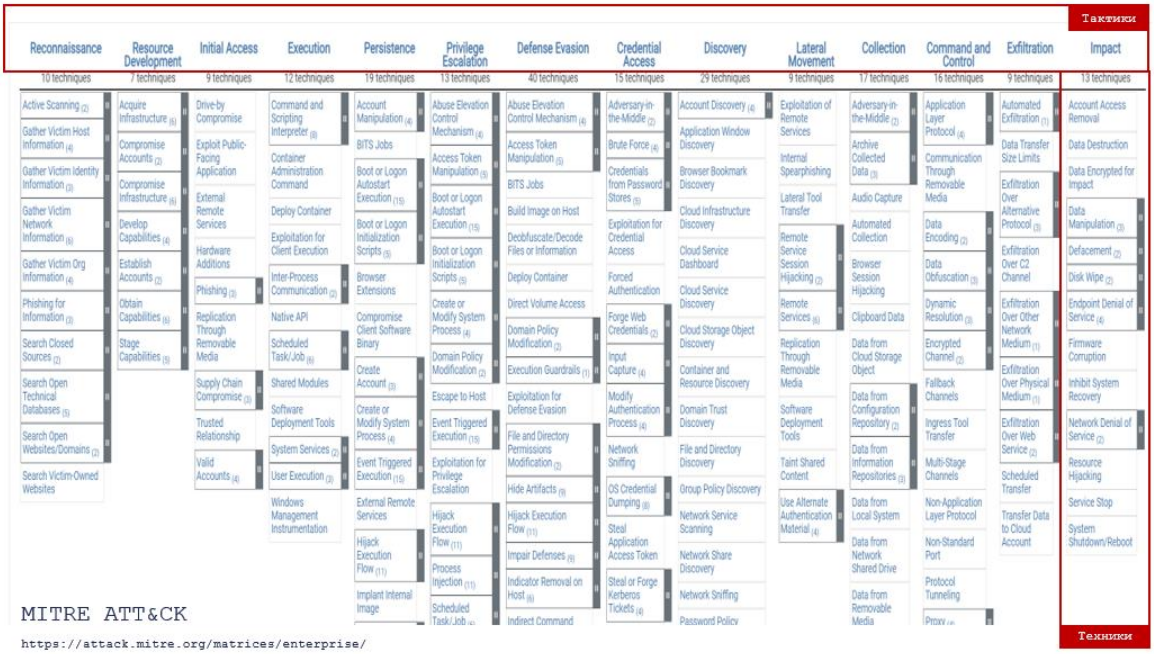



Рисунок 1 – матрица MITRE ATT&CK

На этапе разведки (Reconnaissance) злоумышленники исследуют AD, собирая информацию о пользователях, группах и ресурсах. Например, сканирование SPN (Service Principal Names), сбор данных из общих ресурсов - сетевые папки, файловые сервера, базы данных, NAS (Network Attached Storage), а также такие пользовательские данные (при

наличии привилегий) как учетные данные пользователей, локальные данные, пользовательские файлы. При наличии привилегий, Microsoft Exchange и Outlook также могут быть скомпрометированы [1].

На этапе разработка ресурсов (Resource Development), злоумышленники создают или компрометируют учетные записи и другие ресурсы, которые будут использоваться для атаки на AD. Это может включать в себя создание фальшивых учетных записей или использование украденных учетных данных [2].

На этапе начального доступа (Initial Access), злоумышленники используют различные методы, такие как фишинг или вредоносное ПО, чтобы получить первоначальный доступ к AD. Это может включать в себя отправку фишинговых писем с вредоносными вложениями или ссылками [2].

На этапе выполнения (Execution), злоумышленники выполняют вредоносный код или ПО на скомпрометированной системе. Это может включать в себя использование скриптовых языков, таких как PowerShell, для выполнения вредоносного кода [2].

На этапе закрепления (Persistence), з**лоумышленники используют различные** методы, чтобы сохранить свой доступ к AD. Это может включать в себя создание служб Windows или заданий планировщика, которые автоматически запускают вредоносный код при каждом входе в систему [2].

На этапе эскалации привилегий (Privilege Escalation), злоумышленники используют различные методы, чтобы повысить свои привилегии в AD. Это может включать в себя извлечение пароля локального администратора из SYSVOL (общедоменный ресурс Active Directory, к которому у всех авторизованных пользователей есть доступ на чтение. SYSVOL содержит сценарии входа, данные групповой политики и другие данные, которые должны быть доступны везде, где распространяется политика домена.), также возможно использование метода делегирования Kerberos, загрузка dll библиотеки на DNS-сервер пользователем, входящим в группу DNSAdmins или обладающим правами на запись в объекты DNS-сервера и др. методы [1].

На этапе обхода защиты (Defense Evasion), злоумышленники используют различные методы, чтобы избежать обнаружения. Это может включать в себя отключение антивирусного программного обеспечения или изменение настроек безопасности [2].

На этапе доступа к учетным данным (Credential Access), злоумышленники используют различные методы, чтобы получить доступ к учетным данным. Это может включать в себя кражу хэшей паролей или билетов Kerberos, получение копии файла ntds.dit (база данных, в которой хранится информация Active Directory) [1].

Рассмотренная часть тактик (этапов) показывает, нам что для достижения целей злоумышленник выполняет большое количество операций, которые непременно оставляют следы (артефакты) в системе.

Благодаря найденным артефактам и целям, которые преследует организация при защите своей инфраструктуры может быть использована матрица активной защиты MITRE ENGAGE. MITRE ENGAGE — это платформа для планирования и обсуждения операций по взаимодействию с противником, которая позволяет взаимодействовать с противниками и достигать целей в области кибербезопасности.

. Он основан на простом предположении: поскольку компрометация сети часто неизбежна, защитники могут использовать методологии вовлечения противника, чтобы гарантировать, что компрометация не означает потерю. Вовлечение противника предлагает защитникам возможность увеличить стоимость и уменьшить ценность операций противника. Фреймворк был разработан для обороны от кибератак. Он соответствует фреймворку MITRE ATT&CK, что позволяет специалистам быстро определить уязвимости

злоумышленника при использовании конкретной техники ATT&CK и как использовать эти уязвимости [3].

Для обеспечения более эффективной защиты от киберугроз может быть разработана система мониторинга информационной безопасности Active Directory, основанная на MITRE ATT&CK и MITRE ENGAGE.

Система мониторинга ИБ Active Directory, основанная на матрицах MITRE, может включать следующие компоненты:

- мониторинг аутентификационных сертификатов, который отслеживает запросы сертификатов AD CS (EID 4886), а также выданные сертификаты (EID 4887) на предмет аномальной активности, включая неожиданные регистрации сертификатов и признаки злоупотребления в атрибутах сертификата;
- мониторинг билетов Kerberos, который отслеживает аномальную активность Kerberos, такой как деформированные или пустые поля в событиях входа/выхода из Windows (EID 4624, 4672, 4634), шифрование RC4 в билетах предоставления билетов (TGTs) и запросы билетов предоставления услуг (TGS) без предварительных запросов TGT;
- мониторинг альтернативных материалов аутентификации: отслеживание запросов новых билетов предоставления билетов или билетов на услуги к контроллеру домена, таких как Windows EID 4769 или 4768, которые могут использовать альтернативные материалы аутентификации, такие как хэши паролей, билеты Kerberos и токены доступа к приложениям, чтобы перемещаться по среде и обходить обычные системные контроли доступа.

***Заключение.*** Систем не ограничена описанными компонентами и может быть дополнена. Разработанная система позволит обнаруживать аномалии и подозрительные действия, основываясь на тактиках, методах и процедурах, описанных в матрицах MITRE.

### *Список использованных источников:*

*1. Active Directory глазами хакера. – СПБ.: БХВ-Петербург, 2022 – 176с. – Ralf Hacker.*

*2. Enterprise Matrix [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/matrices/enterprise/. – Дата доступа: 18.02.2024.*

*3. MITRE Engage: A Framework and Community for Cyber Deception [Электронный ресурс]. – Режим доступа: https://www.mitre.org/news-insights/impact-story/mitre-engage-framework-and-community-cyber-deception. – Дата доступа: 18.02.2024.*

UDC 004.056.5

## INFORMATION SECURITY EVENT MONITORING SYSTEM IN ACTIVE DIRECTORY

*Smalko V. P.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics,*
*Minsk, Republic of Belarus*

*Scientific supervisor: Borbotko T.V. – Doctor of Technical Sciences, Professor, Head of the FIB Department*

**Annotation.** Countering an intruder in information systems based on the use of domain controllers is due to the detection of information security events that occur in them during a cyberattack. Such impacts are devastating and lead to unacceptable damage. Therefore, monitoring of such events is a mandatory process in the management of information security of an organization.

**Keywords:** information security events, Monitoring system, Active Directory, MITRE ATT&CK.

УДК 004.056

# НАСТРОЙКА АУДИТА БЕЗОПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

*Смотрук Г.С.*

*гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Петров С.Н. – кандидат технических наук, доцент*

**Аннотация.** Рассмотрены настройки аудита безопасности в операционных система семейства Windows в соответствии с законодательством Республики Беларусь. Правильно настроенный аудит безопасности играет важную роль для обеспечения информационной безопасности.

**Ключевые слова:** приказ Оперативно-аналитического центра № 130, аудит информационной безопасности, операционные системы

***Введение.*** Двадцать пятого июля 2023 года вышел Приказ Оперативно-аналитического центра при президенте Республики Беларусь № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40» [1]. В нем подробно описаны условия, необходимые для обеспечения информационной безопасности, формализованы алгоритмы действий при возникновении киберинцидентов, описаны требования к центрам кибербезопасности и их типовая структура.

Приказом определен перечень типов и записей событий информационной безопасности, которые должны централизованно собираться, обрабатываться, накапливаться, систематизироваться и храниться не менее одного года (далее – перечень). А их сбор должен осуществляться в круглосуточном режиме.

***Основная часть.*** Для операционных систем вышеуказанный перечень выглядит следующим образом: запуск и (или) остановка системы; запуск и (или) остановка процессов; подключение съемных машинных носителей информации; подключение иных периферийных устройств к портам ввода (вывода) (мобильные устройства, сетевые адаптеры, беспроводные модемы и иные); установка и удаление программного обеспечения (изменение компонентов программного обеспечения); аутентификация (вход и (или) выход) пользователей в операционной системе, успешные и неуспешные попытки аутентификации; использование привилегированных учетных записей пользователей; создание, удаление, модификация учетных записей пользователей; неудавшиеся или отмененные действия пользователя и (или) процессы; создание или изменение параметров заданий в планировщике задач; установка, удаление, перезапуск, ошибка запуска службы и (или) сервиса; изменение системной конфигурации, в том числе сетевых настроек и средств межсетевого экранирования; изменение или попытки изменения настроек и средств управления защитой системы, в том числе антивирусного программного обеспечения, систем обнаружения и предотвращения вторжений; контроль несанкционированных сетевых соединений, в том числе попыток несанкционированного удаленного доступа, создания общих сетевых ресурсов, использования нестандартных сетевых портов.

В соответствии с вышеуказанным перечнем сформирована политика аудита [2], представленная в Таблице 1.

Таблица 1 – Политика аудита безопасности ОС Windows

| Категория аудита безопасности | Идентификаторы событий и их описание |
|---|---|
| Аудит изменения состояния безопасности | 4608: Windows запускается<br>4609: завершение работы Windows<br>4616: системное время было изменено<br>4621: администратор восстановил систему из CrashOnAuditFail |
| Аудит создания процессов | 4688: создан новый процесс<br>4696: процессу был назначен первичный маркер |
| Аудит завершения процессов | 4689: процесс завершился |
| Аудит съемного носителя | 4656: запрошен дескриптор объекта<br>4658: дескриптор объекта закрыт<br>4663: предпринята попытка доступа к объекту |
| Аудит активности PNP | 6416: новое внешнее устройство было распознано системой<br>6419: был сделан запрос на отключение устройства<br>6420: устройство было отключено<br>6421: был сделан запрос на включение устройства<br>6422: устройство было включено<br>6423: установка этого устройства запрещена системной политикой<br>6424: установка этого устройства была разрешена, после того как ранее было запрещено политикой |
| Аудит событий, создаваемых приложениями | 4665: предпринята попытка создать контекст клиента приложения<br>4666: приложение попыталось выполнить операцию<br>4667: удален контекст клиента приложения<br>4668: приложение инициализировано<br>7045: в системе установлена служба<br>11724: удаление успешно завершено |
| Аудит входа в систему | 4624: учетная запись успешно выполнена<br>4625: не удалось войти в учетную запись<br>4648: предпринята попытка входа с использованием явных учетных данных<br>4675: идентификаторы безопасности были отфильтрованы |
| Аудит выхода из системы | 4634: процесс выхода был завершен для пользователя<br>4647: инициированный пользователем выход |
| Аудит проверки учетных данных | 4774: учетная запись была сопоставлена для входа<br>4775: не удалось сопоставить учетную запись для входа<br>4776: компьютер пытался проверить учетные данные для учетной записи<br>4777: контроллер домена не смог проверить учетные данные для учетной записи |
| Аудит специального входа | 4964: для нового входа назначены специальные группы<br>4672: специальные привилегии, назначенные новому входу |
| Аудит управления учетными записями пользователей | 4720: создана учетная запись пользователя<br>4722: учетная запись пользователя включена<br>4723: предпринята попытка изменить пароль учетной записи<br>4724: предпринята попытка сброса пароля учетной записи<br>4725: учетная запись пользователя отключена<br>4726: учетная запись пользователя удалена<br>4738: учетная запись пользователя была изменена<br>4740: учетная запись пользователя заблокирована<br>4765: журнал безопасности был добавлен в учетную запись<br>4766: попытка добавить журнал идентификаторов безопасности в учетную запись завершилась ошибкой |

| Категория аудита безопасности | Идентификаторы событий и их описание |
|---|---|
| | 4767: учетная запись пользователя была разблокирована<br>4780: список ACL был установлен для учетных записей, которые являются членами групп администраторов<br>4781: имя учетной записи было изменено |
| Аудит доступа к службе каталогов | 4662: с объектом выполнена операция<br>4661: запрошен дескриптор объекта |
| Аудит других событий доступа к объектам | 4691: запрошен косвенный доступ к объекту<br>5148: платформа фильтрации Windows обнаружила DoS-атаку и вошла в оборонительный режим; пакеты, связанные с этой атакой, будут отброшены<br>5149: атака DoS утихла, и нормальная обработка возобновляется<br>4698: была создана запланированная задача<br>4699: запланированная задача удалена<br>4700: была включена запланированная задача<br>4701: запланированная задача отключена<br>4702: запланированная задача обновлена |
| Аудит других системных событий | 5030: не удалось запустить службу брандмауэра Windows |
| Аудит расширения системы безопасности | 4697: в системе была установлена служба |
| Аудит целостности системы | 4612: внутренние ресурсы, выделенные для постановки сообщений аудита, исчерпаны, что привело к потере некоторых аудитов |
| Аудит изменения политики на уровне правил MPSSVC | 4944: при запуске брандмауэра Windows была активна следующая политика<br>4945: при запуске брандмауэра Windows было указано правило<br>4946: в список исключений брандмауэра Windows внесено изменение (было добавлено правило)<br>4947: в список исключений брандмауэра Windows внесено изменение. (правило было изменено)<br>4948: в список исключений брандмауэра Windows внесено изменение. (правило было удалено)<br>4949: параметры брандмауэра Windows были восстановлены до значений по умолчанию<br>4950: параметр брандмауэра Windows изменен<br>4951: правило было проигнорировано, так как его основной номер версии не распознан брандмауэром Windows<br>4956: брандмауэр Windows изменил активный профиль<br>4957: брандмауэр Windows не применял следующее правило<br>4958: брандмауэр Windows не применил следующее правило, так как оно ссылается на элементы, не настроенные на этом компьютере |
| Аудит изменения состояния безопасности | 4616: системное время было изменено |
| Аудит изменения политики аудита | 4715: политика аудита (SACL) для объекта была изменена<br>4719: политика аудита системы была изменена<br>4817: параметры аудита объекта были изменены |

| Категория аудита безопасности | Идентификаторы событий и их описание |
|---|---|
| | 4902: создана таблица политик аудита для каждого пользователя<br>4906: значение CrashOnAuditFail изменилось<br>4907: параметры аудита объекта были изменены<br>490: таблица входа в специальные группы изменена<br>4912: политика аудита на пользователя была изменена<br>4904: предпринята попытка зарегистрировать источник событий безопасности<br>4905: предпринята попытка отменить регистрацию источника событий безопасности |
| Аудит изменения политики проверки подлинности | 4670: изменены разрешения для объекта<br>4706: для домена было создано новое доверие<br>4707: удалено доверие к домену<br>4716: сведения о доверенном домене были изменены<br>4713: политика Kerberos была изменена<br>4717: доступ к системной безопасности был предоставлен учетной записи<br>4718: доступ к системной безопасности был удален из учетной записи<br>4739: политика домена изменена<br>4864: обнаружен конфликт пространства имен<br>4865: добавлена запись сведений о доверенном лесе<br>4866: удалена запись сведений о доверенном лесе<br>4867: изменена запись сведений о доверенном лесе |
| Аудит общего файлового ресурса | 5140: доступ к объекту сетевой общей папки<br>5142: добавлен объект сетевой общей папки<br>5143: объект сетевой общей папки был изменен<br>5144: объект сетевой общей папки был удален<br>5168: сбой проверки имени субъекта-службы для SMB/SMB2 |

Правильно настроенный аудит безопасности является неотъемлемой частью комплексной стратегии информационной безопасности. Преимущества правильно настроенного аудита безопасности:

Обнаружение угроз и реагирование на инциденты: аудит позволяет организациям отслеживать и регистрировать все важные события безопасности. Это помогает выявлять подозрительную активность, такую как несанкционированные попытки входа в систему или изменения в критических системных файлах, что позволяет организациям быстро реагировать на потенциальные угрозы.

Выявление уязвимостей и улучшение безопасности: аудит помогает выявлять уязвимости в системе безопасности и принимать меры по их устранению, повышая общую эффективность информационной безопасности.

Предотвращение потерь и финансовых последствий: эффективный аудит помогает предотвращать нарушения безопасности и минимизировать их последствия, защищая организации от потерь данных, финансовых потерь и репутационного ущерба.

***Заключение.*** Правильно настроенный аудит безопасности позволяет выбирать главные и нужные события безопасности, подлежащие централизованной консолидации для последующего обращения к ним при расследовании инцидентов информационной безопасности. Это помогает избежать сбора ненужных событий, которые могут перегрузить систему и затруднить выявление реальных угроз. Внедрение и правильная настройка аудита безопасности должны быть приоритетом для всех организаций, стремящихся защитить свои информационные активы.

***Список литературы***

*4. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf. – Дата доступа: 15.02.2024.*

*5. Параметры политики расширенного аудит безопасности Windows. [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings – Дата доступа: 15.02.2024.*

UDC 004.056

## SETTING UP A SECURITY AUDIT IN WINDOWS OPERATING SYSTEMS

*Smotruk H.S.*

*gr. 367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Petrov S.N. – PhD, associate professor*

**Annotation**. The settings for security audits in operating systems of the Windows family are considered in accordance with the legislation of the Republic of Belarus. A properly configured security audit plays an important role in ensuring information security.

**Keywords:** Order of the Operational Analytical Center No. 130, information security audit, operating systems

УДК 004.056.53

## МЕТОДЫ ПЕРЕХВАТА ИНФОРМАЦИИ В ОПТОВОЛОКОННЫХ КАНАЛАХ СВЯЗИ

*Сухоцкий В.В.*

*гр.261402*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Бойправ О.В. – кандидат технических наук, доцент кафедры ЗИ*

**Аннотация.** В материалах доклада рассматриваются методы перехвата информации в оптоволоконных каналах связи. Выявление, оценка эффективности и недостатков данных методов позволит разработать меры противодействия им и повысить безопасность информации, передаваемой по таким каналам.

**Ключевые слова:** оптоволоконный канал связи, перехват информации.

***Введение.*** Современные телекоммуникационные компании переходят к использованию оптоволоконных каналов связи. Это связанно со следующими важными преимуществами таких каналов по сравнению с каналами, основанными на металлических кабелях:

– высокая дальность передачи информации без усиления;

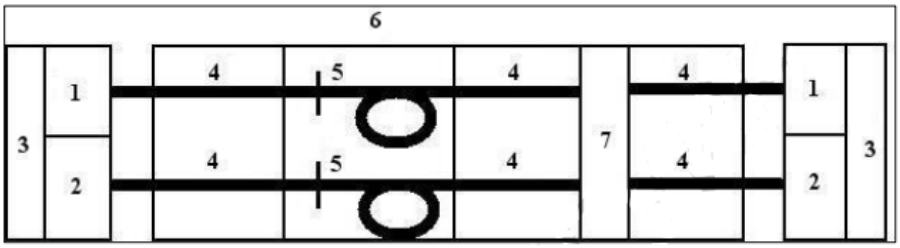
– высокая пропускная способность;

– большие возможности мультиплексирования.

Также преимуществом оптоволоконных каналов связи является то, что для оптоволоконных кабелей не характерны побочные электромагнитные излучения и наводки, что делает очень сложным вмешательство нарушителя в такие каналы связи и перехват информации, передаваемой по ним. Однако последние исследования доказывают, что это

возможно. Поэтому важно исследовать данные методы перехвата информации и понять их принципы, чтобы уметь обнаруживать их реализацию и противостоять им.

***Основная часть.*** Рассмотрим схему оптоволоконного канала связи (рисунок 1).




1 – передатчик оптического сигнала; 2 – приемник оптического сигнала; 3 – оборудование мультиплексирования; 4 – оптоволоконный кабель; 5 – сварное соединение двух оптических волокон на местах стыка строительных длин; 6 – соединительная муфта, в которую помещаются сростки оптических волокон; 7 – пункт регенерации/ усиления оптического сигнала

Рисунок 1 – Схема оптоволоконного канала связи

Места 1, 2, 3, и 7 в оптоволоконном канале связи (рисунок 1) являются наиболее защищенными, так как располагаются на режимных объектах, обеспечивающих высокий уровень защиты. Сам оптоволоконный кабель 4 и сварное соединение 5 являются слабо защищенными частями оптоволоконного канала связи, так как выходят за пределы объектов с высоким уровнем защиты от несанкционированного доступа, следовательно, в этих местах может произойти съем информации нарушителем. Поэтому к наиболее вероятным методам перехвата информации в оптоволоконных каналах связи относятся (рисунок 2):

1) контактный перехват, формируемый путем отвода части информационного оптического сигнала из канала связи в канал утечки, делящийся на:

– A – перехват с разрывом оптоволоконного кабеля и вставкой;

– B – перехват с прямым доступом к оптоволоконному кабелю;

2) дистанционный перехват, формируемый путем регистрации оптических информативных сигналов без или с воздействием на канал связи, подразделяемый на:

– C – перехват с регистрацией паразитных и сопутствующих излучений;

– D – перехват на основе параметрических методов.

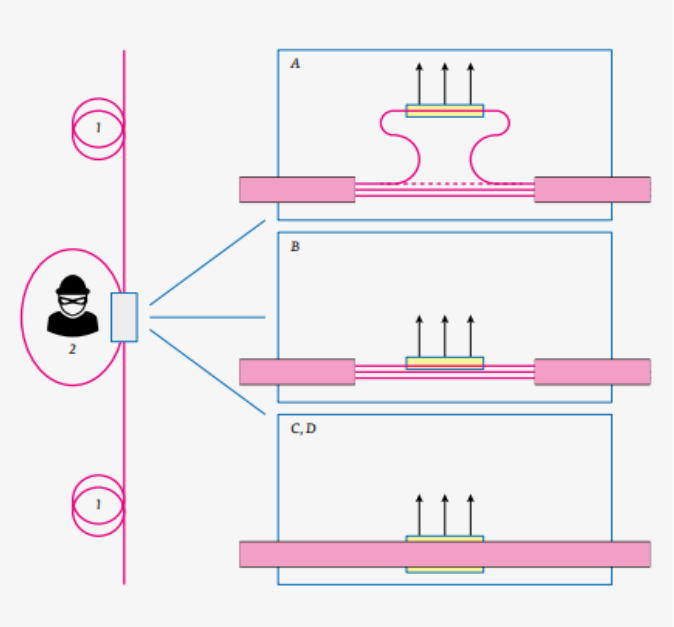



Рисунок 2 – Схематическая иллюстрация наиболее вероятных методов перехвата информации в оптоволоконных каналах связи

Следует отметить, что перехват информации с разрывом кабеля проще всего обнаружить, поэтому его, скорее всего, нарушители редко применяют. Для безразрывного перехвата информации без принудительного отвода мощности используется излучение, возникающее естественным образом в результате рассеяния света на муфтах, соединителях, устройствах ввода и вывода оптической мощности, самом оптоволоконном кабеле. Для того, чтобы осуществить отвод информационного сигнала с кабеля на каком-либо участке без его разрыва, чаще используется локальное воздействие на его волоконные световоды. Это приводит к изменению их оптических свойств, что обуславливает выход оптического излучения за пределы оптоволокна. Методы воздействия на волокно: изгиб волокна, изменение диаметра волокна (например, путем давления), микроизгибы волокна, воздействие химическими реактивами, влияние звуковыми волнами. Однако при изменении диаметра волокна, химическом и акустическом воздействии на волокно световые волны распространяются из канала связи по-разному, поэтому их сложнее собирать. В случае же изгиба оптоволокна электромагнитные волны распространяются вдоль одного направления, поэтому их проще собирать с помощью систем линз и данный способ более популярный среди нарушителей для несанкционированного доступа.

**Заключение.** Методы с использованием изгиба кабеля чаще используются для перехвата информации в оптоволоконных каналах связи, чем методы безразрывного перехвата с принудительным отводом мощности, в связи с тем, что позволяют более эффективно собирать световые волны в одном месте. Следовательно, способы противодействия таким методам на практике должны реализовываться в приоритетном порядке.

## ***Список литературы***

*1. Журнал «Фотоника» [Электронный ресурс]. – 08.2020. Режим доступа : https://www.photonics.su/files/article_pdf/8/article_8588_670.pdf . – Дата доступа : 17.02.2024. – 16 с.*

*2. Дудак, М. Н. Методы несанкционированного доступа к оптическим каналам «многоволновых ВОПС / М. Н. Дудак. – Минск: БГУИР, 2020. – 14 с.*

UDC 004.056.53

## METHODS OF INFORMATION INTERCEPTION IN FIBER OPTIC COMMUNICATION CHANNELS

*Suchotsky V.V.*

*gr. 261402*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Boiprav O.V. – Cand. of Sci. (Tech.), Ass. Prof. of Department of IP*

**Annotation**. The article discusses methods of information interception in fiber optic communication channels. Identifying, evaluating the effectiveness and disadvantages of these methods will allow develop measures to counteract them and improve security of information transferred via these channels.

**Keywords:** fiber optical channel, information interception.

УДК 004.056

## АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

*Фильченков П.А.*

*магистрант кафедры защиты информации гр.367241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Бойправ О.В. – кандидат технических наук, доцент, доцент кафедры ЗИ*

**Аннотация.** В материалах доклада приведены результаты анализа наиболее распространенных и хорошо зарекомендовавших себя на практике программных средств для аудита безопасности информационных систем.

**Ключевые слова:** аудит безопасности, информационная система, программное средство, риски информационной безопасности, угроза безопасности.

***Введение.*** В настоящее время информационные системы используются в деятельности предприятий всех отраслей экономики. Они необходимы для хранения, обработки и передачи информации. Это обстоятельство обуславливает актуальность реализации мер по защите информационных систем. В целях оценки эффективности реализации этих мер, а также их проверки на соответствие требованиям технических нормативных и правовых актов необходимо периодически проводить аудит информационной безопасности в целом и аудит безопасности информационных систем в частности. Под аудитом информационной безопасности понимают системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности предприятия/организации в соответствии с определенными критериями и показателями безопасности [1].

Проведение аудита информационной безопасности состоит из следующих этапов:

– инициирование процедуры аудита,

– сбор информации, необходимой для проведения аудита,

– анализ данных аудита,

– формирование и составление рекомендаций,
– подготовка аудиторского отчета.

При проведении аудита информационной безопасности рассматриваются следующие виды угроз безопасности: организационные, эксплуатационные, программно-технические, а также прочие аспекты обеспечения информационной безопасности, которые необходимо учесть в ходе проведения аудита, для определения их приоритетов [2]. Для увеличения эффективности процесса аудита безопасности информационных систем как одного из направлений аудита информационной безопасности часто используются специальные программные средства, т. к. с их применением аудитору легче оценивать меры по защите информации на предмет их соответствия требованиям, определять области, реализуемые в рамках которых мероприятия необходимо совершенствовать, обеспечивать единообразие реализуемых процедур [3]. К настоящему времени разработано большое количество программных средств, рекомендуемых для использования в ходе проведения аудита безопасности информационных систем. Каждое из таких программных средств характеризуется определенным набором функциональных возможностей, которые определяют способы их применения. В настоящей работе представлены результаты анализа функциональных возможностей

***Основная часть.***

В настоящее время наиболее часто используемыми программными средствами для аудита безопасности информационных систем являются *Efros Defence Operations, Alertix, Ankey SIEM NG, Kaspersky Unified Monitoring and Analysis Platform (KUMA), KOMRAD Enterprise SIEM, MaxPatrol SIEM, R-Vision, RuSIEM*. В таблице 1 приведено краткое описание и особенности этих программных продуктов для проведения аудита безопасности информационных систем.

Таблица 1 – Программные средства для аудита безопасности информационных систем

| № | Наименование программного средства | Краткое описание программного средства | Особенности программного средства |
|---|---|---|---|
| 1 | *Efros Defence Operations* | Многофункциональный комплекс по защите ИТ-инфраструктуры (сетевых и оконечных устройств, компонентов сред виртуализации), а также прикладного ПО: *SCADA, RPA*, СУБД. 1 ноября 2023 получил награду *CNews Awards* в номинации «Защита ИТ-инфраструктуры: платформа года». | Контроль конфигураций и топологии сети<br>Контроль целостности и проверки соответствия хостов и конечных точек<br>Оптимизация и настройка межсетевых экранов (далее – МЭ)<br>Анализ уязвимостей и построение векторов атак<br>Сбор и отображение статистики по потокам данных в сети<br>Централизованная сетевая идентификация администраторов и управление доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы *TACACS+* и (или) *RADIUS*<br>Автоматизация управления МЭ |

| № | Наименование программного средства | Краткое описание программного средства | Особенности программного средства |
|---|---|---|---|
| 2 | *Alertix* | Система представлена на рынке с 2019 г. В функциональные возможности системы входит интеграция с НКЦКИ для оперативного оповещения об инцидентах на объектах КИИ. Сбор событий реализован агентским и неагентским способами. | Блокнот аналитика;<br>Организация взаимодействия с НКЦКИ; управление конфигурацией *Sysmon* и *Beats*<br>Бессрочные лицензии<br>Гибкое управление глубиной хранения и архивации событий от источников |
| 3 | *Ankey SIEM NG* | Основными компонентами программного комплекса являются серверы сбора, обработки и хранения событий, управляющий сервер, сервер корреляции и *APM* администратора. К дополнительным компонентам относятся сервер хранения и сервер аналитики. | Автоматизированный мониторинг ИБ и непрерывное отслеживание изменений в ИТ-инфраструктуре организации<br>Автоматизированное обнаружение известных уязвимостей в программном обеспечении активов (требуется дополнительный компонент *Ankey SIEM NG VM*)<br>Выявление инцидентов среди большого количества событий из области ИБ<br>Обнаружение сбоев в работе ИТ- и ИБ-систем и реагирование на них |
| 4 | *Kaspersky Unified Monitoring and Analysis Platform* | Представлена на рынке с 2020 г., однако за несколько лет стала одним из лидеров по количеству внедрений в сегменте крупного бизнеса. Является частью экосистемы *Kaspersky Symphony XDR*, куда входят также *Kaspersky EDR Expert, Kaspersky Anti Targeted Attack, Kaspersky ASAP* и другие. Возможность интеграции более чем с 10 отечественными ИБ-системами. | Экосистемность (функциональные интеграции с другими продуктами *Kaspersky*), *RESTful API*, возможность взаимодействия с платформами реагирования (*IRP* и *SOAR*)<br>Автоматизация рутинных действий по реагированию, инвентаризации хостов, обогащению ИБ-событий контекстом<br>Производительность более 500 тыс. EPS, проверенная на реальной архитектуре заказчика<br>Минимальные системные требования и гибкая горизонтальная масштабируемость, поддержка географически распределённой инсталляции, режимы высокой доступности (*high availability*) и мультиарендности (*multi-tenancy*) |

| № | Наименование программного средства | Краткое описание программного средства | Особенности программного средства |
|---|---|---|---|
| 5 | *KOMRAD Enterprise SIEM* | Разработка АО «Эшелон Технологии» обладает визуальным конструктором правил корреляции, возможностью автоматизации реагирования на инциденты за счёт использования скриптов на *Bash* и *Python*, встроенной возможностью интеграции с ГосСОПКА. | Возможность автоматизации реагирования на инциденты<br>Визуальный конструктор правил корреляции<br>Наличие постоянно обновляемого пакета экспертиз: бесплатного и расширенного, в рамках действующей технической поддержки<br>Свободно распространяемый дистрибутив с демолицензией |
| 6 | *MaxPatrol SIEM* | Является частью линейки продуктов *Positive Technologies*, куда также входят *MaxPatrol VM, PT Network Attack Discovery (PT NAD), MaxPatrol O2, MaxPatrol EDR* и другие.<br>В *MaxPatrol SIEM* реализованы подходы для обеспечения практической результативности мониторинга событий ИБ и управления инцидентами. | Встроенный модуль обнаружения поведенческих аномалий *BAD* (*Behavioral Anomaly Detection*)<br>Инструментарий для обеспечения практической результативности работы аналитика<br>Работа с потоками более 540 тыс. *EPS*<br>Возможность применения в разных ИТ-инфраструктурах – как малых, так и масштаба страны |
| 7 | *R-Vision* | Один из самых молодых продуктов на рынке. Он вышел только в 2023 г. При его создании учитывались многолетний опыт R-Vision в разработке технологий, а также трудности, с которыми сталкиваются пользователи при работе с другими *SIEM*-системами. | Возможность расширения функциональности за счёт интеграции с другими технологиями экосистемы *R-Vision EVO*<br>Графический редактор конвейера обработки событий<br>Возможность резервирования по схемам «актив – пассив» и «*N + M*»<br>Гибкая модель хранения данных |
| 8 | *RuSIEM* | Одна из старейших российских систем этого класса, отсчитывает свою историю с 2014 г. При необходимости может доукомплектовываться другими продуктами вендора, такими как *RuSIEM IoC, RuSIEM Monitoring, RuSIEM Analytics.* | Микросервисная архитектура<br>Графический конструктор для создания правил корреляции<br>Возможность интеграции со внешними системами за счет использования прикладного интерфейса (*API*)<br>Модуль для работы с активами |

***Заключение.*** Использование специальных программных средств в ходе аудита безопасности информационных систем способствует созданию условий для соблюдения требований, предъявляемых к такому процессу, а также способствует его оптимизации и повышению точности его результатов. Основным преимуществом проанализированных программных средств *Efros Defence Operations, Alertix, Ankey SIEM NG, Kaspersky Unified Monitoring and Analysis Platform (KUMA), KOMRAD Enterprise SIEM, MaxPatrol SIEM, R-Vision, RuSIEM* является реализованная в них усовершенствованная функция оценки риска.

### *Список литературы*

*1. Бойправ, В. А. Программное средство для проведения аудита системы защиты информации организации / В. А. Бойправ, В. В. Ковалев, Л. Л. Утин // Доклады БГУИР. – 2018. – № 5(115). – С. 44–49.*

*2. Концепция информационной безопасности Республики Беларусь, утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1*

*3. Бойправ, В. А. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. 2022; 19(4): 42–52.*


UDC 004.056

## SOFTWARE TOOLS FOR AUDITING THE INFORMATION SYSTEMS SECURITY


*Filchenkov P.A.*

*Master's student of the Department of Information Security, gr.367241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Supervisor: Boiprav O.V. – PhD in Technical Sciences, Associate Professor, Associate Professor of the Department of Information Security*



**Annotation**. The article presents the results of analysis of the most widespread and well-proven in practice software tool for information systems security audit.



**Keywords:** security audit, information system, software tool, information security risks, security threat.


УДК 004.777

## СИСТЕМА И СРЕДСТВА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


*Чаган Н.Ф.*

*гр.267241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Борботько Т.В. – доктор технических наук, профессор кафедры ЗИ*



**Аннотация.** В материалах доклада рассматривается система мониторинга событий информационной безопасности, построенная на основе ханипотов, предназначенная для своевременного и точного обнаружения нарушителя в информационной сети организации, а также для использования на оборудовании или в системах (например, АСУ ТП), где использование традиционных систем, таких как EDR, AVP, DLP и т.д., не представляется возможным.



**Ключевые слова:** система мониторинга, ханипот, DDP


***Введение.*** Нарушители рано или поздно находят способ проникнуть в периметр сети организации. Затем начинается период скрытого распространения, который может продолжаться до года, в зависимости от размера сети. В настоящее время атакующие стараются не применять «шумные» инструменты – активное сетевое сканирование, взлом паролей методом перебора и т.п. Они стремятся максимально использовать информацию, которую могут собрать на скомпрометированных рабочих станциях (роли, сетевое окружение, закладки, файлы, пользователи и конфигурация систем). При этом исходят из того, что эта информация является подлинной. В качестве одного из путей совершенствования систем информационной безопасности является применение

технологии обмана, позволяющей как можно раньше обнаружить факт проникновения в инфраструктуру, переключить внимание нарушителя от критически важных элементов информационно-коммутационной сети и задержать его активные действия. В основе данной технологии лежит четкое понимание того, что любая система защиты может быть преодолена.

В настоящее время существуют современные технологии обмана нарушителей, такие как платформы для создания распределенной инфраструктуры ложных целей (Distributed Deception Platform – DDP), которые являются развитием идеи ханипотов (Honeypots) – отдельных хостов для привлечения нарушителя. Отличительной чертой данных систем является имитация не только серверов и конечных станций, но и сетевой инфраструктуры, а также автоматизация и централизованное управление. Данные платформы можно считать последним рубежом обороны, т.к. нарушитель уже находится внутри сети. Хотелось бы отметить, что технологии обмана не заменяют существующих систем управления событиями (SIEM-систем), системы защиты конечных станций (endpoint protection platform), а лишь дополняют их.

***Основная часть.*** Систему мониторинга событий информационной безопасности в части технологий обмана нарушителей представляется целесообразным строить на основе таких средств, как ханипоты, они же пассивные ловушки, которые всегда имеют дело с действиями нарушителей. Если говорить о таких системах, как EDR, то они не способны определить, использует ли внутренний инсайдер легитимную учетную запись со злым умыслом или у него есть законное право на доступ к активам. SIEM настроены на обнаружение вредоносной активности с помощью заданных корреляционных правил, которые могут быть недостаточно точными и разрабатываются вручную, что делает этот процесс особенно трудоемким. В то же время это не делает EDR, SIEM и другие системы менее значимыми. Ханипоты в свою очередь способны обнаружить попытку атаки с минимальным количеством ложноположительных срабатываний. Это главное отличие и преимущество данного класса решений. Также следует отметить, что они позволяют настроить мониторинг хакерской активности в тех «средах», где установить другие классы решений (например, EDR) зачастую технически невозможно. В последнее время направление атак нарушителей сконцентрировано больше на нетрадиционных поверхностях IT-атак в таких сферах, как здравоохранение или промышленность, так как используемое оборудование или системы (например, АСУ ТП) не поддерживают подобное ПО. Чтобы размыть поверхность атаки, создается эмуляция программируемых логических контроллеров (ПЛК), медицинского оборудования, банковских систем и т.д., в зависимости от конкретной организации, где применяются ловушки. Столкнувшись с одной из них, злоумышленник не поймет, где настоящие активы, а где приманки. С большой долей вероятности он ошибется, и его активность будет зафиксирована.

Обманные технологии в системе мониторинга могут применяться на 3 уровнях.

1-й уровень – конечных устройств. В данном случае требуется использование приманки, так называемые хлебные крошки. К ним относятся имитация cookies, txt-файл с паролями, кэш браузера с чувствительной информацией – все, что привлекает внимание атакующего.

2-й уровень – сетевой. На данном уровне используются ловушки – ложные цели атаки, замаскированные под такие ресурсы, как серверы, рабочие станции, маршрутизаторы. Некоторые сегодняшние решения позволяют эмулировать банкоматы, медицинское оборудование и IoT.

3-й уровень – интерактивных ловушек FullOS. Они занимают физические IT-ресурсы, как и настоящие пользователи.

Реализуется это следующим образом. Нарушитель, который не обладает данными о сети, в процессе разведки находит приманки и начинает с ними взаимодействовать. Когда его заинтересует определенная база данных, он попытается подключиться к операционной системе и взаимодействовать с ней как с активом, не предполагая, что это эмуляция. Легитимные пользователи не знают о существовании таких ловушек, и им нет смысла к ним подключаться. Следовательно, фиксирование попытки подключения, достоверно свидетельствует о том, что данные действия связаны с действиями нарушителя. Таким образом, одним из главных достоинств таких ловушек является то, что они практически единственный класс средств защиты с нулевым процентом ложноположительных срабатываний, в отличие от систем класса DLP, EDR, AntiAPT и т.п. Данные средства являются очень удобными в плане администрирования, так как любые срабатывания в системе автоматически указывают на попытки вредоносной активности. Система мониторинга событий информационной безопасности на основе ханипотов работает на стадии горизонтального распространения атаки в сети (рисунок 1).

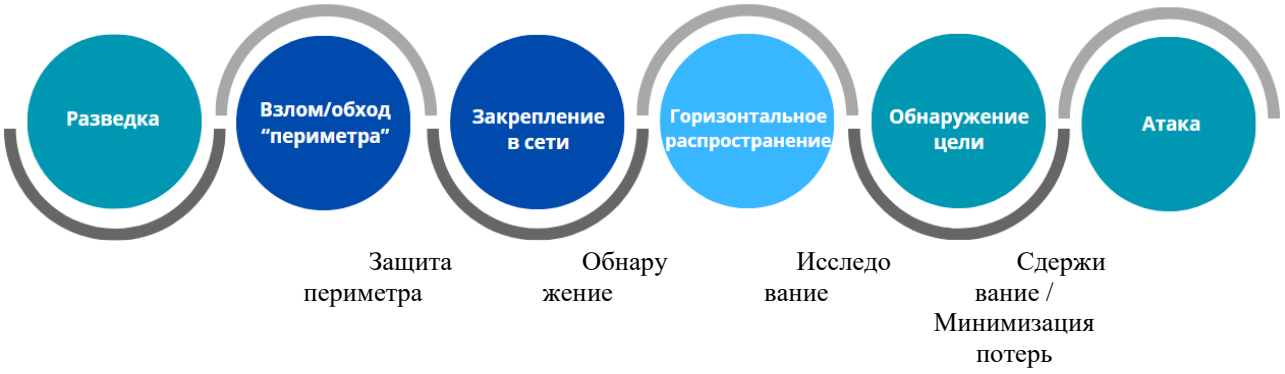



Рисунок 1 – Модель действия нарушителя

Представляется целесообразным применение возможности интеграции с внешними сервисами, например с SIEM. При внедрении ловушек важнейшим этапом для администратора является сбор сведений о том, кто именно и в какую ловушку попался. Администратору необходимо зафиксировать попытку аутентификации с ловушкой. Ханипоты умеют «читать» логи из интегрированных систем о неудачных попытках подключения с подставными учетными данными. В случае с SIEM путем создания правил корреляции событий можно фиксировать факты использования информационных токенов злоумышленником. Это позволит максимально точно и практически мгновенно определить развивающуюся атаку.

Современные системы ханипотов уже значительно продвинулись в развитии по сравнению с их первоначальными версиями, приобрели множество интересных возможностей. Самые первые ловушки могли только эмулировать сервисы, а в настоящее время ханипоты автоматически маскируются под активы, применяемые в каждой конкретной организации. Хороший пример – учетные записи пользователей. В каждой организации есть служба каталогов, в которой зачастую применяется шаблон для формирования имени пользователя для сотрудника. Например, все пользователи домена созданы по шаблону с использованием имени и фамилии. В этом случае будет применяться единый шаблон адреса электронной почты, например с использованием первой буквы имени, точки, фамилии, @ и домена. Система ханипотов анализирует эти паттерны и при

составлении приманок также их придерживается, то есть фейковые пользователи, созданные системой приманок, будут очень похожи на те, что используются в домене компании [2].

***Заключение.*** Ханипоты – один из самых надежных классов решений. Они практически безотказны и помогают предотвратить или остановить атаку в самом начале, минимизируя риски утечки данных и связанные с ними убытки. Они просты в настройке и работают фактически автономно, что делает их подходящими практически любой компании. Таким образом, система мониторинга событий информационной безопасности, построенная на технологии обмана нарушителя с использованием ханипотов, позволит своевременно получить достоверные данные о нахождении нарушителя в информационной сети предприятия, а также экономить финансовые, временные и человеческие ресурсы при технической поддержке и сопровождении данного решения.

### *Список литературы*

*1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.*

*2. CISOCLUB – информационный портал и профессиональное сообщество специалистов по информационной безопасности. https://cisoclub.ru/ [Электронный ресурс]. – Режим доступа : https://cisoclub.ru/hanipoty-zashhishhaem-sistemy-hitrostju/. – Дата доступа : 10.02.2024.*

UDC 004.777

## INFORMATION SECURITY EVENT MONITORING SYSTEM AND TOOLS

*Chagan N.F.*

*gr.267241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Borbotko T.V. – Dr. of Sci. (Tech.), professor at the department of IS*

**Annotation**. The materials of the report consider an information security event monitoring system based on honeypots, designed for timely and accurate detection of an intruder in the organization's information network. Also for use on equipment or systems (for example, automated control systems), where the use of traditional systems such as EDR, AVP, DLP, etc. is not possible.

**Keywords:** monitoring system, Honeypots, DDP

УДК 004.777

## МЕТРИКИ ДЛЯ ОБНАРУЖЕНИЯ DDOS-АТАК

*Шаронова Е.И., магистрант*

*гр. 267241*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Петров С.Н. кандидат технических наук, доцент кафедры защиты информации*

**Аннотация.** В настоящее время актуальные метрики обнаружения DDoS-атак являются неотъемлемой частью защиты сетевой инфраструктуры и помогают обеспечить безопасную и надежную работу систем и сервисов. Они позволяют быстро обнаруживать и блокировать аномальное поведение трафика и предотвращать нарушение работы сети и сервисов.

**Ключевые слова:** DDoS-атака, метрика обнаружения, машинное обучение, мониторинг, сетевой трафик.

***Введение.*** DDoS-атаки, существуя со времени начала массового использования глобальной сети, по-прежнему остаются одной из самых серьёзных угроз для Web-ресурсов, что свидетельствует о необходимости развития средств защиты от этих атак. Грамотно организованная масштабная DDoS-атака в большинстве случаев приводит к значительным финансовым потерям со стороны жертвы. При отсутствии средств обнаружения вторжений ресурс информационной системы тратится на обслуживание DDoS запросов, при этом стоимость использования ресурса многократно возрастает. Такие нападения отличаются простотой организации и высокой эффективностью. Именно эти особенности привлекают к DDoS внимание как специалистов по сетевой безопасности, так и злоумышленников, что обусловливает актуальность исследования DDoS-атак. Метрики обнаружения DDoS-атак являются важными для защиты сетевой инфраструктуры. Это инструменты и метрические показатели, которые помогают идентифицировать и отслеживать аномальное поведение трафика и потенциальные DDoS-атаки. Они служат для установления базовых показателей нормального функционирования сети и обнаружения аномалий, которые могут указывать на возможные атаки. Метрики обнаружения DDoS-атак позволяют предупреждать и реагировать на атаки в реальном времени, повышая уровень безопасности и минимизируя негативные последствия.

***Основная часть.*** Метрики для обнаружения DDoS-атак могут включать следующие аспекты:

1. Трафик: метрики, связанные с объемом и интенсивностью сетевого трафика, могут использоваться для обнаружения аномалий. Например, увеличение входящего или исходящего трафика сверх обычного уровня может указывать на возможную DDoS-атаку.

2. Пропускная способность: метрики, связанные с использованием сетевой пропускной способности, могут быть полезны для обнаружения DDoS-атак. Например, резкое увеличение использования пропускной способности может указывать на DDoS-атаку.

3. Частота запросов: метрики, связанные с частотой поступления запросов на сервер, могут быть полезными для обнаружения DDoS-атак. Например, значительное увеличение количества запросов за короткое время, поступающих с одного или нескольких IP-адресов, может указывать на DDoS-атаку.

4. Распределение IP-адресов: метрики, связанные с распределением IP-адресов, могут помочь в обнаружении DDoS-атак. Например, необычно высокая концентрация запросов с определенных IP-адресов или определенной подсети может указывать на DDoS-атаку.

5. Загрузка ресурсов: метрики, связанные с использованием ресурсов сервера, таких как процессорное время, память и диск, могут быть полезными для обнаружения DDoS-атак. Например, резкое увеличение загрузки ресурсов сверх обычного уровня может указывать на возможную DDoS-атаку.

6. Распределение трафика: метрики, связанные с распределением трафика по портам или протоколам, также могут быть использованы для обнаружения DDoS-атак. Например, необычное увеличение трафика на определенном порту может указывать на DDoS-атаку, нацеленную на этот порт.

Важно отметить, что эти метрики могут быть только основополагающими при обнаружении DDoS-атак, и требуют дополнительной аналитики и контекста для подтверждения наличия атаки. Дополнительно к предыдущим метрикам, можно использовать следующие признаки для обнаружения DDoS-атак:

7. Проверка заголовков пакетов: метрики, связанные с анализом заголовков пакетов могут быть полезными при обнаружении DDoS-атак. Например, проверка значений поля User-Agent или Referer в HTTP-запросах может помочь выявить необычные или подозрительные запросы, связанные с DDoS-атакой.

8. Анализ типов атак: метрики, связанные с анализом типов атак, таких как SYN флуд, UDP флуд или ICMP флуд, могут помочь в обнаружении DDoS-атак. Например, мониторинг аномалий или выявление типичных схем поведения для каждого типа атаки может помочь в их идентификации.

9. Сетевые характеристики: метрики, связанные с расчетом или мониторингом определенных сетевых характеристик, таких как RTT (Round-Trip Time) или TTL (Time-To-Live), могут быть полезны при обнаружении DDoS-атак. Аномалии в таких характеристиках могут указывать на DDoS-атаку.

10. Межсетевая облачность: если ваша сеть использует облачные ресурсы, метрики, связанные с межсетевой облачностью, могут быть полезными для обнаружения DDoS-атак. Облачные провайдеры обычно предоставляют инструменты для отслеживания и мониторинга трафика, что может помочь в обнаружении аномалий и обнаружении DDoS-атак.

11. Машинное обучение и анализ поведения: применение алгоритмов машинного обучения и анализа поведения может помочь выявить аномалии и необычное поведение в сети, что может указывать на DDoS-атаку. Например, обучение модели на основе исторических данных и поведения сети может помочь в обнаружении новых или неизвестных атак.

12. Мониторинг доступности: отслеживание доступности веб-серверов, сервисов или приложений может помочь обнаружить DDoS-атаку. Если вы замечаете необычно высокую нагрузку или снижение доступности во время атаки, это может быть признаком DDoS.

13. Мониторинг сетевого трафика: анализ сетевого трафика может помочь выявить аномалии или необычное поведение, которые могут быть связаны с DDoS-атакой. Можно использовать инструменты для мониторинга сетевого трафика, такие как snort или tcpdump, чтобы обнаружить подозрительный трафик.

14. Анализ логов серверов: мониторинг и анализ логов серверов может помочь обнаружить аномалии в запросах, например, необычно большое количество запросов от одного IP-адреса или необычно высокую загрузку сервера, что может указывать на DDoS-атаку.

15. Мониторинг использования ресурсов: отслеживание использования ресурсов, таких как процессорное время, оперативная память или сетевая пропускная способность, может помочь выявить необычные или аномальные показатели, которые могут указывать на DDoS-атаку.

16. Уровни сигнала и амплитуда: мониторинг уровней сигнала или амплитуды в сети или на хостах может помочь обнаружить аномалии или сигналы высокой мощности, которые могут быть связаны с DDoS-атакой.

Выбор конкретных метрик должен основываться на требованиях и особенностях исследуемой сети и системы. Разнообразие и комплексный подход в мониторинге и анализе помогут повысить эффективность обнаружения DDoS-атак.

На рисунке 1 представлена простая схема, которая иллюстрирует основные компоненты и процессы обнаружения DDoS-атак:

1. Мониторинг сети и серверов: Мониторинг сетевых устройств, серверов и приложений позволяет отслеживать общую производительность и доступность системы. Это включает мониторинг пропускной способности сети, загрузку процессора, использование памяти, логи серверов и другие ресурсы.

2. Обнаружение аномалий: Использование ряда алгоритмов обнаружения аномалий позволяет выявить необычные или аномальные показатели, которые могут указывать на DDoS-атаку. Это могут быть алгоритмы машинного обучения, статистические методы или правила обнаружения аномалий.

3. Анализ трафика и логов: Сбор и анализ сетевого трафика и логов серверов помогает выявить необычное поведение или аномалии, которые могут быть связаны с DDoS-атакой. Это включает анализ сетевого трафика с помощью инструментов, таких как snort или tcpdump, а также анализ логов серверов для выявления подозрительных запросов или необычно высокой нагрузки.

4. Блокировка подозрительного трафика: Если обнаружена DDoS-атака, можно принять

меры для блокировки или ограничения подозрительного трафика. Это может включать фильтрацию IP-адресов, установку правил файрвола или использование специализированных DDoS-защитных устройств или услуг.

5. Реакция на инциденты: В случае обнаружения DDoS-атаки важно иметь четкий план реакции на инциденты. Это включает обмен информацией с провайдером услуг Интернета (ISP) или поставщиком услуг в области безопасности, уведомление персонала и принятие мер для минимизации воздействия атаки на систему.

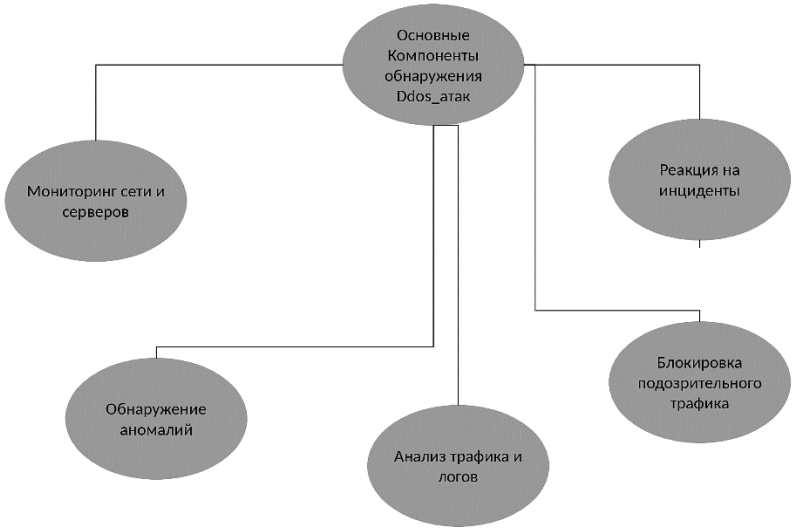



Рисунок 1 – Основные компоненты и процессы обнаружения DDoS-атак

Эта схема предоставляет общий обзор процессов обнаружения DDoS-атаки и не охватывает все возможные методы и технологии. Реальная реализация может включать дополнительные шаги и инструменты в зависимости от специфических потребностей и требований системы.

***Заключение.*** В заключение, метрики обнаружения DDoS-атак являются важным инструментом для защиты сетей и ресурсов от масштабных кибератак. Они позволяют идентифицировать и анализировать аномалии в трафике, соединениях, типах трафика, пакетах и потоках, а также использовании системных ресурсов.

При правильном настройке и использовании метрик обнаружения DDoS-атак, организации и предприятия могут оперативно реагировать на подозрительное поведение и предотвращать серьезные последствия атаки, такие как отказ в обслуживании и потеря бизнесовой продуктивности.

Однако, важно отметить, что метрики обнаружения DDoS-атак не являются единственным и полным решением для защиты от атак. Они должны быть использованы в сочетании с другими мерами безопасности, такими как межсетевые экраны, прокси-серверы, IDS/IPS системы и т.д., для обеспечения полного и надежного обнаружения и защиты от DDoS-атак.

Всегда важно обновлять и совершенствовать метрики обнаружения DDoS-атак, чтобы быть в курсе последних методов и инструментов, используемых злоумышленниками. Также, необходимо проводить регулярное обучение персонала и повышать осведомленность о современных угрозах DDoS-атак, а также оптимизировать и настраивать соответствующие инструменты для эффективного и надежного обнаружения атак.

В целом, метрики обнаружения DDoS-атак являются важным компонентом в общей системе защиты от DDoS-атак, и их использование может помочь улучшить безопасность сетей и ресурсов компаний.

***Список литературы***

1. *Miralda-Espina, R., Baras, JS., Detection capabilities of popular DDoS mitigation systems: A modern evaluation. IEEE International Conference on Communications (ICC), 2018.*
2. *Темный, А.Б., Проблема защиты от атак DDoS на основе анализа сетевых пакетов. Информатика и системы управления, 2014.*
3. *Померанцев, А.Б., Морозов, В.И., Классификация DDoS-атак и архитектура системы их обнаружения на основе SVM. Наукоемкие технологии в образовании, 2011*
4. *. Кудряшов, И.В., Методы обнаружения и предотвращения DDoS-атак./ Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2017.-76с.*

UDC 004.777

## METRICS FOR DETECTING DDOS ATTACKS

*Sharonova E.I,*

*gr. 267241*

*Belarusian State University of Informatics and Radioelectronics,*

*г. Minsk, Republic of Belarus*

*Supervisor: Petrov S.N. Candidate of Technical Sciences, Associate Professor of the Department of Information Protection.*

**Annotation**. Nowadays actual metrics of DDoS-attack detection are an integral part of network infrastructure protection and help to ensure safe and reliable operation of systems and services. They allow to quickly detect and block anomalous traffic behavior and prevent disruption of network and services.

**Keywords:** DDoS attack, detection metrics, machine learning, monitoring, network traffic.

УДК 537.87:53.085.345

## АНАЛИЗ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ С ГЕОМЕТРИЧЕСКИ НЕОДНОРОДНОЙ ПОВЕРХНОСТЬЮ

*Щукина А.А., Скрыт О.Н., Кравченко Е.Д.*

*гр.261402*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Саванович С.Э. – ассистент кафедры ЗИ*

**Аннотация.** В работе приведен обзор основных характеристик экранов электромагнитного излучения с геометрически неоднородной поверхностью и способов их формирования. Установлено, что диапазон рабочих частот таких экранов определяется высотой и формой неоднородностей, сформированных на их поверхности. Показана перспективность применения конструкций экранов, выполненных в виде полусфер на основе углеродосодержащих компонентов, для решения различных задач, в том числе противодействия утечки информации по электромагнитному каналу.

**Ключевые слова:** электромагнитное излучение, электромагнитный канал, экран, геометрически неоднородная поверхность, полусфера, углерод, пирамида, поглотитель электромагнитных волн, радиопоглощающий материал.

***Введение.*** Увеличение количества технических средств, функционирование которых

связано с использованием электромагнитного излучения (ЭМИ) радиочастотного диапазона, или созданием побочного ЭМИ, остро ставит проблему снижения его уровня для решения возникающих в связи с этим задач защиты биологических объектов, обеспечения электромагнитной совместимости радиоэлектронной аппаратуры, а также противодействия утечки информации по электромагнитному каналу [1].

Одним из способов решения указанных задач является экранирование, основанное на поглощении большей части излучений материалами, входящими в состав экрана ЭМИ, при минимальном их отражении за счет наличия в экранирующем материале резистивных, диэлектрических и магнитных потерь в его рабочем диапазоне частот [2].

***Основная часть.***

Устранение остаточного отражения ЭМИ обеспечивается формированием на поверхности экранов геометрических неоднородностей в виде выпуклостей, выступов, впадин или микронеровностей. Достижение требуемых значений коэффициентов отражения и передачи ЭМИ таких конструкций обеспечивается оптимизацией геометрии и структуры экранов применительно к диапазонам частот их применения.

В работе [3] предложен поглотитель ЭМИ, на поверхности которого сформированы неоднородности в виде полусфер высотой 1,0–1,5 см, сформированных на основе углесодержащих компонентов (рисунок 1). Добавление порошкообразного активированного кокосового угля при изготовлении таких полусфер приводит к снижению значений коэффициентов передачи ЭМИ поглотителя до уровня в –21 дБ, отражения до –10 дБ на частотах 6…7 ГГц, что позволяет рекомендовать их для защиты средств вычислительной техники от помех.

Формирование на поверхности экрана ЭМИ, выполненного на основе смеси бетона с порошкообразными шунгитом и тауритом [4], пирамид высотой 30 мм приводит к снижению его значений коэффициента отражения в пределах –10…–20 дБ в диапазоне частот 3…12 ГГц (рисунок 2). Для аналогичного экрана ЭМИ, изготовленного на основе смеси бетона и таурита, значения коэффициента отражения варьируются в пределах –9,8…–16,3 дБ в рассматриваемом диапазоне частот. Введение таких экранов ЭМИ в структуру наружных стен зданий позволяет снизить уровень излучений, сформированных средствами технической разведки и внести помехи в их работу. При этом способность пирамидальных экранов ЭМИ подавлять мощность излучений в диапазоне частот 3...12 ГГц обеспечивает защиту персонала, находящихся внутри таких построек, от негативных электромагнитных воздействий.

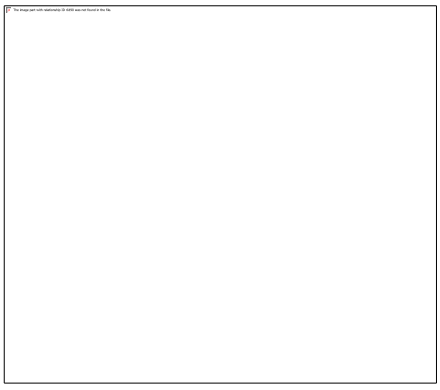


Рисунок 1 – Фрагмент экрана ЭМИ

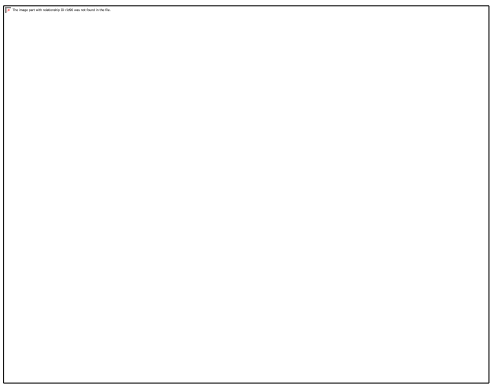


Рисунок 2 – Фрагмент экрана ЭМИ

Поглотитель электромагнитных волн (ПЭВ) для безэховых камер и экранированных помещений [5] представляет собой трехслойную конструкцию, состоящую из

диэлектрического материала клиновидного типа, пластин из магний-цинкового феррита и металлической подложки (рисунок 3). Применение ПЭВ обеспечивает исключение излучений в пределах камеры (помещения), а также позволяет снизить значения коэффициента отражения ЭМИ по мощности в пределах –12…–40 дБ от стен камер (помещений) в диапазоне частот 30…37,5 ГГц за счет изменения его высоты от 250 до 350 мм.

ПЭВ «ТОРА» [6] пирамидального типа, разработанный в НИИ ПФП БГУ, выполненный в виде панелей из эластичного пенополиуретана с углеродным наполнителем (рисунок 4), предназначен для покрытия внутренних поверхностей и оборудования рабочих мест в безэховых камерах. Варьирование высоты поглотителя от 75 до 640 мм обеспечивает снижение его значений коэффициента отражения ЭМИ в пределах –15…–50 дБ в диапазоне частот 0,12…37,5 ГГц.

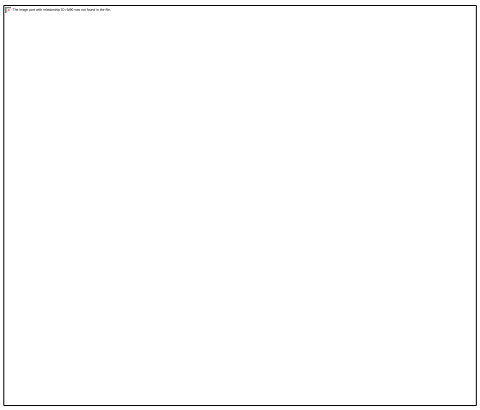


Рисунок 3 – ПЭВ

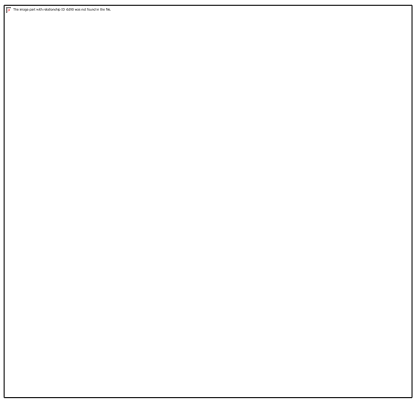


Рисунок 4 – ПЭВ «ТОРА»

Варьирование высоты радиопоглощающего материала (РПМ) «Мох-П» (рисунок 5) в пределах 70…850 мм, выполненного в виде наполненных нанодисперсным углеродным наполнителем пенополиуретановых блоков пирамидальной формы, обеспечивает снижение его значений коэффициента отражения ЭМИ в пределах –3…–60 дБ соответственно в диапазоне частот 0,1…60,0 ГГц [7].

Изменение высоты РПМ «ТЕСАРТ» [8], выполненного в виде диэлектрических панелей пирамидального из эластичного пенополиуретана с углеродным наполнителем, от 165 до 880 мм обеспечивает снижение его значений коэффициента отражения ЭМИ в пределах –20…–50 дБ соответственно в диапазоне частот 0,2…100,0 ГГц. (рисунок 6).

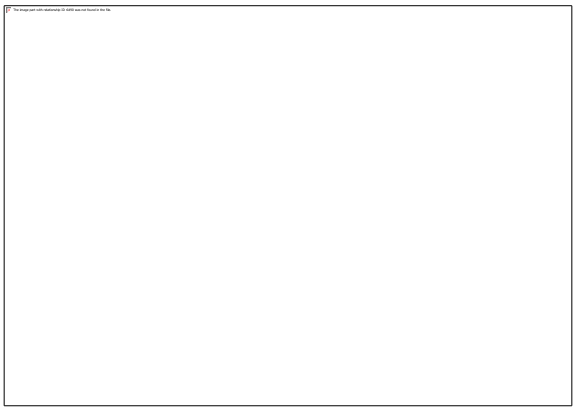


Рисунок 5 – РПМ «Мох–П»

Рисунок 6 – РПМ «ТЕСАРТ»

Варьирование высоты ПЭВ «Универсал-Дельта» [9], выполненного в виде пирамидальных контейнеров заполненных радиопоглощающей композицией с использованием углеродного волокна, в пределах 200…580 мм, обеспечивает снижение его значений коэффициента отражения ЭМИ с –10 до –50 дБ в диапазоне частот 0,1…100,0 ГГц, что показывает актуальность его применения для облицовки безэховых камер, имитирующих свободное пространство при испытаниях радиотехнических комплексов и антенных систем различного назначения; помещений, используемых для проведения аттестационных работ по сертификации технических средств на электромагнитную совместимость, а также обеспечения защиты обслуживающего персонала от воздействия излучений (рисунок 7).

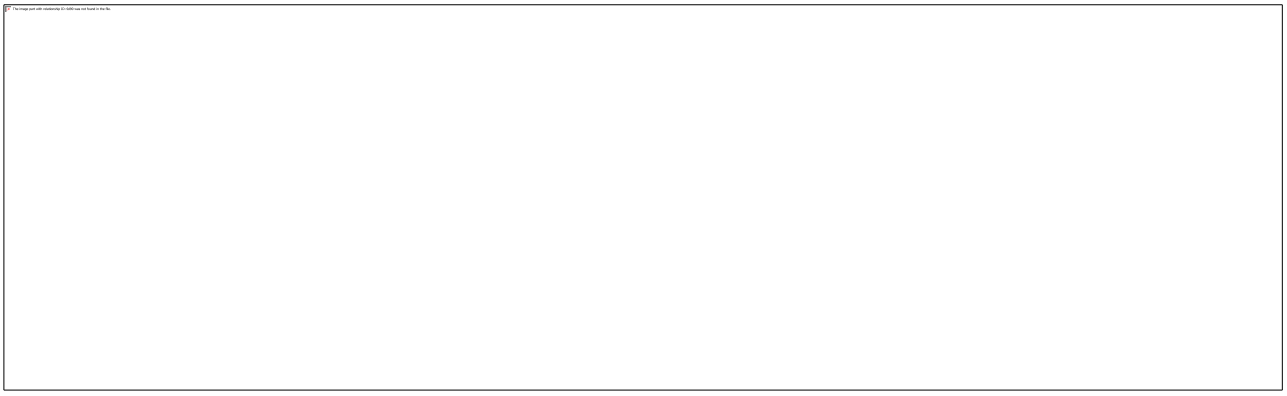


Рисунок 7 – Варианты выполнения ПЭВ «Универсал-Дельта»

***Заключение.*** В результате анализа основных характеристик конструкций экранов ЭМИ с геометрически неоднородными поверхностями установлено, что снижение их значений коэффициентов отражения в пределах –3…–50 дБ в диапазоне частот 0,1…100,0 ГГц обеспечивается за счет формирования на их поверхности пирамид клиновидного типа, выполненных на основе углеродосодержащих компонентов, высотой от 70 до 850 мм. Показано, что такие конструкции экранов ЭМИ применяются для формирования безэховых камер или экранирования помещений в виду их значительных габаритных размеров. Таким образом определено, что увеличение высоты полусфер, сформированных на основе активированного кокосового угля, до 15 мм позволит расширить диапазон рабочих частот поглотителей ЭМИ от 6…7 до 2…100 ГГц при значениях их коэффициента отражения не ниже –10 дБ.

## *Список литературы*

*1. Электромагнитное излучение [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%B8%D1%82%D0%BD%D0%BE%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5. – Дата доступа: 09.03.2024*

*2. Электромагнитное экранирование [Электронный ресурс]. – Режим доступа: https://faradey.ru/electromagnetic-shielding/. – Дата доступа: 09.03.2024*

*3. УГЛЕРОДОСОДЕРЖАЩИЕ ПОГЛОТИТЕЛИ ДЛЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ ПОМЕХ (59 научная конференция аспирантов, магистрантов и студентов БГУИР, 2023 г.) [Электронный ресурс]. – Режим доступа: https://libeldoc.bsuir.by/bitstream/123456789/51909/1/Bordilovskaya_Uglerodosoderjaschie.pdf. – Дата доступа: 11.03.2024*

*4. ВЛИЯНИЕ ЭКРАНОВ С ГЕОМЕТРИЧЕСКИ НЕОДНОРОДНОЙ ПОВЕРХНОСТЬЮ НА ОСЛАБЛЕНИЕ МОЩНОСТИ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ [Электронный ресурс]. – Режим доступа https://libeldoc.bsuir.by/bitstream/123456789/1846/1/Boyprav_Vliyaniye.PDF. – Дата доступа: 11.03.2024*

*5. Сверхширокодиапазонный поглотитель электромагнитных волн для безэховых камер и экранированных помещений [Электронный ресурс]. – Режим доступа: https://patents.google.com/patent/RU2453953C1/ru?oq=RU+2453953+C1+. – Дата доступа: 17.03.2024*

*6. Поглотитель электромагнитных волн «ТОРА» [Электронный ресурс]. – Режим доступа: https://niipfp.bsu.by/index.php/oborud/tora. –*

*Дата доступа: 18.03.2024*
*7. Радиопоглощающий материал типа «МОХ-П» [Электронный ресурс]. – Режим доступа: https://radiostrim.ru/product/moh/. – Дата доступа: 18.03.2024*
*8. Радиопоглощающий материал ООО НПК «ТЕСАРТ» [Электронный ресурс]. – Режим доступа: https://tesart.ru/products/item/amp/. – Дата доступа: 18.03.2024*
*9. ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНЫХ ВОЛН «УНИВЕРСАЛ - ДЕЛЬТА» [Электронный ресурс]. – Режим доступа: https://rpm-delta.com/products.– Дата доступа: 18.03.2024*

UDC 537.87:53.085.345

## ANALYSIS OF ELECTROMAGNETIC SCREENS WITH A GEOMETRICALLY INHOMOGENEOUS SURFACE

*Shchukina A.A., Skryt O.N., Kravchenko E.D.*

*gr.261402*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Savanovich S.E. – assistant of the department of information security*

**Annotation**. The article provides an overview of the main characteristics of electromagnetic radiation screens with geometrically non-uniform surfaces and methods of their formation. It has been established that the operating frequency range of such screens is determined by the height and shape of the non-uniformities formed on their surface. The potential of using screen structures, in the form of hemispheres made of carbon-containing components to address various tasks, including counteracting information leakage through the electromagnetic channel, is demonstrated.

**Keywords:** electromagnetic radiation, electromagnetic channel, screen, geometrically non-uniform surface, hemisphere, carbon, pyramid, electromagnetic wave absorber, radio-absorbing material.

# СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

УДК 004.777

## МЕТОДОЛОГИЯ ВЫБОРА ЭФФЕКТИВНОГО АЛГОРИТМА ПОИСКА

*Довгулевич Е.В., Шука В.С.*

*гр.267041, гр. 263001*
*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Шевчук О.Г. – канд. техн. наук, доцент кафедры ИКТ*

**Аннотация.** В данном тезисе предлагается анализ процесса выбора алгоритма поиска, включая рассмотрение основных критериев, влияющих на это решение, а также предоставление рекомендаций по оптимальному подходу, учитывая разнообразие задач и требований современных информационных систем.

**Ключевые слова:** алгоритм поиска, критерии поиска, матрица сравнения алгоритмов

***Введение.*** Одной из важнейших процедур обработки информации является поиск. Алгоритмы поиска успешно применяются в различных сферах современных информационных систем (ИС), включая анализ данных, биоинформатику, машинное обучение, криптографию, робототехнику, игровую индустрию и др.

Выбор эффективного алгоритма поиска играет ключевую роль в обеспечении производительности и функциональности ИС. Существует ряд актуальных проблем, с которыми сталкиваются специалисты, включающие в себя учет различных требований задач, высокая производительность с большими объемами данных, а также необходимость адаптации к изменяющимся условиям.

***Основная часть.*** Существует множество различных алгоритмов поиска, имеющих свои преимущества и недостатки [1]. Рассмотрим основные классы алгоритмов, представляющие собой фундаментальные подходы к решению задач поиска.

Линейный. Один из наиболее простых методов, при котором элементы последовательно проверяются на соответствие критерию поиска, однако, эффективность снижается с увеличением объема данных. Применяется в случаях, когда структура данных не предоставляет дополнительной информации о распределении элементов.

Бинарный. Метод для упорядоченных данных, при котором диапазон поиска сокращается в два раза на каждом шаге, обеспечивая значительный прирост производительности, особенно в случае больших объемов данных.

Хеширование. Алгоритмы хеширования преобразуют входные данные в уникальные значения, обеспечивая быстрый доступ к ним. Однако эффективность зависит от качества хеш-функции и уровня коллизий. Идеально подходит для поиска в базах данных и словарях.

Алгоритмы поиска в графах. Методы для решения задач поиска в сетевых и графовых структурах данных, таких как алгоритм Дейкстры, алгоритмы поиска в ширину (BFS) или в глубину (DFS) [2].

Алгоритмы машинного обучения. Поиск информации в собранных данных на этапе моделирования производится математической функцией. Обучение зависит от типа используемой модели [3].

Выбор подходящего алгоритма для конкретных требований – это важная задача, и существует несколько методов для определения, какой алгоритм может быть наиболее оптимальным. Однако, универсального метода нет, а эффективность каждого зависит от конкретной задачи, данных и условий применения. Необходимо предварительно систематизировать задачи по их характеристикам. Разработка методологии систематизации задач позволит более точно определить, какие критерии следует учитывать при выборе алгоритма. Рекомендованы следующие критерии:

1. Эффективность по времени и ресурсам. Скорость выполнения является главным фактором при обработке запросов в реальном времени. Ресурсоемкость актуальна в условиях ограниченных вычислительных мощностей или при работе в облачных сервисах.

2. Работа с большими объемами данных. Алгоритмы должны быть спроектированы таким образом, чтобы обеспечивать высокую скорость поиска и обработки больших объемов данных. Эффективность алгоритма может зависеть от того, каким образом данные организованы в памяти. Существенно улучшить производительность позволит использование оптимальных структур данных, таких как деревья или хеш-таблицы.

3. Устойчивость к изменениям в данных. Способность динамически адаптироваться к изменениям входных данных, включая добавление или удаление элементов. Особенно актуально в системах, в которых данные поступают или изменяются часто.

Определение алгоритма в рамках каждой категории задач производится созданием матрицы сравнения, в которой алгоритмы оцениваются по различным критериям. Матрица приоритетов (матрица критериев) – это инструмент, с помощью которого можно ранжировать по степени

важности данные и информацию [4]. Критерии не ограниченны перечисленными выше, к примеру, критериями могут являться простота реализации, специфические требования к задаче и другие. Оценки могут быть представлены в числовой форме или использоваться качественные оценки, в зависимости от конкретных требований. Матрица представляет собой таблицу, в которой в строках указываются алгоритмы, а в столбцах – критерии сравнения. Пример матрицы сравнения алгоритмов приведен в таблице 1.

Таблица 1 – Матрица сравнения алгоритмов поиска.

| Класс алгоритмов | Основные характеристики | Эффективность по времени | Работа с большими объемами данных | Устойчивость к изменениям в данных |
|---|---|---|---|---|
| Линейный поиск | Простота реализации | Низкая Линейная | Затраты растут экспоненциально с увеличением данных | Неустойчив |
| Бинарный поиск | Требуется отсортированный массив | Логарифмическая | Не подходят для неупорядоченных данных | Требует пересортировки данных при изменениях |
| Хеширование | Быстрый доступ к данным | Константная | Зависит от хеш-функции, возможны коллизии | Устойчив |
| Алгоритмы поиска в графах | Требует оптимизации и адаптации | Зависит от конкретной задачи и характеристик графа (количество вершин и рёбер) | Некоторые алгоритмы становятся вычислительно сложными с увеличением размера графа | Зависит от конкретного алгоритма. DFS и BFS -устойчивы |
| Алгоритмы машинного обучения | Высокая точность, но требуется обучение | Зависит от модели и данных | Подходят для обработки больших объемов данных | Устойчив |

Следующим этапом методологии анализа алгоритмов предполагается создание методов количественной оценки критериев для каждого алгоритма. Эти методы могут включать в себя разработку метрик. Позволяет выразить оценки по каждому критерию в числовой форме, что упрощает анализ и сравнение алгоритмов, обеспечивает систематизацию подхода к этому процессу.

Применим методологию выбора алгоритма на примере конкретной задачи: анализ данных в области медицинского исследования. Характеристики задачи: объем данных – большой (медицинские записи, изображения и результаты исследований); временные ограничения – разные, в зависимости от конкретной задачи; структура данных – разнообразная (текст, изображения, числовые данные).

Систематизация задачи по поиску в базе данных медицинских записей включает в себя разделение задачи на подзадачи в соответствии с характеристиками данных (текстовые, изображения, числовые данные) и определение ключевых критериев для каждой подзадачи. Таким образом, можно выделить три подзадачи. Подзадача 1: поиск в текстовых медицинских записях. Значимо точное нахождение информации, учитывая особенности медицинской терминологии и семантики. Подзадача 2: распознавание и поиск в медицинских изображениях, в снимках с медицинских устройств (например, в рентгеновских снимках). Подзадача 3: поиск в числовых данных, таких как результаты лабораторных исследований. Каждая подзадача подчиняется своим уникальным требованиям, и выбор алгоритмов для решения этих подзадач должен быть согласован с соответствующими ключевыми критериями для обеспечения оптимальной эффективности системы поиска в базе данных медицинских записей.

Создадим матрицу сравнения основных алгоритмов (представлена в таблице 2) в базе данных медицинских записей, учитывая следующие критерии: точность, возможность работы с различными типами данных и устойчивость к изменениям в данных.

Таблица 2 – Матрица сравнения алгоритмов в базе данных медицинских записей.

| Алгоритм поиска | Точность | Возможность работы с различными типами данных | Устойчивость к изменениям данных |
|---|---|---|---|
| Линейный | ++ | ++++ | --- |
| Бинарный | +++ | +++ | --- |
| Хеширование | ++++ | ++++ | -- |
| Алгоритмы поиска в графах | +++ | ++++ | ++++ |
| Машинное обучение | ++++ | ++++ | ++++ |

Объяснение обозначений:

++++ : очень высокий уровень соответствия критерию;

+++ : высокий уровень соответствия критерию;

++ : умеренный уровень соответствия критерию;

--- : низкий уровень соответствия критерию;

-- : очень низкий уровень соответствия критерию.

Оценив различные алгоритмы поиска с учетом требований задачи в базе данных медицинских записей, резюмируем:

- не рекомендованы линейный и бинарный поиски. Первый, т.к. менее эффективен для больших объемов данных, второй – по причине того, что требует упорядоченных данных;
- предпочтительны в использовании: для текстовых данных и изображений –машинное обучение, для числовых данных – алгоритмы в графах, при хорошей хеш-функции и ограниченном объеме данных – хеширование.

***Заключение.*** Методология выбора алгоритма является критическим элементом в области информационных систем и приложений, где эффективность поиска напрямую влияет на общую производительность. Анализ различных критериев выбора, таких как эффективность по времени и ресурсам, работа с большими объемами данных и устойчивость к изменениям, позволил выделить важные аспекты, которые следует учитывать при выборе алгоритма. Методология, предложенная в тезисе, предоставляет систематизированный и комплексный подход к этому процессу. Применение методологии на практике, через рассмотрение конкретной задачи и сравнение результатов выбранных алгоритмов, демонстрирует ее эффективность в различных областях, и подтверждает необходимость индивидуального подхода к выбору алгоритмов в зависимости от контекста задачи.

### *Список литературы*

1. *Алгоритмы поиска данных [Электронный ресурс]. – Режим доступа : https://top-technologies.ru/ru/article/view?id=24620 - Дата доступа : 13.02.2024.*

2. *Базовые алгоритмы на графах [Электронный ресурс]. – Режим доступа : https://habr.com/ru/companies/timeweb/articles/751762/- Дата доступа : 13.02.2024.*

3. *Машинное обучение как инструмент анализа данных [Электронный ресурс]. – Режим доступа : https://rep.bntu.by/bitstream/handle/data/110567/304-309.pdf?sequence=1&isAllowed=y - Дата доступа : 16.02.2024.*

4. *Матрица приоритетов [Электронный ресурс]. – Режим доступа : https://www.kpms.ru/Implement/Qms_Prioritization_Matrix.htm. - Дата доступа : 19.02.2024.*

UDC 004.777

## METHODOLOGY FOR SELECTING AN EFFECTIVE SEARCH ALGORITHM

*Dovgulevich E.V.*

*gr. 267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Shevchuk O.G. - Kand. techn. sciences, associate professor of the department of ICT*

**Annotation**. This report provides an analysis of the process of selecting a search algorithm, including consideration of the main criteria influencing this decision, as well as recommendations for an optimal approach, taking into account the diversity of tasks and requirements of modern information systems.

**Keywords:** search algorithm, search criteria, algorithm comparison matrix

# APPLICATION OF SMART WATCH-BASED DATA SET ANALYSIS IN MEDICAL INTERNET OF THINGS

*Wu Haoran*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Вишняков Владимир Анатольевич. – Doctor of Technical Sciences, BSUIR Technology*

**Abstract:** In the field of medical physical therapy, the identification of human body activities is of great significance. Smartwatches are equipped with powerful sensors that provide a convenient platform for acquiring data sets to implement and deploy mobile motion-based behavioral biometrics. This study explores various activities of daily living and evaluates motion-based biometrics using smartwatches. The results show good results, indicating the applicability of these techniques in identifying human activities. And implemented through LSTM-CNN.

**Keywords:** medical physio therapy ,smart watches, sensors, biometric recognition, activity recognition, LSTM-CNN.

***Introduction.*** Identifying and verifying an individual's physical condition and human body activities are crucial in the medical field. With advancing technology, smart watches have emerged as powerful tools in healthcare[1]. These watches combine intelligent sensors, data analysis, and real-time communication functions, offering new possibilities for medical monitoring and management.

Smart watches play a vital role in health monitoring by incorporating features such as heart rate sensors, exercise trackers, and sleep monitoring functions. These functions enable real-time monitoring of users' physiological indicators[2]. By collecting and analyzing this data, smart watches provide health status assessments and recommendations, facilitating better health management. Additionally, smart watches can monitor essential parameters like blood pressure and blood oxygen saturation, issuing early warnings and health risk alerts. The gyroscope sensor in smart watches accurately recognizes daily human activities, ensuring timely acquisition of important activity information.

Gyroscopes in smart watches also prove valuable for sports monitoring and fitness management[3]. By recognizing human body postures and movements, smart watches can accurately track activities like walking, running, and cycling. They record key indicators such as exercise duration, distance, and speed, offering personalized fitness suggestions. This benefits individuals seeking health management and sports enthusiasts, enhancing their understanding of exercise status and progress.

Furthermore, the activity recognition function of smart watch gyroscopes plays a significant role in chronic disease management and recovery. For instance, in stroke rehabilitation, smart watches can recognize hand movements and postures, monitor rehabilitation training progress and effectiveness, and provide real-time feedback and guidance. This personalized rehabilitation monitoring and auxiliary training improve patients' rehabilitation outcomes and quality of life. Smart watch gyroscopes can also identify and monitor various human activities, contributing to behavior analysis and management. By integrating activity recognition data with physiological parameters like heart rate and blood pressure, smart watches can provide more accurate health assessments and personalized treatment recommendations. The broad application prospects of smart watch gyroscopes in smart medical care offer accurate and personalized

services for personal health. Further technological advancements will expand the application potential, introducing more innovation and convenience to smart medical care.

The study described in this article evaluates the use of accelerometer and gyroscope sensors on commercially available smart watches for biometric authentication and identification across a wide range of daily life activities. Different models are introduced for each activity. This study is unique as it assesses the biometric potential of smartwatches across numerous daily life activities. Assessing a diverse set of activities is crucial for generating effective data sets for medical human activity analysis.

***Data Collection and Transformation.*** This section outlines the process of data collection and transformation. The study encompasses a variety of regular physical activities, most of which are performed daily. Physical activity is defined as specific identifiable actions with associated start and end times. While some activities (e.g., eating pasta) may not be practical for on-demand biometric systems, they are useful when subjects perform their normal daily activities. A continuous biometric system operating during normal activities proves valuable. However, activities like palming and writing are easily performed on demand. Section 6 discusses the overall biometric effectiveness of the campaign, considering its usefulness if executed on demand.The raw sensing data consists of time series sensor data stored in separate files. Each file contains data from one sensor (accelerometer or gyroscope) on one device (smartphone or smartwatch) for one subject. Therefore, there are four files associated with each subject, and the sensor data from these files can be linked through timestamp information collected during the same time period. Each sensor measurement is recorded on a separate line in the data file, following the format: subject-id (identifying the test subject), activity (code identifying the physical activity performed), timestamp (Unix time when the sensor value was recorded), x, y, and z values (sensor values for x, y, and z spatial axes). The format of recorded sensor data remains the same, regardless of whether it comes from an accelerometer or gyroscope on a smartphone or smartwatch. The accelerometer measures linear acceleration (in meters/second), while the gyroscope measures angular velocity (in rad/second). The raw sensor data used in this study is publicly available from the UCI repository as the WISDM Human Activity Recognition and Biometric Recognition Dataset[4]. Figure 1 illustrates a graphical representation of smartphone accelerometer data for walking and jogging activities, where the y-axis corresponds to the vertical direction and exhibits the largest magnitude. Jogging activities are more frequent than walking activities, as one would expect.

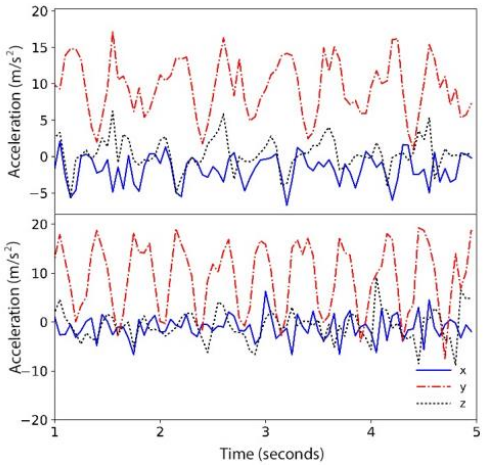


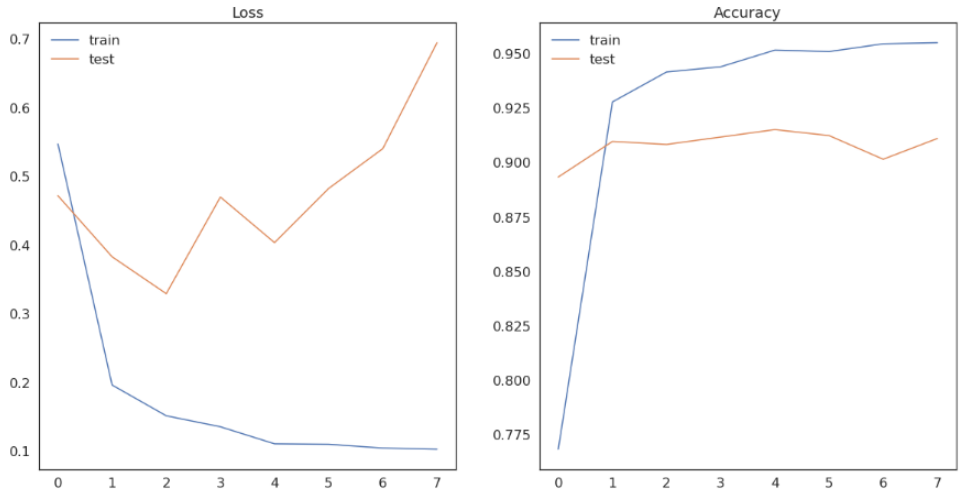

Figure 1 Plot of three-axis accelerometer data for smartphone walking activity (top) and jogging activity (bottom)

***Classification algorithm.*** Three classification algorithms were used to generate the authentication and recognition models evaluated in the cost study: k-neighbors, decision trees, and random forests. We use implementations of these algorithms in Python's scikit-learn module, an open source library for data mining and analysis. Default parameters are used unless otherwise noted.

***Evaluation process.*** In this study, a data set named "UCI_HAR_Dataset" was added and divided into a training set and a test set, where X_train and X_test contain two-dimensional tensors of the number of time steps (n_timesteps) and the number of features (n_features) , while y_train and y_test contain one-

dimensional tensors of the number of outputs (n_outputs). These parameters are used to build the model.

***Model building.*** Define an LSTM model and use the model to run a complete pipeline, including data loading, model training, visualization results and other steps. Train the model on the training data using the




given model and grid search results, and evaluate the model performance on the test data. To get the best hyperparameters, get the best epochs and batches from the grid search results. The detection results obtained are shown in Figure 2.

Then build the CNN model and use adam as the optimizer. Find the loss rate and accuracy of the run. Finally, the CNN-LSTM neural network is constructed. After training the model, the loss rate and accuracy curves are constructed as shown in Figure 3. Three deep learning models are defined using different neural networks for training (LSTM, CNN, LSTM-CNN). Among them, the training process of each model includes techniques such as parameter optimization and early stopping to avoid overfitting.

Figure 2 Training data loss and accuracy

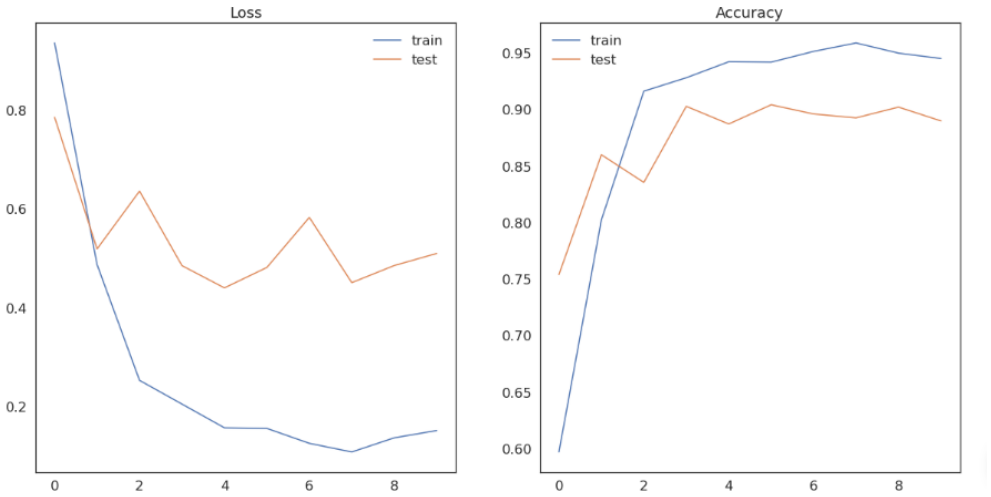



Figure 3 LSTM-CNN mode training data loss and accuracy

***Conclusion.*** By analyzing the training results, we can clearly observe the ROC curve of the model, and the accuracy of the training results is still close to 100%. This study constructed a dataset for medical activity analysis by collecting and analyzing sensor data from smart watches. For the medical field, forming valid data sets is very important for accurate analysis and evaluation of human activities. Through smart watch data collection, we can obtain a large number of sample data of different activities, which provides strong support for medical activity analysis and research. From the overall research point of

view,Human activity detection applications based on smart watches have broad application prospects in the medical field. The gyroscope sensor of smart watches can accurately identify and monitor human body activities, providing important support for smart medical care. With the continuous development of technology, smart watches will play an increasingly important role in medical monitoring, rehabilitation and health management, and provide more accurate and personalized services for personal health.

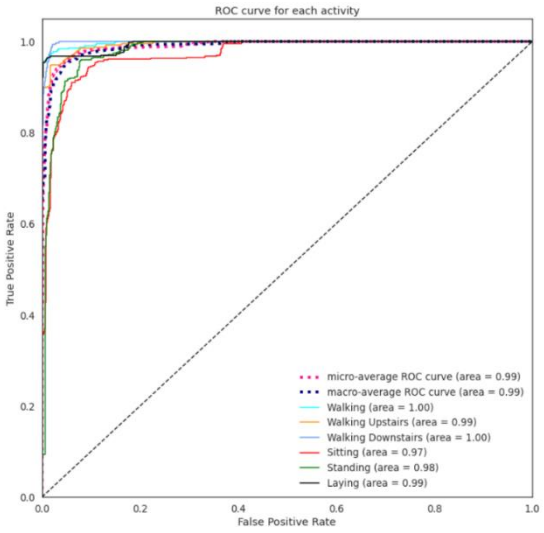



Figure 4 mode ROC curve for each activity

## *REFERENCES*

*1. Lin Yue, Jia Guoying, Sun Junwei, etc. Design research of a smart watch [J]. Technology and Innovation, 2023, (14): 49-51. DOI: 10.15913/j.cnki.kjycx.2023.14.014.*

*2. Cao Shumin. Human action recognition and interaction based on smart wearable devices[D]. University of Science and Technology of China, 2020.DOI:10.27517/d.cnki.gzkju.2020.001029.*

*3. Pan Jiayao. Research and implementation of intelligent control technology for wearable devices based on inertial sensors [J]. Information Technology and Informatization, 2018, (11): 58-61.*

*4. Weiss ,Gary. (2019). WISDM Smartphone and Smartwatch Activity and Biometrics Dataset . UCI Machine Learning Repository. https://doi.org/10.24432/C5HK59.*

UDC 620.9:.658.42

## EXTRACTION OF IRIS IMAGES FOR IT DIAGNOSIS

*Zhao Yi'an*

*gr. 267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Vishniakou U.A. – Dr. of Sci. (Tech.), Professor at the department of ICT*

**Annotation**. Iris diagnostics is a method based on the recognition of its features to determine the state of human health, genetic information and other relevant characteristics. One of the most distinctive features of the iris is the constrictor located in

its middle, surrounding the pupil. This is important for diagnosis, because its shape, size and other characteristics can reveal a person's physical health..

**Keywords:** recognition of patterns, iris diagnosis, constrictor

***Introduction.*** In pattern recognition, a method that uses basic element structures (primitives) and the structural relationships between primitives to describe patterns and complete the recognition and classification process is called structural pattern recognition [1]. Through a large number of observations of existing iris images, it can be found that there are boundary areas with drastic changes in grayscale in the iris part of the image, and most of these areas with drastic changes in grayscale exist in a few pixels.

***Crimp wheel extraction based on structural pattern*.** The study found that the most drastic changes in grayscale The part is around the inner edge of the iris image, which is a boundary in the iris image. However, compared with the pupil boundary edge, the grayscale of the shrink wheel shows a slowly changing trend within a certain pixel range. Compared with the non-border area There are also many pixels with large grayscale changes. As shown in Figure 1, the pupil area is between the 40th pixel and the 95th pixel, and the curling wheel area is between the 20th and 40th pixels. The curve in the figure Reflects the change in grayscale around the constriction wheel and around the pupil. In order to better find the boundary point, this paper approximately defines the center point within the boundary range as the boundary point of the image within the range, that is, using the basic element structure to count the image range with the largest change in the curling wheel texture in the iris image, and at the same time defining Two modes: border mode and non-border mode, and use the sliding window method to count the number of times each of the two modes appears in the window, find the window containing the curling wheel texture through the rules of the number of occurrences of each mode, and complete the curling Round extraction. [2]

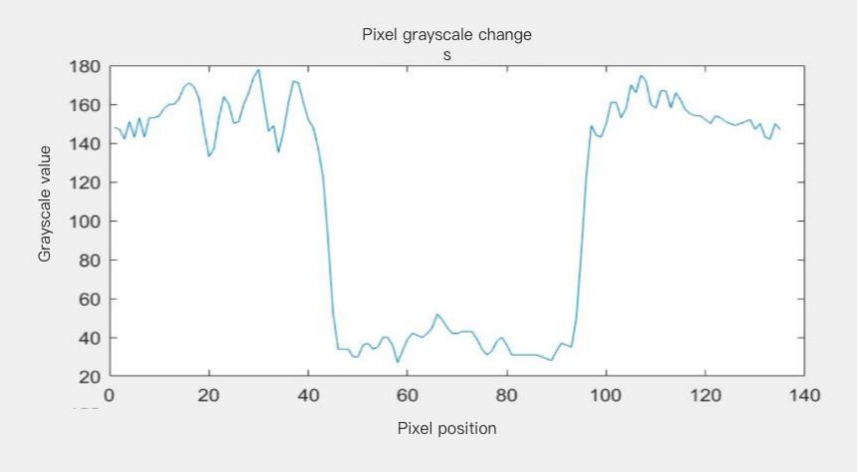



Figure 1 – Boundary area grayscale changes

***Iris preprocessin.*** Due to the unique structural characteristics of the human eye, iris extraction is easily affected by lighting, collection angle, environment and other factors. In order to correct the elastic deformation problem caused by this and eliminate the impact of translation and rotation on iris feature extraction, it is necessary to collect the iris features. The image is preprocessed, including iris positioning and normalization. The specific extraction process is shown in Figure 2.

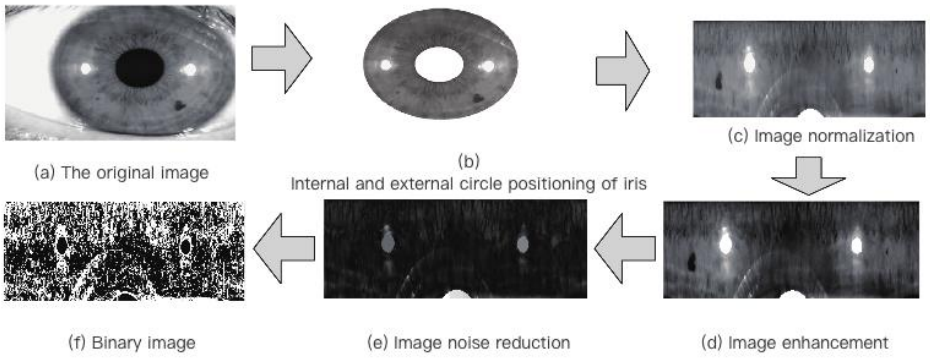



Figure 2 – Extraction process

***Define primitives and patterns.*** The primitive in this article is a basic unit used to describe the degree of grayscale change within a certain pixel range. Through the observation of the curling wheel part in the normalized iris image, combined with the analysis of multiple experimental results, This article defines a primitive as five consecutive pixels in the vertical direction, consisting of a central pixel and two edge pixels at the top and bottom.

In order to accurately describe the grayscale difference between each edge pixel and the center pixel in the primitive, this paper records the grayscale difference between the edge pixels 1, 2, 3, 4 and the center pixel as $q_i$=(i=1,2,3, 4), and define the threshold as a=9, b=4, and define the relationship between the absolute value of the grayscale difference between each edge pixel and the center pixel and the threshold to define the primitive mode, recorded as P{$p_1$, $p_2$, $p_3$, $p_4$}. It stipulates three modes of 0, 1, and 2 to represent $p_i$ = (i = 1, 2, 3, 4), which represents the relationship between the absolute value of qi and the two thresholds. If the absolute value of qi is greater than a, then $p_i$ =0. If the absolute value of $q_i$ is less than b, then $p_i$=1 is recorded. If the absolute value of qi is between a and b, $p_i$=2 is recorded. When there is a large change in grayscale between the edge pixels and the center pixels, the image at this time is mostly in the boundary area, and $p_i$=0 is often present at this time. Therefore, P {0,0,0,0} can be defined as Boundary mode; Similarly, when the edge pixels have almost no change compared with the center pixels, the image at this time is mostly in the non-border area, that is, $p_i$=1, and the non-edge mode can be defined as P {1,1,1,1}. It would be too simple to consider just using the above two modes as the judgment conditions for boundary areas and non-boundary areas. In order to find out the boundary area of the crimping wheel as completely as possible, this article adds several more types that often appear in boundary areas and non-boundary areas. The mode of the non-boundary area is used to determine whether the image is at the boundary, that is, let P {2,0,0,0}, P {0,2,0,0}, P {0,0,2,0}, P {0,0,0,2} to jointly serve as the boundary determination mode, let P{2,1,1,1}, P{1,2,1,1}, P{1,1,2,1}, P{1,1,1,2} to jointly define the non-boundary mode. [3]

***Crimping wheel extraction implementation.*** Select a 15*15 window and slide it along the direction of Figure 3 on the normalized image. In the same window, if the boundary mode appears more often, the non-border mode will appear less often, and vice versa. In order to achieve an accurate description, the boundary point on a certain column is determined by using the quotient of the number of occurrences of the boundary pattern within the window and the number of occurrences of the non-border pattern within the window, and the quotient is recorded as B. [4]

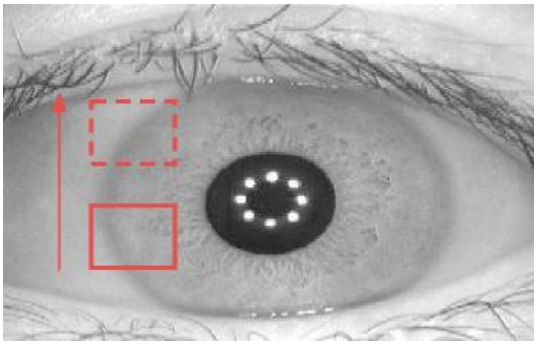


Figure 3 – Window sliding direction

The extraction steps of the crimping wheel are as follows, and the extraction flow chart is shown in Figure 4.

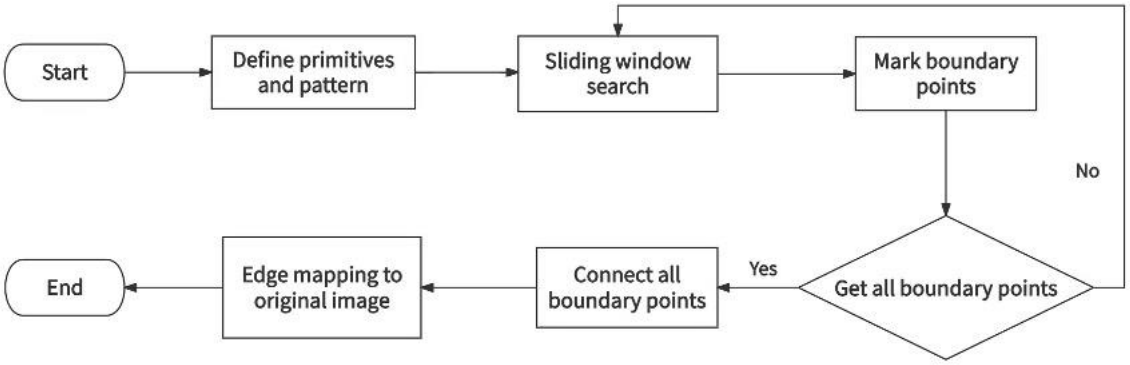



Figure 4 – Curled round extraction flow chart

(1) Use a 15×15 window to slide on the normalized image in the direction, count all B, record the maximum value, and save the center point of the window where the maximum value of the quotient is located, which is the boundary point of the column.

(2) Move the window one pixel to the right and repeat the above steps until the image is traversed and all boundary points are found.

(3) Connect all the boundary points and map them to the original image, which is the calibrated shrinking wheel.

***Experimental results and analysis.*** The results of the curling wheel extraction are shown in Figure 5. It can be seen from the figure that the curling wheel outline extracted by this algorithm covers the entire curling wheel area, basically outlines the outline shape of the curling wheel, and is not affected by the eyelashes above the iris. interference.

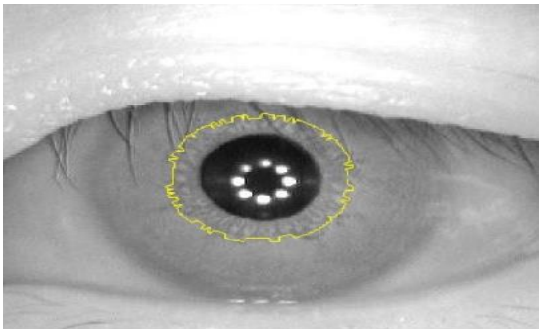


Figure 5 – Curled round extraction

***Conclusion.*** As a combination of traditional Chinese medicine visual examination and western medicine iridology, iris diagnostics plays a huge role in the field of human sub-health evaluation and disease prevention. It has gradually been valued by various countries in the world. As a subject that has attracted widespread attention from the world, iris diagnostics has developed a An iris-assisted diagnosis system based on this discipline has become an inevitable trend. Crimping wheel extraction is a key step in the iris diagnosis process. Deep learning algorithms can quickly and automatically identify and extract key features such as crimping wheels from a large number of iris images, significantly improving the speed of analysis and batch processing. The use of deep learning to extract crimped wheels in iris diagnosis is not only a technological advancement, but its practical significance and application value involve many aspects such as medical health, safety certification, and technological innovation. It is an important step in the current and future field of artificial intelligence. one of the research directions.

## *References*

*1. Xin Guodong, Wang Wei. Research on iris constriction wheel extraction method. Computer Engineering and Design, 2008, 29(9): 2290-2292.*

*2. Yuan Weiqi, Ye Bingwen, Sun Xiao, Teng Hai. Iris curling wheel detection method based on gradient extreme value. Computer Engineering, 2014,40(2):162-165.*

*3. Dong Feixia. Eye syndrome differentiation and iris diagnosis. Journal of Changchun University of Traditional Chinese Medicine, 2010, 26(1):8-9.*

*4. Gao Yuan. Research on feature extraction method of iris texture. Shenyang University of Technology, 2015.*

УДК 620.9:.658.42

## ИЗВЛЕЧЕНИЕ ИЗОБРАЖЕНИЙ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА ДЛЯ ИТ-ДИАГНОСТИКИ

*Чжао Иань*

*Гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ*

**Аннотация.** Диагностика по радужной оболочке глаза это метод, основанный на распознавании ее особенностей для определения состояния здоровья человека, генетической информации и других соответствующих характеристик. Одной из наиболее отличительных особенностей радужной оболочки является констриктор, расположенный в ее середине, окружающий зрачок. Это важно для ИТ-диагностики, поскольку ее форма, размер и другие характеристики могут выявить физическое здоровье человека.

**Ключевые слова**: распознавание закономерностей, диагностика радужной оболочки, констриктор.

UDC 620.9:.658.45

## GRAD-CAM VISUALIZATION MODEL FOR LUNG DISEASE DIAGNOSIS

*He Tao*

*gr. 267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Vishniakou U.A. – Dr. of Sci. (Tech.), Professor at the department of ICT*

**Annotation**. When applying the diagnosis of lung diseases in the Internet of Things networks,

the Grand-Cam model can be used to provide assistance to doctors by imaging lungs and diagnosing diseases. By creating heatmaps of attention, Cad-Cam can visualize areas in an image. Doctors can observe heat maps to make decisions about the disease and ensure that the model focuses on areas related to specific lung diseases, increasing the accuracy and reliability of diagnosis.

**Keywords:** Cad-Cam, solution model, heat map of attention, diagnosis of lung diseases.

***Introduction.*** Grad-Cam is a technique for interpretable deep learning model decisions that can be applied in areas such as computer vision and natural language processing [1]. These techniques can help us understand the model's focus on the input and the basis for its decision-making, rather than just treating the deep learning model as a black box. In the application of diagnosing lung diseases in IoT networks, Grad-Cam can be used to provide interpretability of model decisions, helping doctors and researchers understand the model's focus on lung images and the basis for disease diagnosis. By generating attention heatmaps, Grad-Cam can visualize the model's areas of attention in an image, thereby revealing how much the model pays attention to different areas in the image. Specifically, when applying Grad-Cam to the diagnosis of lung diseases, you first need to train a deep learning model that can classify or locate diseases based on lung images. Grad-Cam technology is then used to generate a heat map that shows the model's areas of interest in the lung image. These areas of concern may provide doctors with important clues in diagnosing lung disease [2]. By observing the resulting heatmaps, physicians can better understand the model's decision-making process and verify that the model is focusing on areas associated with specific lung diseases. This can help doctors verify the reliability and accuracy of the model and provide additional support and evidence to make more accurate diagnoses.

***Principle of Grad-Cam.*** Grad-Cam computes the gradient of the predicted class score relative to the activations in the last convolutional layer [3]. These gradients represent the importance of each activation map for predicting a specific class. The general process is shown in the figure. This method does not change the two-point structure of the model and does not require retraining the model. It only needs to obtain the gradient of the last stage and back-transmit it.

In order to obtain the category discriminant map Grad-Cam, it is recorded as the class positioning map $L^c_{Grad-CAM} \in R^{u \times v}$ with height $h$, width $w$, and category $c$. First, use $y^c$ (logits before softmax) to calculate the gradient of class $c$, and define the activation value of the feature map as $A^k$[4]. The gradients of these backflows are globally average pooled over the width and height dimensions (indexed by $i$ and $j$ respectively) to obtain neuron importance weights $a^c_k$:

$$a^c_k = \frac{1}{Z} \sum_i \sum_j \frac{\partial y^c}{\partial A^k_{ij}} \quad (1)$$

Among them, $Z$ represents the number of pixels of the feature map, and $Aij$ represents the (pixel value of $i, j$ position) of the k-th feature map.

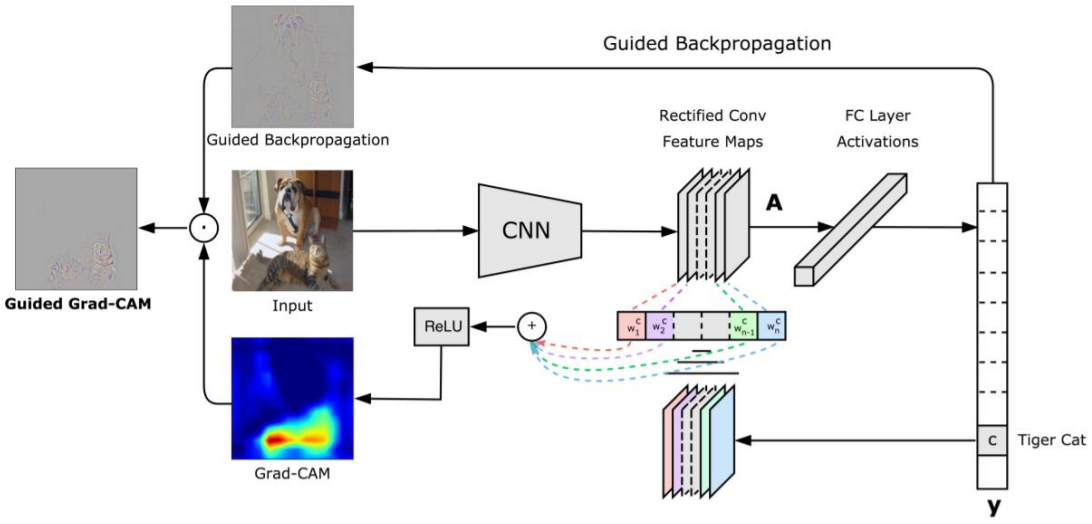



Figure 1 – Grad-Cam calculation structure diagram

While calculating $a_k^c$, the gradients are backpropagated with respect to the activations. The exact calculation equals the successive matrix products of the weight matrix and the gradient with respect to the activation function until the final convolutional layer to which the gradients are propagated. Therefore, this weight $a_k^c$ represents a partial linearization of the deep network downstream of A and captures the "importance" of feature map k for target category $c$ [5]. Calculate the product of the weight matrix and gradient of the activation function, and finally perform a weighted sum and output it after activation through ReLU:

$$L_{Grad-CAM}^{C} = ReLU(\sum_k a_k^c A^k) \quad (2)$$

It is worth noting that the rough heat map output after weighting here is consistent with the feature size of the selected convolution layer, and then the heat map is obtained through the ReLU operation. The purpose is to only consider pixels that have a positive impact on category $c$.

***Breath sound feature optimization based on Grad-Cam.*** The model in this article uses the Mel spectrogram features of breath sounds as network input [6]. The extraction process includes: input audio data in wav format, resample the audio at 16kHz frequency, set the window function to Haining window, window length 25ms, step size 10ms, perform short-time Fourier transform on the audio to obtain the spectrogram, use 64-order The Mel filter group calculates the Mel spectrum on the spectrogram obtained in the previous step, calculates log(mel-spectrum+0.01) to obtain a stable Mel spectrum, and frames the frame for 0.96s per second, in which the frames are not stacked, each frame contains 64 Mel bands, and each second contains a total of 96 frames. The model in this article uses the Mel spectrogram features of breath sounds as network input. Figure 2 shows an example of a breath sound Mel spectrum.

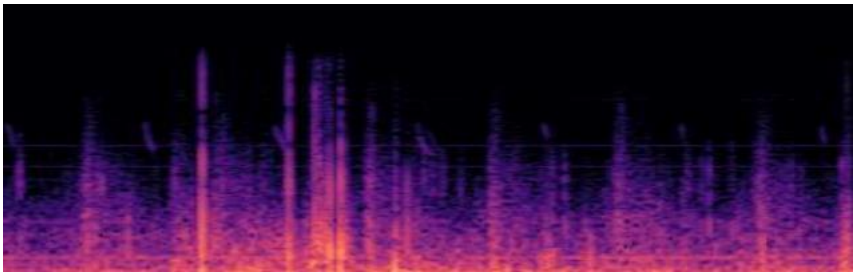


Figure 2 – Breathing sound Mel spectrum sample

The features used in the basic model of this article were selected in the frequency range of 100-2000Hz. After preliminary experiments, when Grad-Cam was used to analyze the samples classified by the basic model, significant low-heat areas were found in the high-frequency areas of their spectra. As shown in Figure 3, the high-heat area in the figure represents the part that is more important to the classification model, and the low-heat area represents the part that is relatively unimportant for target prediction and classification.

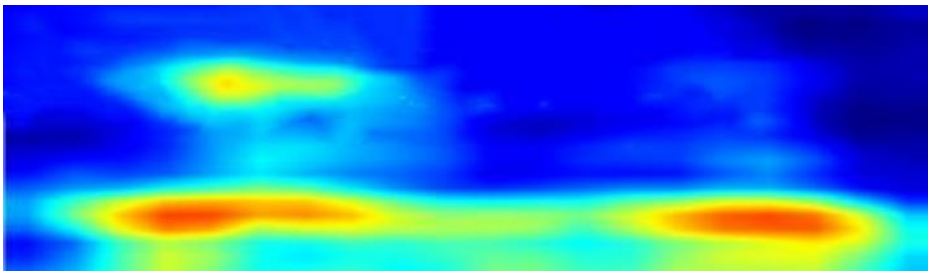


Figure 3 – Grad-Cam analyzes raw samples

The model's focus on the input image is mainly concentrated in the lower half of the input image, indicating that some areas within the audio high-frequency range cannot provide good features for the model's classification judgment [7]. Further analysis reveals that many samples have blank areas, especially in the frequency range 1500-2000Hz. This may have an adverse effect on the network performance of this article. In order to optimize the model effect, this article selectively cuts blank lines from the high-frequency areas of these spectra. The purpose of this is to ensure that the network focuses on the area of interest and reduces interference in irrelevant areas, thereby improving model performance [8]. This article chooses to cut out the area above the audio Mel frequency of 1500Hz. After pruning out the high-frequency regions, the network starts paying more attention to the lower half of the spectrogram, as shown in Figure 4.

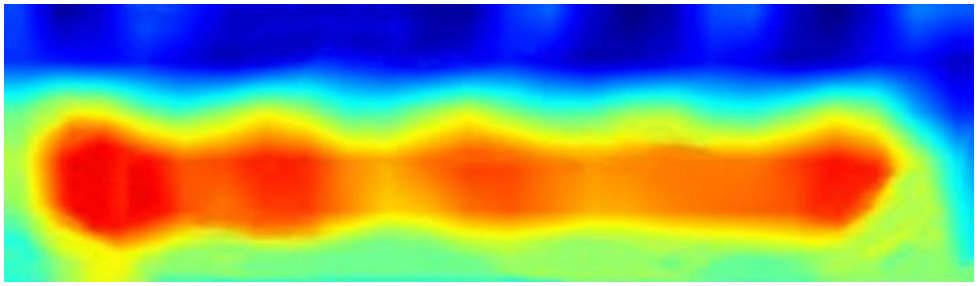


Figure 4 – Grad-Cam analyzes optimized samples

***Conclusion.*** GRAD COM helps explain why the deep learning model focuses on breathing sounds and lung images and is the basis for disease diagnosis. The generated heat map of attention shows how much the model pays attention to different regions, thus providing detailed information about the disease. This visualization method helps to verify the reliability and accuracy of the model and increases the reliability of the diagnosis. By observing the heat map, the doctor can better make a decision and check whether the model focuses on areas related to the sound of breathing and lung diseases.

## ***References***

*1. Zhou, Bolei, et al. Learning deep features for discriminative localization // Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.*

*2. Selvaraju, Ramprasaath R., et al. Grad-Cam: Visual explanations from deep networks via gradient-based localization // Proceedings of the IEEE International Conference on Computer Vision. 2017.*

*3. M. D. Zeiler, R. Fergu. Visualizing and understanding convolutional networks // European conference on computer vision. Springer, 2014, pp. 818–833.*

*4. Ba L J, Caruana R. Do Deep Nets Really Need to be Deep?. Advances in Neural Information Processing Systems, 2013:2654-2662.*

*5. Bastani O, Kim C, Bastani H. Interpreting Blackbox Models via Model Extraction. 2017.*

*6. Che Z, Purushotham S, Khemani R, et al. Distilling knowledge from deep networks with applications to healthcare domain[J]. arXiv preprint arXiv:1512.03542, 2015.*

*7. Xiao J, Ye H, He X, et al. Attentional Factorization Machines: Learning the Weight of Feature Interactions via Attention Networks. 2017:3119-3125.*

*8. Liu Q, Zeng Y, Mokhosi R, et al. STAMP: short-term attention/memory priority model for session-based recommendation // Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. ACM, 2018: 1831-1839.*

УДК 620.9:.658.45

## МОДЕЛЬ ВИЗУАЛИЗАЦИИ GRAD-CAM ДЛЯ ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ ЛЕГКИХ

*Не Тао*

*Гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ*

**Аннотация.** При применении диагностики заболеваний легких в сетях Интернета вещей модель Grad-Cam может использоваться для обеспечения помощи врачам путем изображениях легких и диагностики заболеваний. Создавая тепловые карты внимания, Grad-Cam может визуализировать области на изображении. Врачи могут наблюдать за тепловыми картами, чтобы принять решений о заболевании и убедиться, что модель фокусируется на областях, связанных с конкретными заболеваниями легких, повышая точность и достоверность диагностики.

**Ключевые слова**: Grad-Cam, модель решения, тепловая карта внимания, диагностика заболеваний легких.

УДК 004.777

## Машинное зрение. Перспективы оценки 3D-позы человека.

*Типун А.Ф.*

*гр.267041*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Хацкевич О.А. – кандидат технических наук, доцент кафедры ИКТ*

**Аннотация.** В материалах доклада рассматривается оценка возможностей и перспективы применения технологии распознавания позы человека роботом. Так же описаны основные проблемные вопросы с которыми придётся столкнуться осваивая данную технологию.

**Ключевые слова:** машинное зрение, поза человека, 3D-пространство, моделирование.

### *Введение.*

Актуальность проекта определяется тем фактом, что трехмерное представление позы предоставляет дополнительную информацию о глубине по сравнению с двухмерным представлением позы, трехмерная оценка позы человека обеспечивает более широкое применение.

Оценка позы человека обычно рассматривается как задача прогнозирования положения сочлененных суставов человеческого тела на основе изображения или последовательности изображений этого человека. Благодаря широкому спектру потенциальных применений оценка позы человека является фундаментальным и активным направлением исследований в области компьютерного зрения. Благодаря мощным методам глубокого обучения и недавно собранным крупномасштабным наборам данных оценка позы человека продолжает добиваться больших успехов, особенно на 2D-изображениях.

***Основная часть.***

**1. Перспективы и возможности**

Чтобы лучше понять использование 3D-оценки позы человека, приведем примеры открывающихся реальных возможностей:

***Взаимодействие человека с компьютером.*** Робот сможет лучше служить и помогать пользователям, если сможет понимать трехмерные позы, действия и эмоции людей. Например, робот может предпринять своевременные действия, когда обнаружит 3D-позу человека, склонного к падению. Более того, люди могут играть в игры, используя свои позы и жесты с помощью сенсоров.

***Автономное вождение.*** Беспилотные автомобили должны принимать решения, чтобы избежать столкновения с пешеходами, поэтому понимание позы, движения и намерений пешехода очень важно

***Биомеханика.*** Поза и движения человека могут указывать на состояние здоровья человека. Таким образом, методы трехмерной оценки позы можно использовать для создания системы коррекции сидячей позы для мониторинга состояния пользователей.

***Анализ спортивных результатов***. Автоматическое извлечение 3D-поз из видео может помочь в дальнейшем анализе результатов спортсменов и обеспечить немедленную обратную связь для их улучшения

***Психология***. Трехмерные позы человеческого тела также могут раскрывать психическое состояние людей, а эмоции можно даже распознать по позам

***Примерка и мода***. В последние годы покупки в Интернете становятся все более популярными, особенно в отношении модной одежды. Пользователи могут увидеть, как они выглядят при ношении определенного предмета одежды в Интернете в виртуальной системе примерки, основанной на трехмерной оценке позы

**2. Трехмерное моделирование человеческого тела**:

Как правило, структура человеческого тела очень сложна, и в разных методах используются разные модели, основанные на их конкретных соображениях. Тем не менее, наиболее часто используемыми моделями являются модели скелета и формы. Кроме того, новая оценка позы представляет собой поверхностное представление под названием DensePose, ее стоит упомянуть в связи с расширением существующего представления позы.

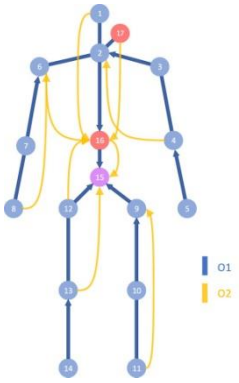



Рисунок 1 – Представление скелета человека по методу DensePose

Скелет человеческого с корневым суставом 15, O1 (синий): относительно первого порядка и O2 (оранжевый): относительно родителей второго порядка в иерархии кинематического скелета.

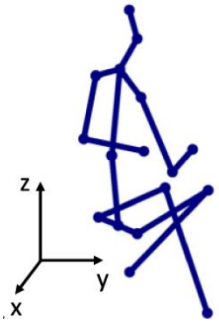



Рисунок 2 – Представление скелета человека в 3D-пространстве

**3. Проблемы**.

В 3D-оценке в отличие от 2D-оценки позы человека основные проблемы включают в себя вариации поз тела, сложный фон, разнообразный внешний вид одежды и окклюзии. Трехмерная оценка позы человека сталкивается с дополнительными проблемами, включая отсутствие реальных наборов трехмерных данных, неоднозначность глубины, огромный спрос на обширную информацию о позе (например, сдвиги и вращения), большое пространство состояний поиска для каждого сустава.

***Заключение.*** Использование вышеописанной технологии позволит улучшить «диалог» между «машиной» и человеком в его естественной среде обитания, будь то плотно застроенный город с колоссальным дорожным трафиком, будь то безжизненная пустыня или неизведанное дно Марианской впадины.

И без того автоматизированные процессы можно полностью освободить от участия человека, обезопасить их.

***Список литературы***

*1. Toshev, A. DeepPose: Human Pose Estimation via Deep Neural Networks / A. Toshev, C. Szegedy // 2014 IEEE Conf. Comput. Vis. Pattern Recognit. – 2014. – C. 1653-1660.*

*2. Benjamin Sapp. MODEC: Multimodal Decomposable Models for Human Pose Estimation / Benjamin Sapp, B. Taskar // CVPR. – 2013.*

UDC 004.777

## Machine vision. Prospects for evaluating a person's 3D pose.

*Tipun A.F.*

*gr.267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*
*Khatskevich L.P. – D.Ph.. of Sci. (Tech.), associate professor at the department of IKS*

**Annotation**. The materials of the report consider the assessment of the possibilities and prospects for the use of human pose recognition technology by a robot. The main problematic issues that you will have to face while mastering this technology are also described.

**Keywords:** machine vision, human posture, 3D space, modeling

UDC 004.021

## APPLICATION OF BLOCKCHAIN IN ELECTRONIC HEALTHCARE RECORD

*Gao Yalu*

*gr.267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*
*Tsviatkou Viktar, head of the department of infocommunication technologies*

**Annotation.** Blockchain's decentralized and immutable nature provides a secure and transparent platform for data exchange, guaranteeing data integrity, privacy, and security. This essay endeavors to delve into the potential of blockchain technology in mitigating the issues confronting the healthcare system, with a focus on Electronic Health Record (EHR).

**Keywords:** BlockChain, Decentralized, Immutable, EHR

***Introduction.*** Given the accumulation of significant personal data[1], it is imperative to establish dependable storage and sharing mechanisms to safeguard patient privacy. Traditional medical data management systems typically rely on centralized servers to construct large-scale site systems or centralized relational database systems, Blockchain, an open distributed ledger based on a peer-to-peer network and consensus algorithm, inherently offers solutions to these issues[2].

***Framework Structure of Blockchain.*** The framework and structure of blockchain can be divided into six layers (figure1): Data layer is where the actual data is stored on the blockchain. It consists of blocks of data that are linked together in a chain. Each block contains a set of transactions, and each transaction contains data that is relevant to the blockchain network. Network layer is responsible for the communication between nodes on the blockchain network. It ensures that data is transmitted securely and efficiently between nodes. The network layer also handles tasks such as peer discovery, routing, and synchronization. Consensus layer is responsible for reaching agreement among nodes on the blockchain network about the validity of transactions and the state of the blockchain[3]. It ensures that all nodes on the network have a consistent view of the blockchain and that no single node can manipulate the blockchain. Contract layer is responsible for providing incentives to nodes on the blockchain network to participate in the network and perform tasks such as validating transactions and maintaining the blockchain. It typically involves the use of cryptocurrencies or tokens as rewards for participating in the network. Application layer is where applications and services are built on top of the blockchain network. It includes user interfaces, APIs, and other tools that allow users to interact

with the blockchain network and access its features.

These layers are intricately interconnected and collaborate to guarantee the security, efficiency, and dependability of the blockchain network. The data layer serves as the bedrock of the blockchain, while the network layer ensures the secure and efficient transmission of data. The consensus layer ensures a uniform perspective of the blockchain across all network nodes, while the incentive layer motivates nodes to engage in network activities. The contract layer facilitates the execution of smart contracts, while the application layer furnishes users with an interface to engage with the blockchain network.

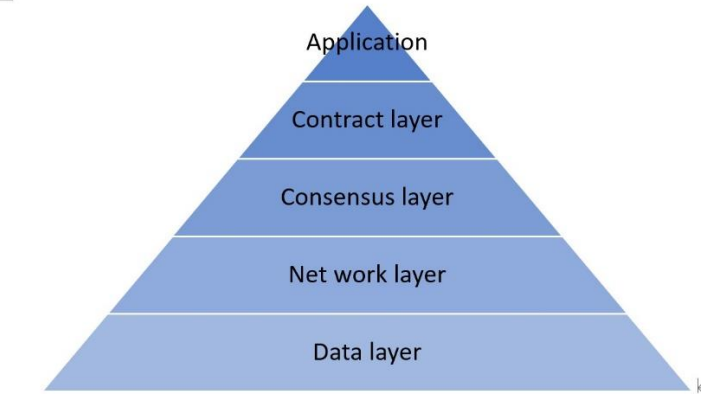



Figure 1 - Structure of Blockchain

***Transaction Process.*** Patient: When a patient visits a hospital, they first register on the hospital server. Upon registration, the hospital server assigns a unique identifier to the patient, equivalent to a medical card. The patient keeps this identifier confidential and presents it during visits. The doctor generates electronic medical records and keywords for the patient, encrypting them using the patient's public key[4]. If the patient seeks treatment at another hospital and the doctor needs access to the patient's medical history, the patient generates a search trapdoor and uploads it to the alliance chain. After running the search algorithm on the alliance chain, the nodes send the encrypted medical records to the patient, who can then decrypt them.

Doctor: Each hospital has a local server and several client devices operated by doctors. When a patient visits, the doctor generates a pseudonym, encrypted electronic medical records, encrypted keywords, and evidence. The doctor uploads the encrypted medical records to the hospital server and the hash value of the medical records, along with the encrypted keywords and evidence, to the private chain. A new transaction is generated and broadcasted. Other nodes on the private chain validate the transaction, and if successful, a new block is added to the private chain.

Data User: When a third-party institution or individual (referred to as a data user) other than the hospital and patient accesses patient data, they require authorization from the patient. The patient generates a search trapdoor and uploads it to the alliance chain. The nodes on the alliance chain perform a search, and when the corresponding patient cipher is found, the nodes act as proxies to generate proxy re-encrypted ciphertexts for the data user. Finally, the data user can decrypt the ciphertext using their private key.

Hospital Server: After the doctor treats the patient and generates electronic medical records, the hospital server extracts the private chain block identifier, patient pseudonym, and keyword index to construct a new transaction on the alliance chain. Other nodes on the alliance chain validate the transaction, and if successful, a new block is added to the alliance chain as shown in Figure 2.

Private Chain: The doctor uploads the hash value of the encrypted medical records and the

keyword index constructed from encrypted keywords and evidence to the private chain, generating a new transaction. Nodes on the private chain validate the transaction. The hospital server extracts the private chain block identifier, patient pseudonym, and keyword index to construct a new transaction on the alliance chain. During the data retrieval phase, if the search is successful, the nodes on the alliance chain extract the secure index from the block to obtain the private chain block identifier. Using the private chain block identifier, the nodes on the alliance chain can retrieve the hash value of the medical record ciphertext.

Alliance Chain: During the search process, when the nodes on the alliance chain receive the trapdoor sent by the patient, they run the search algorithm. If the search is successful, the nodes extract the secure index from the block to obtain the private chain block identifier. Using the private chain block identifier, the nodes on the alliance chain retrieve the hash value of the medical record ciphertext and send it back to the hospital server. The hospital server compares the hash value with the one it has. If they match, the medical record ciphertext is sent to the nodes on the alliance chain, which then return it to the patient. When a third-party data user accesses the patient's electronic medical record, the nodes on the alliance chain act as proxies to generate proxy re-encrypted keys, which are used to perform proxy re-encryption on the ciphertext of the electronic medical record before sending it to the third-party user. System Model Diagram as shown in Figure 2.

.

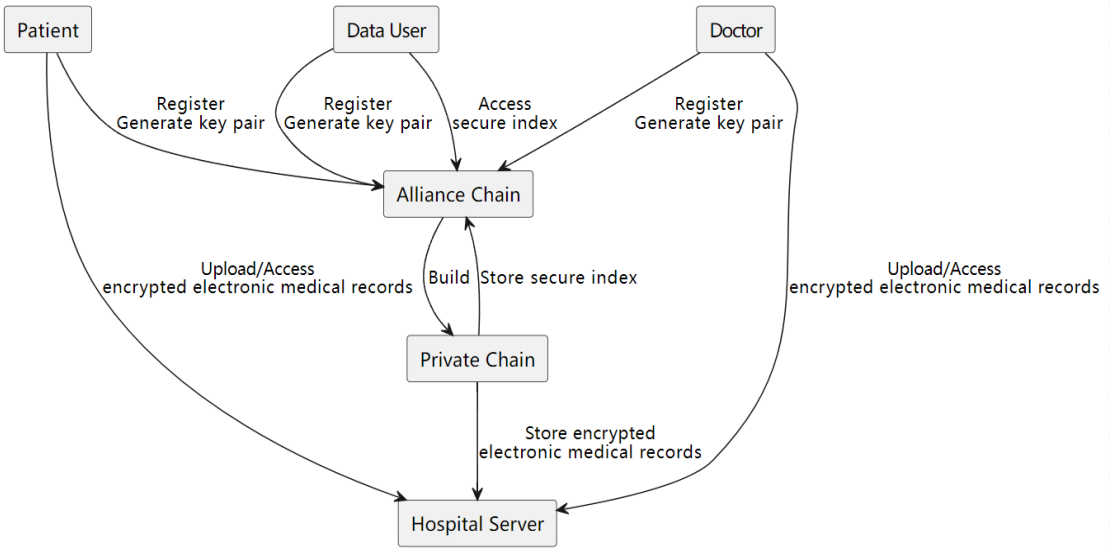



Figure 2 - System Model Diagram

## *References*

*1. Hossain, A., Quaresma, R., & Rahman, H. (2019). Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study. International Journal of Information Management, 44, 76-87.*

*2. Menachemi N, Collum T H. Benefits and drawbacks of electronic health record systems[J]. Risk management and healthcare policy, 2011: 47-55..*

*3. Quasim M T, Khan M A, Algarni F, et al. Blockchain frameworks[J]. Decentralised Internet of Things: A Blockchain Perspective, 2020: 75-89.*

*4. Gupta S, Sadoghi M. Blockchain transaction processing[J]. arXiv preprint arXiv:2107.11592, 2021.*

UDC 004.021

## ПРИМЕНЕНИЕ БЛОКЧЕЙНА В ЭЛЕКТРОННОЙ МЕДИЦИНСКО УЧЕТЕ

*Гао ялу*

*гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Цветков Виктор Юрьевич, заведующий кафедрой, профессор кафедры ФИБ*

**Аннотация.** децентрализации и неизменный характер блокчейна обеспечивает безопасную и прозрачную платформу для обмена данными, гарантируя целостность, конфиденциальность и безопасность данных. В этом эссе предпринята попытка углубиться в потенциал технологии блокчейн в смягчении проблем, с которыми сталкивается система здравоохранения, с упором на электронные медицинские записи (EHR).

**Ключевые слова:** блокчейндецен,трализованный, неизменяемый, EHR

UDC 004.921

## IMAGE COMPRESSION METHOD BASED ON WAVELET TRANSFORM

*Zeng Peng, Wang Ying, Wei Zijian*

*gr.267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Tsviatkou Viktar, head of the department of infocommunication technologies*

**Annotation.** In many algorithms for image compression, the SPIHT and SPECK algorithms based on wavelet transform have good performance. This article introduces the basic principles of wavelet transform, and implements the SPHIT and SPECK image compression algorithms based on wavelet transform. Besides, the two algorithms are compared, and experimental results and experimental conclusions are given in conclusion.

**Keywords:** wavelet, image compression, SPECK, SPIHT

***Introduction.*** The main problem solved by image compression is to minimize the amount of data used to represent image information. Some kind of transformation is usually used to remove redundant information in the image to achieve the purpose of compression. Image transformation for image compression concentrates the energy of the image in the transformation domain It means that a large amount of information is concentrated on a small number of coefficients, while other data is very small or almost zero. When the data is compressed and encoded, the data can be compressed more effectively, which is very important for the efficient storage and transmission of images significance. At present, the common transformations used for image compression mainly include K-L exchange, Fourier transform, discrete cosine transform (DCT), wavelet transform, and geometric multi-scale analysis that have appeared in recent years [1].

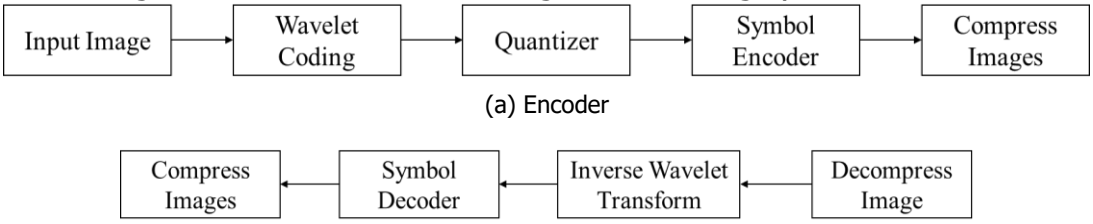
Wavelet transform is a signal processing technique that decomposes the original signal into multiple sub bands, each sub band containing information in a different frequency range. It has good scale invariance and local adaptability, can perform good sparse representation of irregular area images, and has a complete theoretical system to restore the original image from sparse

coefficients, and has developed rapidly in the field of image processing.

To improve the shortcomings of poor reconstruction quality of wavelet compressed images, this paper uses spectrogram wavelet transform to decompose the Set Partitioning in Hierarchical Trees (SPIHT) and Set Partitioned Embedded Block (SPECK) algorithm. In the lab, the results shown that SPECK algorithm has higher encoding speed and it is one of the better-performing embedded image coding algorithms. This algorithm achieves good compression effects after compressing and encoding classic images, and has a high compression ratio and peak signal-to-noise ratio.

***Classic Wavelet Transform.*** For a long time, image compression coding has used discrete cosine transform (DCT) as the main transformation technology, and has been successfully applied to various standards, such as JPEG, MPEG. However, in DCT-based image transformation coding, people divide the image into blocks of 88 pixels or 1616 pixels for processing, which is prone to block effects and mosquito noise.

Wavelet transform is a global transform with good local optimization performance in both time domain and frequency domain. Wavelet transform encodes the transform coefficients of image pixel decorrelation, which is more efficient than classical encoding and has almost no distortion. It is easy to consider human visual characteristics in applications, thus becoming one of the main technologies for image compression and coding. Wavelet transform can achieve better time resolution in the high-frequency part of the signal: better frequency resolution can be achieved in the low-frequency part of the signal, thereby effectively extracting information from signals (such as speech, images, etc.) to achieve Data compression purposes [2]. The figure below is a block diagram of the wavelet encoding and decoding system.




(a) Encoder

(b) Decoder

Figure 1 – Block diagram of the wavelet encoding and decoding system

The basic steps of image compression based on wavelet transform are as follows, and Figure 2 shows the wavelet transform decomposition steps taking the 'Lena' image as an example.

①Use wavelet to decompose the image layer and extract the low-frequency and high-frequency coefficients in the decomposition structure.

②Reconstruction of each frequency component.

③Compress the first layer of low-frequency information.

④ Compress the second layer of low-frequency information.

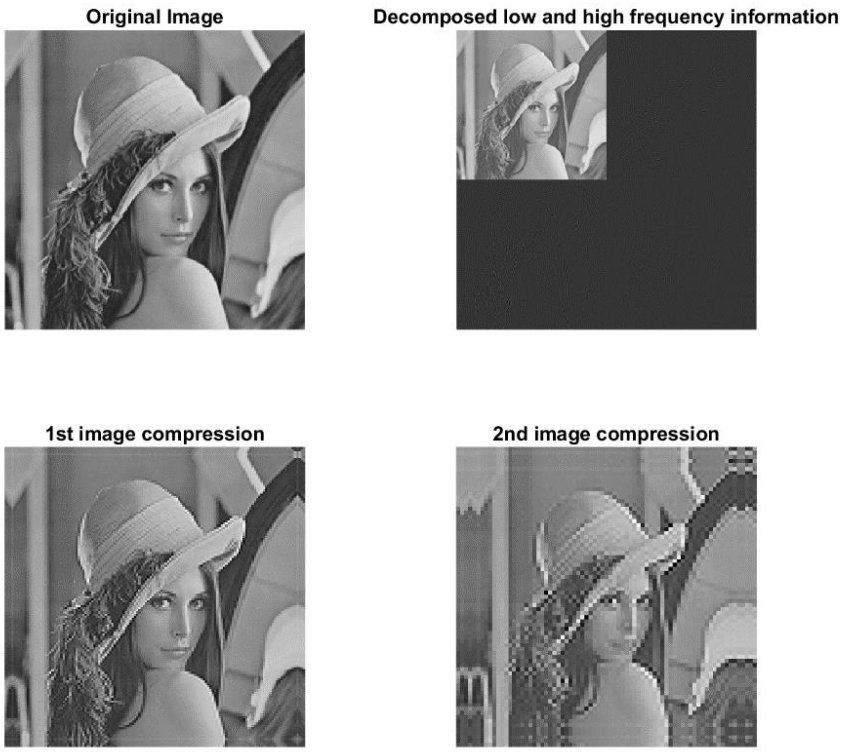



Figure 2 – An example process of Wavelet compression

***SPIHT Algorithm.*** After completing the spectral wavelet transform of the image, multiple one-dimensional wavelet coefficient vectors are obtained.

The main idea of the SPIHT algorithm is to use a given threshold to compare each coefficient in the wavelet coefficient set. If the value is greater than the threshold, a binary number is output as a sign of the importance of the coefficient; this binary flag is the key to the image [3]. The code stream generated after encoding the coefficients. After all the wavelet transform coefficient values have been traversed, the threshold value is halved, and then the wavelet coefficient set is scanned, compared with the updated threshold value, and then the corresponding image compression code stream is output until the threshold value becomes 1. Figure 3 and Figure 4 illustrate the wavelet principle of SPIHT transform, which is an image compression process based on wavelet blocks.

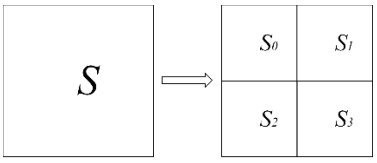



Figure 3 - Wavelet block of partitioning

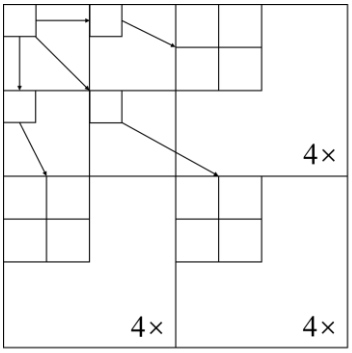
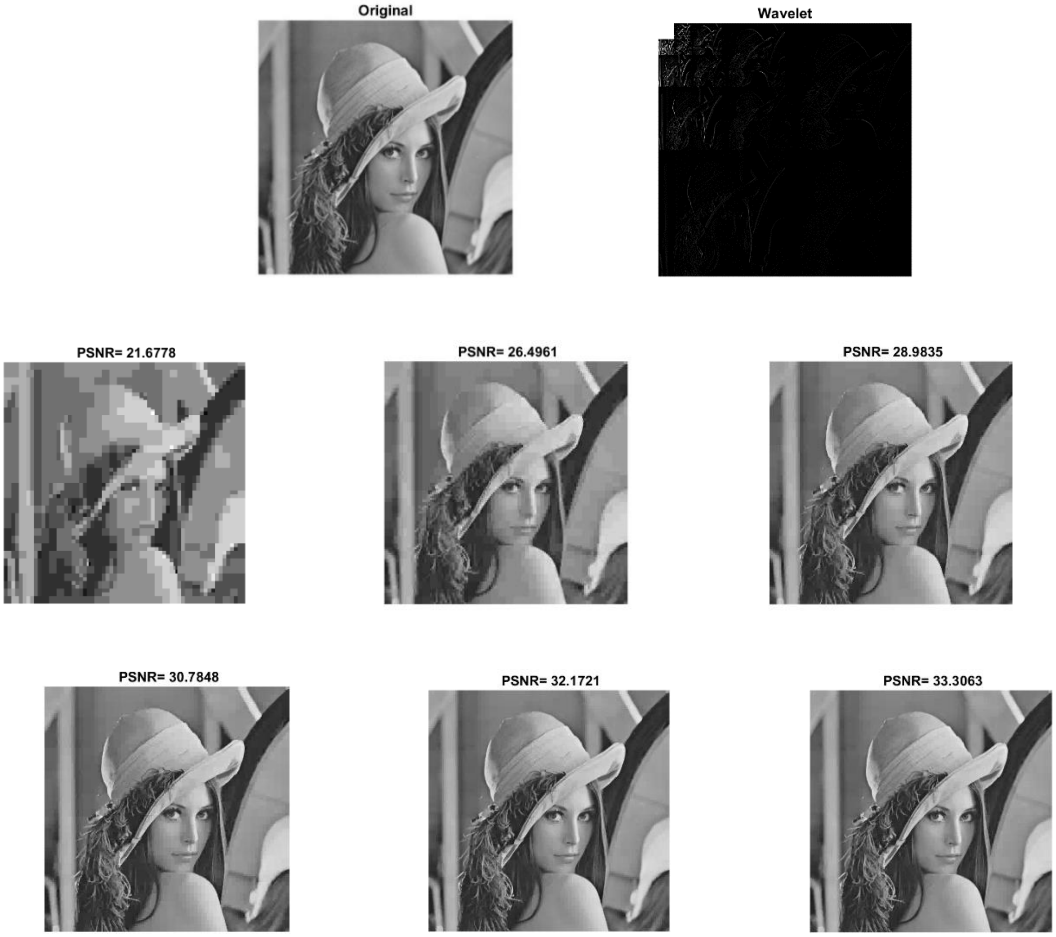



Figure 4 - Tree-based organization in wavelet transform

Here is an example of SPIHT algorithm based on wavelet. In Figure 5, wavelet 'haar' is used and the transform level is 4. PSNR stands for Peak Signal-to-Noise Ratio. In the process of using speck to process images, 9 iterations were carried out, the PSNR continued to increase, and the compression quality became better and better.




(a) Interaction times 1-6


(a) Interaction times 7-9
Figure 5 – An example of SPIHT algorithm, level = 4, wavelet 'haar', 9 interaction times

To the set classification strategy of the SPIHT algorithm is relatively complex, three lists are needed to store the wavelet coefficients to be encoded and quantized, and the calculation amount is relatively complex, so the encoding speed will be reduced accordingly.

***SPECK Algorithm.*** When the SPIHT algorithm performs image compression, it needs to be iterated many times, so there is an improved algorithm. Since there are many unimportant coefficients in the wavelet coefficients, which have the characteristics of energy aggregation and energy attenuation as the scale increases, based on block set division the ideological SPECK (Set Partition Embedded Block Code) algorithm is a coding algorithm for wavelet coefficients. This algorithm is one of the better performing embedded hierarchical image coding algorithms in recent times. In SPECK, the blocks are recursively and adaptively partitioned such that high energy areas are grouped together into small sets whereas low energy areas are grouped together in large sets.

Here is an example of SPECK algorithm based on wavelet. In Figure 6, wavelet 'haar' is used and the transform level is 4. PSNR stands for Peak Signal-to-Noise Ratio. In the process of using speck to process images, 4 iterations were carried out, the PSNR continued to increase, and the compression quality became better and better.

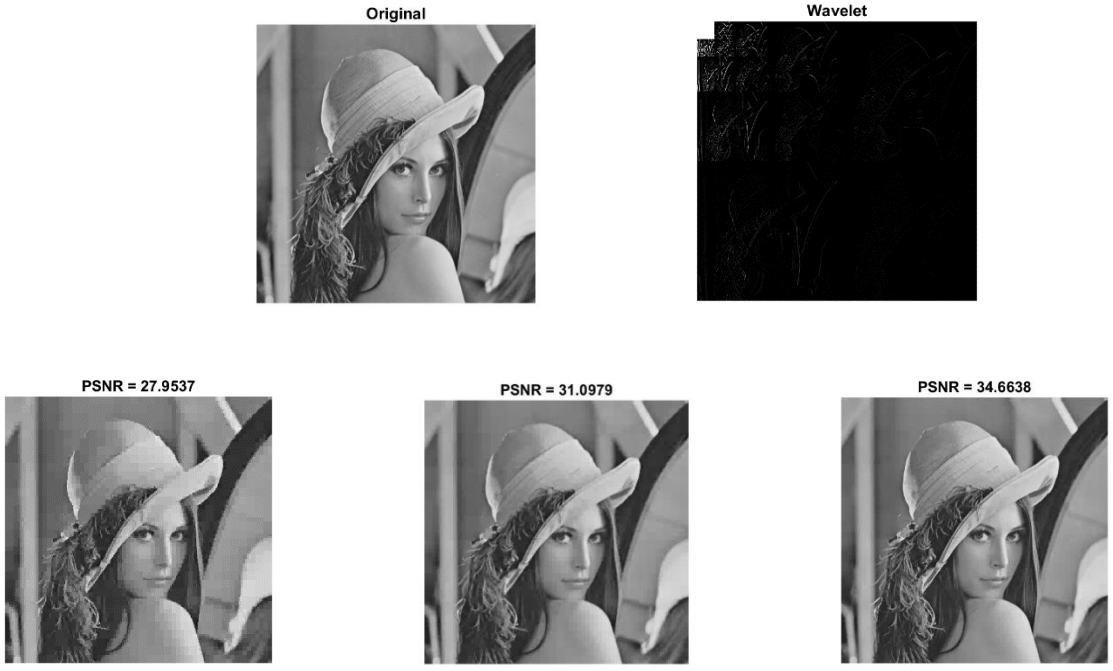



Figure 6 – An example of SPECK algorithm, level = 4, wavelet 'haar', 3 interaction times

Compared with the SPIHT algorithm, this algorithm reduces the number of recursive calls of the function, which improves memory space utilization, so the complexity of the algorithm is reduced, and the operation rate increases accordingly.

***Conclusion.*** This article introduces the basic principles of wavelet transform, and takes the 512pixel×512pixel×8bit standard image 'Lena' as an example to conduct a 4-level wavelet decomposition and reconstruction experiment, and conducts a 4-level wavelet decomposition and reconstruction experiment on the SPIHT algorithm, and in the same situation compare with the SPECK algorithm. Combining the above results, the following conclusions can be drawn:

(1) Compared with the SPIHT algorithm, due to the reduced memory space of the SPECK encoding algorithm, the bit allocation is more reasonable and the classification strategy is more complete. Under the same compression ratio, the image restoration quality of this algorithm is better than that of the original SPIHT algorithm.

(2) The SPECK algorithm is more efficient than SPIHT algorithm. It mainly reduces the complexity of the algorithm and allocates bits reasonably, so that under the same compression ratio, not only the reconstruction quality of the algorithm is better than that of the SPIHT algorithm, but also the operation rate is also higher than the before one.

## *References*

*10. Xiao Xiazi, Ma Yongjie, Xu Guowei. Research of SPIHT and SPECK Compression Algorithms. Computer Technology and Development, 2011, 21(1):3.DOI:10.3969/j.issn.1673-629X.2011.01.022.*

*11. Zhou Yufeng, Cheng Jingquan, Wavelet transform and its application, PHYSICS, 2008, 37(01): 24-32*

*12. Pragya Tiwari1, Mohd Ahmed, S.G.Kerhalkar. Transmission of Images Using SPECK. IJCSNS International Journal of Computer Science and Network Security, Nov 2014, VOL.14 No.11.*

УДК 004.921

## МЕТОД СЖАТИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

*Цзэн Пэн, Ван Ин, Вэй Цзыцзянь*

*гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Цветков Виктор Юрьевич, заведующий кафедрой, профессор кафедры ФИБ*

**Аннотация.** Во многих алгоритмах сжатия изображений хорошую производительность демонстрируют алгоритмы SPIHT и SPECK, основанные на вейвлет-преобразовании. В этой статье представлены основные принципы вейвлет-преобразования и реализованы алгоритмы сжатия изображений SPHIT и SPECK, основанные на вейвлет-преобразовании. Кроме того, проводится сравнение двух алгоритмов, а в заключение приводятся экспериментальные результаты и экспериментальные выводы.

**Ключевые слова:** вейвлет, сжатие изображения, SPECK, SPIHT

UDC 004.722.2

# BATMAN-ADV: An Energy-Efficient Wireless Routing Protocol for Dynamic Ad Hoc Networks

*Wei ZiJian, Zeng Peng, Wang Ying*

*gr.267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Tsviatkou Viktar, head of the department of infocommunication technologies*

**Annotation**. BATMAN-ADV is a wireless routing protocol operating at the data link layer of the OSI model. It transmits routing information using Ethernet frames and utilizes MAC addresses for node identification. With the ability to run multiple protocols at the network layer, BATMAN-ADV offers flexibility and scalability. By functioning as a Linux kernel module, it minimizes CPU overhead and energy consumption. This makes it a favorable choice for energy-sensitive MANNET systems.

**Keywords:** BATMAN-ADV, Wireless routing protocol, MANNET

***Introduction.*** BATMAN-ADV (Better Approach to Mobile Ad-Hoc Networking Advanced) is a new wireless routing protocol. The protocol runs on the data link layer of OSI model in the form of Linux kernel module, and transmits routing information through Ethernet frame. Each node is identified by MAC address instead of IP address for communication. The network layer is free to run a variety of protocols, with better flexibility and scalability.

Most wireless routing protocols run on Layer 3 of the model. They send packets, exchange routing information, and process the kernel's routing table to implement routing policies. BATMAN-ADV operates entirely at the second layer of the model, transmitting routing information through Ethernet, and the protocol also handles data traffic. The protocol encapsulates and forwards all data until it reaches its destination, simulating a virtual network exchange environment [1]. As a result, all nodes act as if they are in a local link; they are not aware of the topology of the network and are not affected by changes in the network.

The BATMAN-ADV routing protocol is essentially an integrated module of the Linux kernel, and data is processed in the kernel space, which greatly reduces the overhead of system CPU resources and correspondingly reduces energy consumption. The vehicle node of the tactical MANNET system is very sensitive to the weight, volume and energy consumption of the electronic equipment, so the choice of this protocol is very advantageous.

***Packet classification.*** The BATMAN-ADV protocol has eight packet formats.

BATADV_IV_OGM: OriginatorMessage (Source node message) is used to discover nodes in the wireless environment and establish routing information. At the same time, the protocol determines the metric value based on the number of legitimate messages received. This is the most important packet format, its main functions are: to the whole network other nodes to show their own existence; The route measurement is carried out by counting the received OGM messages [2]. The corresponding route is established through OGM messages.

BATADV_BCAST: Packet with broadcast payload, which is broadcast information to all nodes, since it is implemented at the data link layer, sent to nodes in the same conflict domain;

BATADV_CODED: This is a network coded packet. It uses network coding technology to combine two packets into one transmission process to reduce the total transmission time.

BATADV_UNICAST: A packet with a unicast payload, which is sent to a single node with a MAC address as its ID;

BATADV_UNICAST_FRAG: If the length of the - packet exceeds the value of the link, the

packet needs to be fragmented. In this packet, in addition to the payload, there is also fragmentation information;

BATADV_UNICAST_4ADDR: unicast packet that contains the source address of the sender in addition to the payload;

BATADV_ICMP: Similar to ICMP in the IP protocol, the ping or traceroute command can be used at the data link layer (the return message is a MAC address).

***BATMAN-ADV route discovery mechanism.*** The main function of the BATMAN-ADV routing protocol is to find the appropriate next hop for a given destination node. In other words, for a node running the BATMAN-ADV routing protocol in the network [3], it needs to maintain information about all reachable nodes in the whole network, and for each reachable node, it needs to maintain information about all neighboring nodes that can reach the node. Transmission Quality (TQ) is use for measures the transmission quality of the path (Link quality). The neighbor node with the highest TQ is the next hop of the route.

The BATMAN-ADV routing protocol runs in the following parts:

(1) Each node broadcasts an OGM (Original Message) message;

(2) When a node receives an OGM message from another node, it forwards it according to the policy so that the OGM message can be spread to the whole network. Therefore, according to the source node of the detection packet, all the nodes that can be reached in the whole network can be known, and the relevant information of these nodes can be maintained, and the path of all the reachable nodes can be obtained.

(3) In a wireless multi-hop network, there may be multiple reachable paths for a given destination node. Therefore, for each reachable node, maintain a list of local neighbors that are reachable to the node, and perform appropriate routing metrics on each path to select the best path for routing.

***Operation mechanism.*** For the node running the BATMAN-ADV routing protocol, it will periodically broadcast OGM packets [1]. Its main functions are: (1) to show its existence to other nodes in the whole network; (2) Route measurement is carried out by statistics of legitimate OGM messages received; (3) Establish the corresponding route through OGM messages.

The format of the OGM frame is shown in Figure 1.

<table>
<tr><td>Type</td><td>version</td><td>Survival time</td><td>Flag</td></tr>
<tr><td colspan="4">Serial number</td></tr>
<tr><td colspan="4">Source node mac address (first four bytes)</td></tr>
<tr><td colspan="2">Last two bytes of the mac address of the source node</td><td colspan="2">Last two bytes of the mac address of the previous hop</td></tr>
<tr><td colspan="4">Last-hop mac address (last four bytes)</td></tr>
<tr><td>Reserved field</td><td>TQ</td><td colspan="2">TVLV length</td></tr>
</table>

Fig. 1. OGM frame format

Type is the type that distinguishes packets. Version is the version number of the protocol. The serial number is used to identify whether the same OGM packet is received from multiple places. Time To Live (TTL) is the maximum number of forward hops before they are discarded [5].

After receiving OGM packets from other nodes, each node broadcasts the OGM packets to the outside through the corresponding forwarding mechanism, so that the OGM messages sent by one node

can flood to all nodes in the whole network. To reduce the overhead of message flooding, each node receives the same OGM packet only once.

After receiving an OGM packet from an interface, a node processes the packet, including determining whether the packet is valid and determining the relationship between the local node and the source node. Each time a node receives an OGM packet, it updates the information in the routing table. The main contents of the update are: (1) The link quality between the local node and the one-hop neighbor; (2) List of source nodes reachable by local nodes; (3) For each source node, the next hop neighbor node quality of all reachable paths; (4) Information about local network interfaces that reach all neighboring nodes (figure 2).

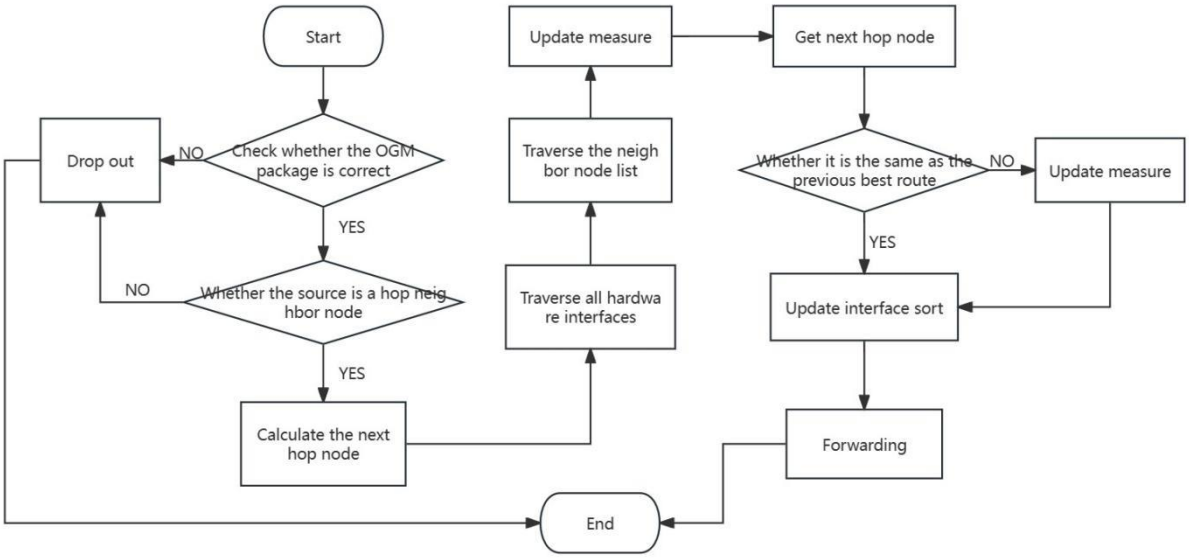



Fig. 2. Operation when a node receives an OGM packet

***Application of BATMAN-ADV protocol in wireless AD hoc network.*** Discovering the AD hoc topology: BATMAN-ADV collects and exchanges neighbor information of nodes to automatically build and maintain the AD hoc topology [6]. Nodes can join or leave the network dynamically without manually configuring routing information. This makes the deployment and management of AD hoc networks easier and more flexible.

Multipathing and load balancing: BATMAN-ADV supports multipath routing, that is, packets can be transmitted to their destination through multiple different paths. This improves the reliability and fault tolerance of the network, and enables load balancing, making the transmission of data across the network more efficient.

Network extensibility: BATMAN-ADV allows nodes in the network to join and leave freely without complex configuration or management. This allows the scale of the network to be flexibly scaled according to demand, suitable for a variety of scenarios, such as mobile sensor networks in cities, emergency communications at disaster sites, etc.

Low power consumption: The BATMAN-ADV protocol is designed with energy efficiency in mind, reducing the CPU overhead and energy consumption of the system through data processing and transmission in the kernel space. This is particularly important for mobile devices and sensor nodes in wireless AD hoc networks, extending their battery life and improving the sustainability of the system.

***Conclusion.*** The application of BATMAN-ADV in wireless AD hoc networking makes network deployment more simple, more scalable, with multipath and load balancing capabilities, and can reduce energy consumption, and is suitable for a variety of mobile and dynamic network environments.

## *REFERENCES*

*[1] L. Liu, J. Liu, H. Qian, and J. Zhu, "Performance Evaluation of BATMAN-Adv Wireless Mesh Network Routing Algorithms," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, 2018, pp. 122-127, doi: 10.1109/CSCloud/EdgeCom.2018.00030.*

*[2] ZHAO Zhihao, CHEN Yabing, ZHANG Jian. "Multi-hop wireless network research based on BATMAN-adv." Journal of Terahertz Science and Electronic Information Technology, 2021, 19(3): 433-437.*

*[3] Oh, Minseok. "An Effective, Secure, and Loop-Free Mesh Network Implementation." Information; Koganei Vol. 17, Iss. 5, (May 2014): 1913-1919.*

*[4] J. Lin, Z. Liu, and J. Dai, "Research and Optimization of Wireless Mesh Network Routing Protocol with Multiple Criterions," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 2019, pp. 72-78, doi: 10.1109/IAEAC47372.2019.8997932.*

*[5] B. Sliwa, S. Falten, and C. Wietfeld, "Performance Evaluation and Optimization of B.A.T.M.A.N. V Routing for Aerial and Ground Mobile Ad Hoc Networks," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-7, doi: 10.1109/VTCSpring.2019.8746361.*

*[6] E. Kulla, M. Ikeda, L. Barolli, and R. Miho, "Impact of Source and Destination Movement on MANET Performance Considering BATMAN and AODV Protocols," 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan, 2010, pp. 94-101, doi: 10.1109/BWCCA.2010.54.*


## BATMAN-ADV: ЭНЕРГОЭФФЕКТИВНЫЙ ПРОТОКОЛ БЕСПРОВОДНОЙ МАРШРУТИЗАЦИИ ДЛЯ ДИНАМИЧЕСКИХ ОДНОРАНГОВЫХ СЕТЕЙ


*Wei ZiJian, Zeng Peng, Wang Ying*

*гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Цветков Виктор Юрьевич, заведующий кафедрой*



**Аннотация.** BATMAN-ADV – протокол беспроводной маршрутизации, работающий на канальном уровне модели OSI. Он передает информацию о маршрутизации с помощью кадров Ethernet и использует MAC-адреса для идентификации узла. Благодаря возможности запуска нескольких протоколов на сетевом уровне BATMAN-ADV обеспечивает гибкость и масштабируемость. Функционируя как модуль ядра Linux, он минимизирует нагрузку на процессор и потребление энергии. Это делает его выгодным выбором для энергочувствительных систем MANNET.



**Ключевые слова:** BATMAN-ADV, протокол беспроводной маршрутизации, MANNET



UDC 004.921


## IMAGE COMPRESSION METHOD BASED ON RUN LENGTH ENCODING


*Wang Ying*

*gr.267011*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Tsviatkou Viktar, head of the department of infocommunication technologies*



**Annotation.** Video compression is an important part of image manipulation. This article first briefly introduces several commonly used video compression methods. Then, based on the file format of BMP images, a compression program using run length encoding (RLE) and C language was proposed, and the compression effect was discussed. Finally, this article discusses the characteristics of RLE and proposes several reasonable methods to improve its compression performance.



**Keywords:** RLE, image manipulation, BMP

***Introduction.*** Due to the large amount of data in images and videos, they bring a lot of inconvenience to storage and transmission. Therefore, image compression and video compression have been widely used. There are many types of data compression methods, which can be divided into lossless compression and lossy compression. Lossless compression uses statistical redundancy of data for compression, which can completely restore the original data without introducing any distortion. However, the compression rate is limited by the theoretical redundancy of data statistics, generally 2:1 to 5:1. The lossy compression method utilizes the insensitivity of human vision to certain frequency components in the image, allowing for the loss of certain information during the compression process; Although the original data cannot be fully restored, the lost part has a relatively small impact on understanding the original image, but has resulted in a much larger compression ratio [1]. It should be pointed out that the compression methods involved in this article are all lossless compression (with recoverability). There are several commonly used lossless compression methods for images:

RLE: Run length encoding is one of the simplest methods for compressing a file. Its approach is to replace a series of repeated values (such as the grayscale values of image pixels) with a single value and a count value. This method is easy to implement and effective for compressing strings with long repeated values. For example, for images with large areas of continuous shadows or the same color, The compression effect is very good using this method.

Arithmetic encoding: Arithmetic encoding is one of the main algorithms for image compression. This is a lossless data compression method and also an entropy encoding method. Unlike other entropy coding methods, other entropy coding methods typically divide the input message into symbols and then encode each symbol, while arithmetic coding directly encodes the entire input message into a number, a decimal n that satisfies ($0.0 \leqslant n<1.0$).

LZW encoding: The principle is to pair the value of each byte with the value of the next byte as a character pair, and set a code for each character pair. When the same character pair reappears, it is replaced by a code, and then paired with the next character. Its code can not only replace a string of data with the same value, but also, It can also replace a string of data with different values. If there are some data with different values that frequently appear repeatedly in image data, a code can be found to replace these data strings[2].

Huffman coding: Huffman encoding is achieved by replacing the original data with an unfixed length encoding. It was originally established to compress text files, but now there are many variants. Its basic idea is that values with higher frequencies correspond to shorter encoding lengths, while values with lower frequencies correspond to longer encoding lengths.

BMP is the abbreviation of Bitmap, which supports RGB color mode, index mode, grayscale, and bitmap color mode. It is the standard image file format in the Windows operating system and can be supported by various Windows applications. With the popularity of the Windows operating system and the development of rich Windows applications, BMP bitmap format is naturally widely used. The characteristic of this format is that it contains rich image information, which is almost not compressed, but this has resulted in its inherent disadvantage of occupying too much disk space[3]. In a BMP image file, the first 54 bytes of space are used to write basic information about the file, which can be divided into two parts: the file header (14 bytes) and the file information header (40 bytes).

In addition to the basic information of the file header and file information header, the content of the image body part of the BMP file is recorded line by line in the form of dots. The color information of each dot is recorded in three bytes, which respectively record the saturation of B (blue), G (green), and R (red) colors saturation, expressed as integers ranging from 0 to 255. In addition, the number of bytes recorded for each line of point element information in the BMP file must be a multiple of four. If the actual point element information is not a multiple of

four, a few bytes of zeros must be added at the end of each line.

***Implementation of compressed programs.*** The C source code uses run length encoding to compress BMP images. The principle is to first read a point as a reference after processing the basic information of the file, and then read the next point to see if it has the same value as the reference point. If it is the same, add the statistical number of the reference point by one, and continue to count the number of points with the same value. When a new point with a different value from the reference point is read, the new point is used as the reference point, and the pixels in the image are read in this way until the end of the file.

***Explore and improve methods.*** The compression ratio that RLE can achieve mainly depends on the characteristics of the image itself. If the image has larger blocks of the same color and fewer blocks, the compression ratio obtained will be higher. Conversely, RLE may not be able to handle natural images with rich colors, and there are often very few continuous pixels with the same color on the same line, And the number of consecutive rows with the same color value is even fewer. If RLE encoding method is still used, not only can image data not be compressed, but it may also make the original image data larger. Therefore, in specific implementation, it needs to be applied in conjunction with other compression encoding techniques.

Reading Point Path: The C program example given above reads points in line (main) order. Using this encoding method to compress bitmaps with no or minor changes in the horizontal direction can achieve a higher compression ratio. However, in practical situations, we often encounter images with more changes in the horizontal direction but the same pixel values in the local block range. In this case, We can use two other encoding methods for reading point paths, as shown in Figures 1 and 2:

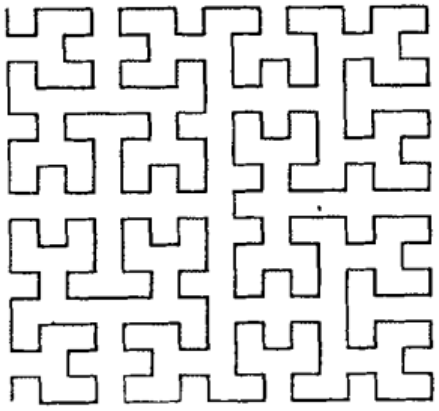


Figure 1 – Morton sequence

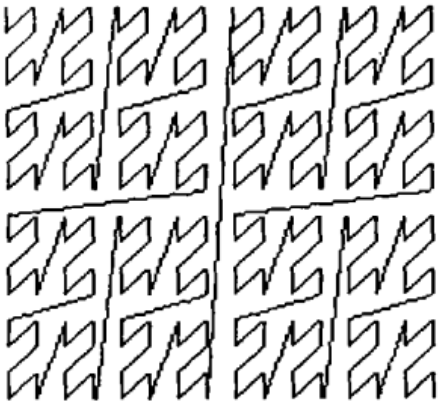


Figure 2 – Pi sequence

The use of the above two types of read point path encoding can achieve good compression ratios when compressing block like images with the same value. The phenomenon of block like images with the same value is common in various images, but the complexity and length of the program will increase significantly when using the above two read point paths.

Establishing a color index: In the above program, we can see that in the compressed file, a set of identical points should be recorded for at least four bytes (three bytes are used to record the saturation of R (red), B (blue), and G (green) colors, that is, the color values of the same value points in that group, and the other byte is used to record the number of same value points), If one or several sets of points of the same value with different sizes appear frequently

in the image, a considerable amount of space in the compressed file is used to repeatedly record the color values of these groups of points. To avoid wasting this resource, we can establish a color index, which is a shorter encoding to replace a color value. For example, if we want to record 40 positive red points, we originally need to write 0000FF 28 four bytes, When we use 1 to do the color index code for positive red, only 0128 bytes are needed. This means that when using run through encoding to compress an image with few color values, we can first traverse each pixel value of the image and index each different pixel value with a shorter code[4]. This way, when recording a set of same value points in the compressed file, Only using the index of the same value point color values can improve the compression ratio to a certain extent. It is not difficult to see why using run length encoding to compress binary images achieves better results.

***Conclusion.*** Firstly, the image can be compressed by changing the order of the pixels in the read image, such as Morton sequence and Pi sequence. These two types of read path encoding can achieve better compression ratios when compressing block like images with the same value. Secondly, establish a color index. When compressing an image with low color values, using a shorter code as the index can also improve the compression ratio.

## *References*

*[1] Rong Guan'ao. Computer Image Processing [M]. Beijing: Tsinghua University Press, 2000.*
*[2] Statement Peng. Introduction to Geographic Information Systems [M]. Beijing: Science Press, 1997.*
*[3] Tan Haoqiang. C Language Programming [M]. Beijing: Tsinghua University Press, 2001.*
*[4] Wayne E. Carlson. A Survey of computer Graphics Image Encoding and Storage Formats [J]. Computer Graphics, 1991, 25(2) :20-23.*

UDC 004.921

## МЕТОД СЖАТИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ КОДИРОВАНИЯ ПУТЕШЕСТВИЙ

*Ван Ин*

*гр.267011*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Цветков Виктор Юрьевич, заведующий кафедрой, профессор кафедры ФИБ*

**Примечания.** Сжатие видео является важной частью обработки изображений. Эта статья начинается с краткого описания нескольких распространенных методов сжатия видео. Затем формат файла, основанный на изображениях BMP, предлагает программу сжатия, которая использует кодирование путешествий (RLE) и язык C, и обсуждает эффект сжатия. Наконец, в этой статье обсуждаются характеристики RLE и предлагаются несколько разумных способов улучшить его производительность сжатия.

**Ключевые слова:** RLE, Обработка изображений, BMP

УДК 004.7:004.715

## ВЫБОР ПРОТОКОЛА МАРШРУТИЗАЦИИ ДЛЯ ОРГАНИЗАЦИИ VPN

*Ковалько О.А., Кулешов И.С.*

*гр. 367041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Саломатин С.Б. – кандидат технических наук, доцент кафедры ИКТ*

**Аннотация.** В статье рассматривается вопрос выбора протокола маршрутизации для организации сетей VPN. Анализируются наиболее популярные протоколы маршрутизации, такие как MPLS, IPSec, и OpenVPN, их преимущества и недостатки в различных сценариях использования. Статья помогает инженерам и администраторам сети сделать обоснованный выбор в пользу наиболее подходящего протокола для их конкретных нужд.

**Ключевые слова:** VPN, протоколы маршрутизации, MPLS, IPSec, OpenVPN, сетевая безопасность.

***Введение.*** В эпоху цифровой трансформации, когда объемы цифровых данных растут с невиданными ранее темпами, а угрозы информационной безопасности становятся всё более прогрессивными и хитрыми — защита конфиденциальности и целостности данных приобретает критическое значение.

Особенно это касается организаций, стремящихся обеспечить безопасное и надежное взаимодействие внутри своих корпоративных сетей и за их пределами. Виртуальные частные сети (VPN) — на сегодняшний день, являются одним из ключевых инструментов, обеспечивающих защиту данных в процессе их передачи через общедоступные сети [1]. Однако эффективность VPN во многом зависит от выбора подходящего протокола маршрутизации, который обеспечивает не только безопасность, но и высокую производительность, масштабируемость и экономическую эффективность.

В этом контексте, выбор протокола маршрутизации для VPN представляет собой сложную задачу, требующую учета множества факторов, от технических характеристик и требований к безопасности до стоимости внедрения и поддержки [2]. Настоящая статья посвящена обзору этих ключевых аспектов и предлагает комплексный анализ, направленный на помощь в выборе наиболее подходящего протокола маршрутизации для организации эффективных и безопасных VPN-сетей [3].

***Основная часть.*** Обзор протоколов маршрутизации, MPLS (Multiprotocol Label Switching). MPLS представляет собой механизм в высокопроизводительных телекоммуникационных сетях, который направляет данные от одной сетевой ноды к другой на основе коротких путевых меток вместо длинных сетевых адресов, ускоряя тем самым процесс передачи данных. Он поддерживает разделение трафика и его приоритизацию, что критически важно для приложений, требующих высокой пропускной способности и низкой задержки, таких как видеоконференции и VoIP. В корпоративных сетях MPLS обеспечивает улучшенное качество обслуживания, позволяя компаниям гарантировать определенный уровень производительности сети для критически важных приложений [4].

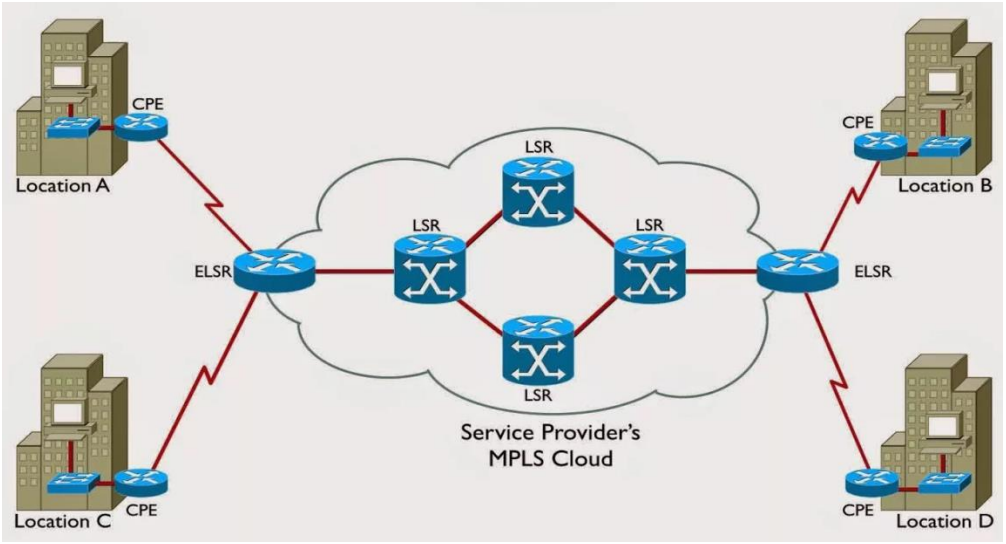



Рисунок 1 – Структура работы MPLS (Multiprotocol Label Switching)

IPSec (Internet Protocol Security). IPSec является набором протоколов для защиты данных, передаваемых через IP-сети, путем аутентификации и шифрования каждого IP-пакета в потоке коммуникации. Он широко применяется для создания защищенных соединений между сетями (сайт-сайт VPN) или между удаленным пользователем и сетью (клиент-сеть VPN). IPSec обеспечивает конфиденциальность передаваемых данных, защищая их от прослушивания, а также проверяет целостность и подлинность данных, предотвращая их подмену или несанкционированный доступ [5].

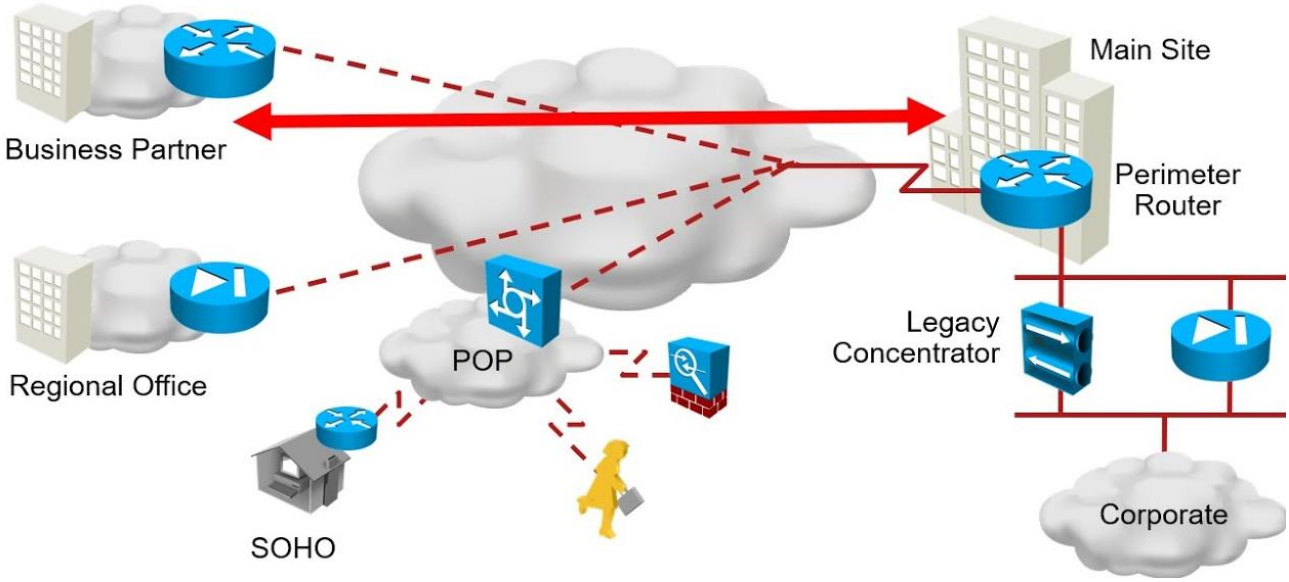



Рисунок 2 – Структура работы IPSec (Internet Protocol Security)

OpenVPN. Этот протокол представляет собой решение с открытым исходным кодом, обеспечивающее создание защищенных VPN-соединений. OpenVPN характеризуется высокой степенью гибкости и конфигурируемости, поддерживая различные типы аутентификации, включая сертификаты, ключи предварительного обмена, и двухфакторную аутентификацию. Благодаря поддержке стандартного SSL/TLS для шифрования сессий, OpenVPN предоставляет сильную защиту данных, делая его подходящим для использования в малых и средних предприятиях, которые ищут надежное, но при этом экономически эффективное решение для организации VPN [6].

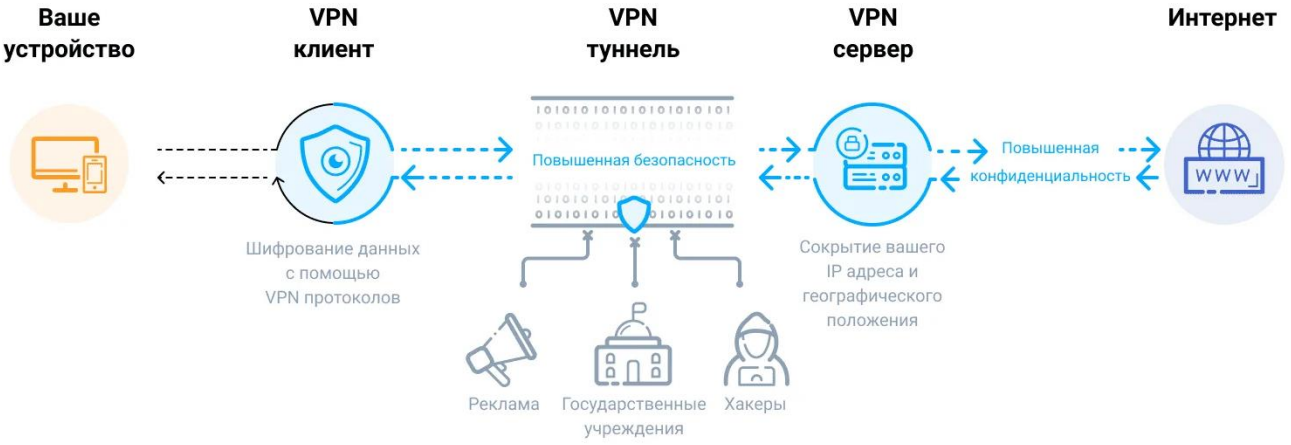



Рисунок 3 – Структура работы OpenVPN

Комплексный анализ преимуществ и недостатков протоколов маршрутизации MPLS, IPSec и OpenVPN с учетом технических и экономических аспектов:

- MPLS предлагает высокую производительность и надежность для корпоративных сетей, поддерживая различные типы трафика и качество обслуживания. Однако, внедрение MPLS может быть дорогостоящим и сложным, требуя специализированных знаний и оборудования.

- IPSec обеспечивает сильную защиту на сетевом уровне, шифрует весь трафик между точками. Он подходит для создания безопасных соединений через общедоступные сети, но может быть сложен в настройке и управлении, особенно в крупных сетях.

- OpenVPN предлагает высокую гибкость и конфигурируемость, подходят для малых и средних предприятий благодаря открытому исходному коду и поддержке различных методов аутентификации и шифрования. Его недостатком может быть необходимость в дополнительной настройке и потенциально более низкая скорость передачи данных по сравнению с MPLS в некоторых случаях.

Важно учитывать специфику организации и ее требования к безопасности, производительности и стоимости при выборе между этими протоколами.

При выборе протокола маршрутизации для VPN следует учитывать следующие критерии, адаптированные к специфике организации:

- Требования к безопасности. Если высокий уровень безопасности является приоритетом, IPSec может быть предпочтительным выбором за счет его способности шифровать весь трафик на сетевом уровне. OpenVPN также предлагает сильную защиту с гибкостью настройки.

- Производительность и масштабируемость. Для крупных корпоративных сетей, где важны высокая производительность и масштабируемость, MPLS может быть лучшим выбором благодаря его способности управлять различными типами трафика и обеспечивать качество обслуживания.

- Сложность настройки и стоимость. Если ресурсы ограничены, и требуется более экономичный вариант с простотой настройки, OpenVPN может быть наиболее подходящим из-за его открытого исходного кода и поддержки широкого спектра операционных систем.

- Объем и характер передаваемых данных. Рассмотрите характер вашего трафика и какие данные передаются. Для чувствительных данных, где требуется гарантия целостности и конфиденциальности, IPSec или OpenVPN могут предложить более надежные решения.

Выбор должен базироваться на комплексном анализе текущих и будущих потребностей организации в области безопасности, производительности и стоимости владения.

***Заключение.*** Анализ выбора протокола маршрутизации для VPN показал, что эффективное обеспечение безопасности корпоративной сети требует тщательного подхода к выбору протокола. Отсутствие универсального решения подчеркивает необходимость взвешенного анализа сильных и слабых сторон каждого протокола, в зависимости от специфических потребностей и условий использования. Ключевые аспекты, такие как технические характеристики, экономическая эффективность, и требования к безопасности, должны быть тщательно оценены для достижения оптимального баланса между стоимостью внедрения и уровнем защиты данных. Этот комплексный подход позволит организациям эффективно защитить свои сети, обеспечив при этом соответствие их бизнес-целям и требованиям.

## *Список литературы*


1. *Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник / В. Олифер, Н. Олифер. — СПб.: Питер, 2016. — 318 с.*
2. *Рыленков, Д. А. Анализ механизмов безопасности в протоколах динамической маршрутизации / Д. А. Рыленков. — Текст : непосредственный // Молодой ученый. — 2021. — № 43 (385). — С. 13-16. — URL: https://www.elibrary.ru/item.asp?edn=ebpbix (дата обращения: 15.02.2024).*
3. *Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2018. — 512 с.*
4. *Гольдштейн, А. Б. Транспортные сети IP/MPLS. Технология и протоколы : учебное пособие / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016. — 78 с. — ISBN 978-5-89160-129-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180139 (дата обращения: 15.02.2024). — Режим доступа: для авториз. пользователей.*
5. *Dayananda M.S., Kumar A. Architecture for Intercloud Services Using IPsec VPN // Second International Conference on Advanced Computing & Communication Technologies. Rohtak, Haryana, 2012. Pp. 463-467.*
6. *OpenVPN Cookbook - Second Edition - Keijser, J.J. SN - 9781786463128 UR - https://books.google.kz/books?id=AlgXvgAACAAJ - 2017. Packt Publishing*

UDC УДК 004.7:004.715

**THE CHOICE OF THE ROUTING PROTOCOL FOR THE VPN ORGANIZATION**

*Kovalko O.A, Kuleshov I.S.*

*gr.367041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Salomatin S.B. – Candidate of Technical Sciences, Associate Professor of the Department of ICT*

**Annotation.** The article discusses the issue of choosing a routing protocol for organizing VPN networks. The most popular routing protocols, such as MPLS, IPsec and OpenVPN, are analyzed, their advantages and disadvantages in various use cases. The article helps engineers and network administrators to make an informed choice in favor of the most appropriate protocol for their specific needs.

**Keywords:** VPN, routing protocols, MPLS, IPsec, OpenVPN, network security.

УДК 004.725.5

**МОДЕРНИЗАЦИЯ ВНУТРИЗОНОВЫХ СЕТЕЙ СВЯЗИ НА БАЗЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ**

*Ножников Р.А., магистрант гр.367041; Ножников Е.А., магистрант гр.367041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Хацкевич О.А. – кандидат технических наук, доцент*

**Аннотация.** В материалах доклада рассматриваются способы повышения эффективности работы зоновых и местных сетей связи на базе современных технологий. Внедрение современных технологии позволит обеспечить абонентов сельских сетей связи современными услугами, а также унифицировать оборудование, что упростит обслуживание сети связи.

**Ключевые слова:** модернизация, внутризоновые сети связи, современные технологии

***Введение.*** Актуальность темы данной работы состоит в том, что в настоящее время Министерство Связи РБ реализует проект развития широкополосного доступа в сетях связи. Основная цель стратегии – строительство на территории страны мультисервисных сетей связи следующего поколения с использованием архитектуры NGN (Next Generation Networks) на базе платформы IMS (IP Multimedia Subsystem). Концепция IMS представляет собой решение для предоставления услуг в сетях, основанных на IP-протоколе, вне зависимости от использования абонентом мобильного или стационарного доступа. Для обеспечения необходимой емкости сети для передачи больших объемов информации необходимо проведение модернизации существующих магистральных и внутризоновых сетей с внедрением новых технологий.

В качестве исследования в работе была рассмотрена сеть связи одного из районов Могилевской области.

IMS (IP Multimedia Subsystem) – технология передачи мультимедийных данных в электросвязи на основе протокола IP.

Возможность передачи мультимедиа даёт возможность оператору предоставлять разнообразные услуги, использование протокола IP позволяет построить гибкую сеть с низкими операционными расходами.

В IMS выделяются 3 уровня сети: пользовательский уровень или уровень передачи данных уровень управления и уровень приложений.

Внедрение технологии IMS позволит обеспечить абонентов сельских сетей связи современными услугами, а также унифицировать оборудование, что упростит обслуживание сети связи.

Технология плотного волнового мультиплексирования DWDM предназначена для создания оптических магистральных сетей связи, работающих на гигабитных и терабитных скоростях. Такой скачок производительности обеспечивает принципиально иной, нежели у сетей SDH, метод мультиплексирования – информация в оптическом волокне передается одновременно большим количеством световых волн. Каждая волна несет собственную информацию, при этом для оборудования DWDM неважно, каким способом она кодируется, и какие протоколы используются для передачи данных – устройства DWDM занимаются только объединением различных волн в одном световом пучке, а также их выделением из общего сигнала. Кроме большого увеличения пропускной способности технология плотного волнового мультиплексирования позволяет максимально использовать уже имеющуюся инфраструктуру за счёт возможности коммутации с технологией SDH и обеспечить возможность полного удовлетворения роста потребностей в скорости передачи информации.

***Основная часть.*** Существует много методов повышения производительности и гибкости сети, увеличения скорости передачи и увеличения ёмкости. Сравним разные методы наращивания производительности:

– дополнительная прокладка волоконно–оптического кабеля;

– переход к аппаратуре временного мультиплексирования TDM;

– применение технологий волнового мультиплексирования (WDM).

Первый способ до недавнего времени являлся стандартным для многих операторов связи, испытывающих необходимость в увеличении пропускной способности каналов связи. Как правило, прокладка нового кабеля оправдывается только при небольших расстояниях и если она не сопряжена с трудностями. Но даже в таком случае оператор вряд ли сможет предоставить новые сервисы и утилизировать полосу пропускания в достаточной степени. Это может показаться неожиданным, но установленное сегодня оборудование TDM использует менее 1 % возможностей оптического волокна. В большинстве случаев такое решение оказывается непрактичным или даже невозможным.

Второй способ – технология TDM предусматривает объединение нескольких входных низкоскоростных каналов в один составной высокоскоростной канал. Входные каналы по очереди модулируют высокочастотную несущую в течение выделенных им коротких промежутков времени (тайм–слотов), которые периодически повторяются. Например, в течение первого тайм–слота несущая модулируется первым входным каналом, в течение второго – вторым, в течение третьего – третьим, в течение четвертого – четвертым, в течение пятого – снова первым, в течение шестого – снова вторым и т. д. в соответствии с рисунком 1.


Рисунок 1 – Принцип передачи информационных каналов в системах TDM

Реализация второго варианта в сетях дальней связи SDH тоже связана с рядом трудностей. До недавнего времени в таких сетях самым быстрым был канал STM–64 (скорость передачи информации 10 Гбит/с). Затем началось внедрение аппаратуры уровня STM–256, обеспечивающей производительность 40 Гбит/с. Однако здесь возникает целый ряд проблем. Дело в том, что большая часть инсталлированной базы кабелей использует одномодовое оптическое волокно, для которого дисперсия в окне прозрачности 1550 нм оказывается слишком высокой. В результате для эффективной передачи необходимо прокладывать либо отрезки кабеля с дисперсией противоположного знака, либо полностью новое волокно со смещенной ненулевой дисперсией (Non–Zero Dispersion Shifted Fiber – NZDSF). Кроме этого, увеличение скорости передачи приводит к высокой плотности потока излучения на достаточно протяженных участках. Это, в свою очередь, вызывает нелинейные оптические эффекты. Вот далеко не полный перечень ограничений при переходе к высоким скоростям. Поэтому при таком подходе оператор вынужден протестировать буквально каждый канал на его совместимость с аппаратурой уровня сигнала STM–64 и STM–256.

Теперь рассмотрим третий вариант – технологию WDM, позволяющую заметно повысить эффективность использования суммарной пропускной способности оптических волокон.

WDM это вид технологии передачи в волоконно–оптической связи. Исходя из факта, что по волокну можно передавать одновременно несколько несущих с разной длиной волны, эта технология делит пригодные для передачи по волокну длины волн на несколько диапазонов. В каждом диапазоне передаётся оптический сигнал на заданной длине волны и эти каналы независимы. Оптическое и волновое мультиплексирование по сути является оптическим и частотным уплотнением волокна (OFDM), но в оптическом диапазоне используют длину волны вместо частоты для описания процессов мониторинга и контроля. С развитием электронно–оптической техники, плотность уплотнения волокна будет сильно возрастать. В отличии от DWDM (Dense Wavelength Division Multiplexing/ Плотное волновое мультиплексирование) WDM с низкой плотностью называется CWDM (Coarse Wave Division Multiplexing/ Грубое волновое мультиплексирование).

Структура WDM системы приведена на рисунке 2.

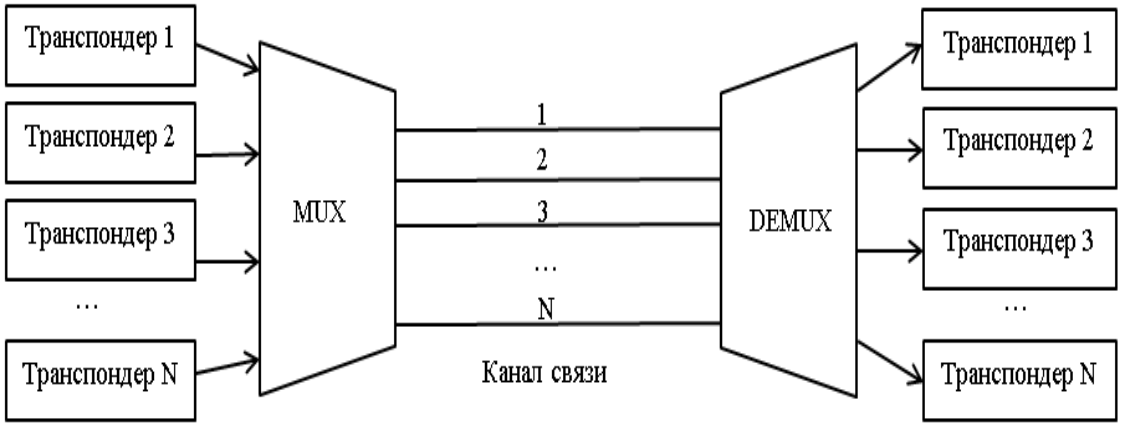



Рисунок 2 – Структура WDM системы

Технология плотного волнового мультиплексирования (Dense Wave Division Multiplexing, DWDM) предназначена для создания оптических магистралей нового поколения, работающих на гигабитных и терабитных скоростях.

Структура DWDM системы представлена на рисунке 3.

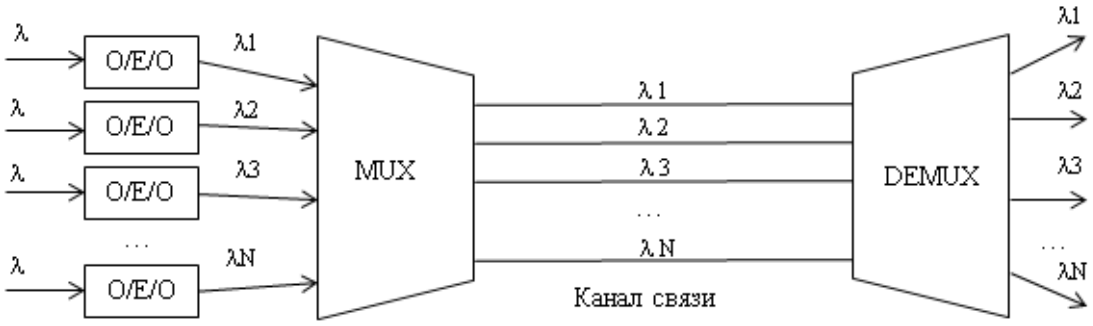



Рисунок 3 – Структура DWDM системы

Технология DWDM несомненно это предпочтительная технология в сфере современных волоконных приложений, но с другой стороны, довольно дорогостоящая. Более дешёвой WDM технологией является CWDM (Coarse wavelength division multiplexing/ Грубое мультиплексирование с разделением по длине волны).

Технология CWDM очень похожа на DWDM. Разница состоит в следующем:

– В CWDM большой промежуток между каналами, и в одном волокне можно мультиплексировать от 2 до 16 спектральных каналов. Поэтому они называются «грубым» и «плотным».

– Модуль лазера CWDM использует лазер без охлаждения, а DWDM использует охлаждение, технология охлаждения нужна для стабилизации длин волн, что довольно сложно реализовать и требует больших расходов. CWDM обходит эту трудность. DFB лазер применяемый в системе CWDM не нуждается в охлаждении, что намного сокращает его стоимость.

Пример построения CWDM системы представлен на рисунке 4.

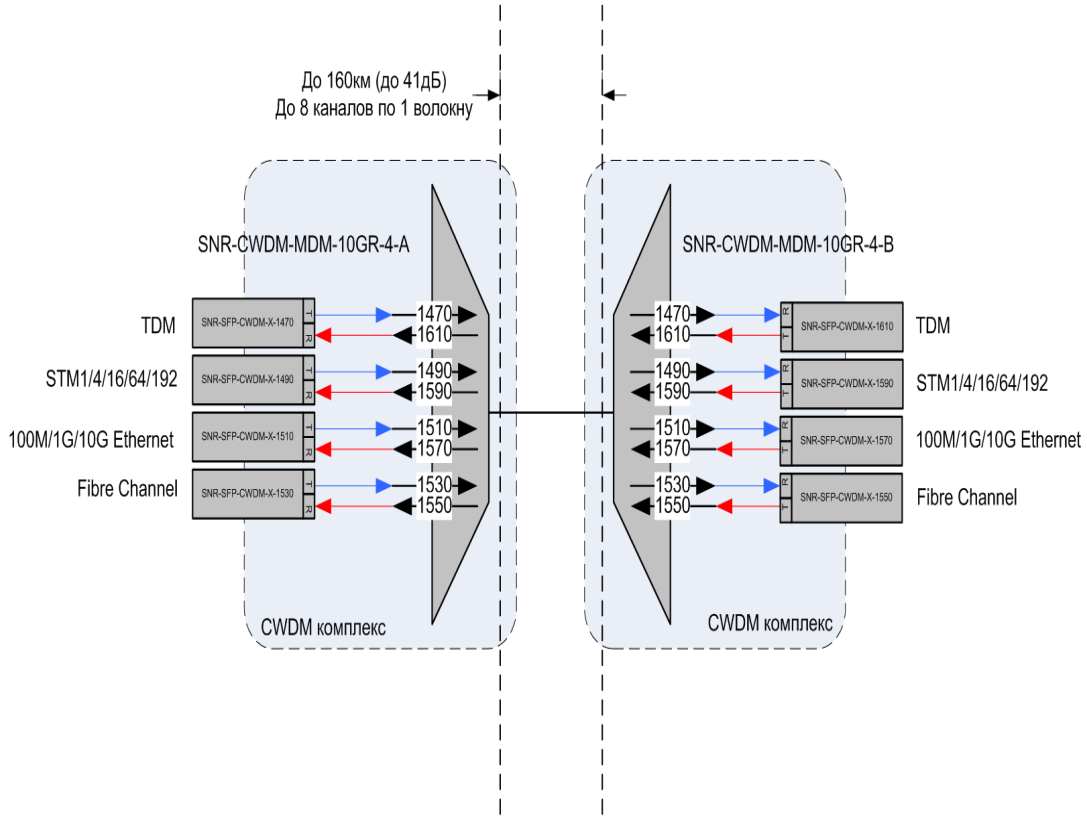



Рисунок 4 – Построение CWDM системы по топологии «точка–точка»

***Заключение.*** Модернизация местных зоновых сетей связи должны быть направлена на повышение объема передачи данных и увеличения количества абонентов. Модернизация должна учитывать перспективы развития сети связи и изменения в области технологии. Модернизацию можно проводить на базе уже существующих сетей технологии SDH, IMS. Этот подход до недавнего времени являлся стандартным, однако оправдывался только при небольшом расстоянии и небольшом количестве абонентов.

Технология сложного волнового мультиплексирования (Duxe Wave Division Multiplexing, DWDM), позволяет создать магистральные линии нового поколения с гигабитными и терабитными скоростями. Технология DWDM позволяет увеличить пропускную способность линии связи без прокладки новых кабелей.

Понизить стоимость модернизации местных и зоновых сетей связи можно с помощью использования технологии CDWM (Глубокое мультиплексирование с разделением по длине волны). Такую технологию можно использовать на сетях городов области.

## *Список литературы*

*1. Institute of Health Metrics and Evaluation. Global Health Data Exchange (GHDx) [Электронный ресурс]. – IHME – 2006. – Режим доступа : https://vizhub.healthdata.org/gbd-results/. – Дата доступа : 05.03.2023.*

2. *Современные технологии для модернизации сети. – Режим доступа : http://naviny.by rubrics/computer/2012/01/11/ic_news*

UDC 004.725.5

**MODERNIZATION OF INTRAZONE COMMUNICATION NETWORKS BASED ON MODERN TECHNOLOGIES**

*Nozhnikov R.A., gr. 367041; Nozhnikov E.A., gr. 367041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Khatskevich O.A. – PhD in technical sciences, associate professor*

**Annotation**. The report discusses ways to improve the efficiency of zonal and local communication networks based on modern technologies. The introduction of modern technologies will make it possible to provide subscribers of rural communication networks with modern services, as well as to unify equipment, which will simplify the maintenance of the communication network.

**Keywords:** modernization, intrazonal communication networks, modern technologies

УДК 330.344.25

## ПОДСИСТЕМЫ ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО, ЛОГИСТИКА КОМПЛЕКСА «УМНЫЙ ГОРОД»

*Сидоренко С.А., Усевис А.В.*

*гр.267041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ*

**Аннотация.** В докладе представлен анализ построения государственных цифровых платформ как основы для электронного правительства. Рассматривается эффективность использования технологии интернета вещей в транспортной логистике. Описаны основные элементы интернета вещей (IoT), реализуемые в транспортной логистике.

**Ключевые слова:** государственные цифровые платформы, государственное управление, транспортная логистика, цифровизация, интернет вещей, блокчейн.

***Введение.*** Системы «Умный город» является стратегией позволяющая объединять разнообразные факторы городского развития, направленная на модернизацию и обновление инфраструктуры с принципиально новыми возможностями предоставления услуг, повышенный уровень безопасности, простоты в управлении и использовании [1]. Двумя важными подсистемами являются электронное правительство и логистика [2]. В связи с совместным использования различных технологий возможно решение многих задач таких как предоставление государственных услуг через цифровые платформы, ом и построение системы логистики.

***Электронное правительство.*** Цифровизация затрагивает все сферы жизнедеятельности любого государства. Не обошла она стороной и государственные органы управления. Все взаимотношения государства, бизнеса и гражданского общества строится посредством внедрения государственных цифровых платформ.

Большинство исследователей рассматривают платформу как цифровую форму организации взаимодействия между поставщиками и потребителями с целью минимизации транзакционных издержек при поиске партнеров, товаров, услуг, организации платежей, заключении контрактов, контроле исполнения договоренностей, оценке репутации отраслевых участников и т.д.

Государственная цифровая платформа (ГЦП) – это система формальных и неформальных правил и алгоритмов сетевого взаимодействия пользователей (потребителей), функционирующая на основе открытых и масштабируемых архитектурных стандартов программно – аппаратного обеспечения, необходимого для хранения, анализа и передачи цифровых данных об участниках взаимодействия [3].

К основному функционалу ГЦП относятся:

– снижение издержек государственного регулирования в различных отраслях

(сферах) госуправления посредством последовательного внедрения принципов good governance и lean government на основе полной цифровизации ключевых процессов отраслевого взаимодействия;

– формирование, динамическое обновление и анализ цифровых профилей участников ключевого взаимодействия;

– создание комплексной системы оценки эффектов и (или) общественной ценности ГЦП;

– реализация оптимальной для конкретной сферы госрегулирования модели монетизации ГЦП;

– агрегация и обеспечение доступа к структурированной информации о деятельности отрасли по различным аспектам, включая механизмы многопараметрического поиска и обратной связи с пользователями.

Создание ГЦП – это масштабные по количеству необходимых мер и вовлекаемых в ее создание участников проекты. При этом внедренная платформа позволяет осуществлять эффективный обмен готовыми решениями между большим количеством региональных и муниципальных органов власти, обеспечить им равный доступ к технологиям и иной поддержке по внедрению проектов цифровой трансформации, что многократно превышает однократно затраченные усилия.

При внедрении ГЦП государственные органы должны реализовывать принцип равнодоступности ресурсов для всех отраслевых участников. Правила и критерии доступа на ГЦП должны быть прозрачными и понятными для всех участников; предварительно эти правила должны пройти обсуждение с участниками регулируемой через платформу отрасли. Несмотря на более высокую скорость внедрения цифровых технологий, государству важно осуществлять оперативные изменения в нормативно-правовой базе, которые позволят легитимизировать правила доступа участников на платформу.

Одним из базовых условий для создание «куста платформ», или экосистемы цифровых платформ, где портал госуслуг – основной, но не единственный инструмент получения государственных, бюджетных и муниципальных услуг. Таким образом, трансформация в платформу происходит на основе единых механизмов включения новых акторов для содействия в исполнении сложных услуг или суперсервисов.

Государство может выступать координатором, сохраняющим контрольные функции при создании платформы «с нуля», но делегируя часть регуляторных функций уже созданным или создаваемым рыночным платформам, тем самым сокращая масштабы госрегулирования.

Основным риском для государства в роли координатора ГЦП является установление сбалансированных отношений с отраслевыми партнерами при создании совместных цифровых продуктов на базе платформы. При этом государство должно действовать в интересах граждан, обеспечивать высокий уровень конкуренции среди частных партнеров по предоставлению услуг, допущенных на платформу. В нормативно-правовой плоскости следует четко прописать функции и ответственность подрядчика, оператора платформы и ее владельца.

Государство также может стимулировать создание коммерческих цифровых платформ на тех рынках и в отраслях, где это экономически целесообразно. Это не должно означать исключительно выделение бюджетных средств на создание цифровых платформ, например, на платформу транспортного комплекса или платформу поддержки производственной и сбытовой деятельности субъектов малого и среднего предпринимательства. Это могут быть стимулы нескольких видов:

– предоставление доступа к критически важным для формирования цифровой

платформы данным из государственных информационных систем, перечням, реестрам и т.д. а также к необходимой государственной инфраструктуре взаимодействия с платформой;

– предоставление льготных условий и ставок для налогообложения, государственных грантов и субсидий;

– создание регуляторных песочниц для тех сфер и отраслей, где высокие транзакционные издержки, большое количество посредников между поставщиками и потребителями, фрагментированные, несвязанные источники поставок товаров (услуг) и т. д.;

– популяризация отраслевых платформенных сервисов;

– разработка нормативно-правовой базы, обеспечивающей равный доступ на платформу для всех участников, действенные механизмы разрешения споров, предоставление государственных гарантий законности взаимодействий через платформу.

Государство может делегировать часть регуляторных функций уже созданным или создаваемым рыночным платформам, тем самым сокращая масштабы госрегулирования. В действующей модели государственного регулирования объектом регулирования являются участники рынка, которые, в зависимости от осуществляемой деятельности, должны получать государственные лицензии (разрешения), периодически проходить проверки, предоставлять отчетность, оплачивать налоги (сборы) и т. д. При переходе участников рынка на платформу последняя берет на себя часть функций регулятора.

Таким образом, высокий уровень проникновения цифровых технологий и накопленный опыт использования государственных информационных систем, созданные элементы электронного правительства вместе с гибким подходом по оптимизации отраслевого управления предоставляют возможность реализовать принципы хорошего и бережливого госуправления на основе цифровых платформ [3].

***Логистика.*** Мир технологий постоянно развивается и расширяет свои границы. «Умные» технологии не обошли стороной и транспортную логистику. Логистика стала одной из первых отраслей, которая использовала IoT, оценила её преимущества и выявила недостатки. Контроль за движением транспорта, целостность упаковки, ускоренные сроки доставки, оптимизация производства и хранения продукции на складах всегда на первом месте для поставщиков продукции [4]. Именно от этого зависит их прибыль, рост активов и укрепление положения на рынке.

В зависимости от потребности того или иного бизнеса, целей и стратегий компании выделяют несколько направлений, где активно используется технология IoT. Отслеживание транспорта, управление парком и планирование маршрутов, контроль запасов, безопасность на дорогах – приоритетные сферы бизнеса для внедрения IoT [4]. Рассмотрим подробнее каждый аспект, с целью определения актуальности и выявления будущих рисков и проблем в реализации.

*Отслеживание транспорта.* Несомненно, для каждого покупателя важно знать, где находится его посылка и когда она будет доставлена «лично в руки». Вместе с этим, каждый продавец заинтересован в целостности груза, его безопасности и надлежащих условиях перевозки. GPS и RFID-метки успешно справляются с такими задачами как информирование обеих сторон сделки о нахождении и состоянии товара. Наличие и использование таких меток делает совершенно прозрачным путь от продавца к покупателю, что, в свою очередь, увеличивает уровень доверия потребителя.

*Управление парком* позволяет не только оптимизировать процесс транспортировки товара, но и контролировать сотрудников предприятия. Различные датчики GPS позволяют ответственному менеджеру контролировать весь процесс доставки в

режиме реального времени. Датчики могут передавать информацию не только о состоянии груза (температуре, уровне влажности), о месте нахождения водителя, соответствие движения заданному маршруту. Использование такой технологии позволит сократить расходы, связанные с недобросовестным поведением сотрудников при выполнении перевозки.

*Планирование маршрутов* – применение IoT позволит сократить количество потребляемого топлива, грамотно выстроить маршрут движения, снизить риск дорожно-транспортных происшествий. Это заметно снизит затраты на топливо в условиях нынешней экономической ситуации, позволит исключить «пустое» движение автомобиля и непредвиденные простои.

*Контроль запасов и прогнозирование*. В условиях действующих ограничений на мировом рынке, поставщикам и производителям продукции нужно быть начеку и вовремя пополнять запасы комплектующих, сырья, топлива. Соответствующие датчики позволят контролировать как объемы производства, так и остатки продукции на складах. Это позволит спрогнозировать будущий объем производства, закладывать бюджет на приобретение сырья и оплату труда сотрудникам.

Что касается *безопасности на дорогах и транспорте*, то здесь следует выделить опыт зарубежной железнодорожной компании ЮнионПацифик. Компания использует IoT в качестве инструмента по предупреждению поломок, сбоев в работе паровозного состава, отключению энергосетей. Такое использование IoT в прогнозировании происшествий значительно сокращает затраты компании на ремонт оборудования, устранению последствий после аварий, и главным образом, избежать гибели людей на железной дороге.

Вместе с активным использованием технологии IoT, следует помнить и о безопасности данных, которые передаются всеми устройствам в цепи поставок в большом количестве. Для достижения «прозрачности» доставки продукции, необходимо контролировать за тем, чтобы в эту цепочку не вклинились злоумышленники и мошенники.

Блокчейн – вот решение для обеспечения безопасного производства, транспортировки и доставки продукции из рук поставщика в руки покупателя. Все данные, которые будут считываться с датчиком и меток перевозимого груза, и отправляться в базы блокчейна, который не допустит стороннего проникновения. Одновременное внедрение в систему производства IoT и блокчейна обеспечит максимальную надежность и безопасность как для производителя, так и для конечного покупателя [4].

***Заключение.*** Платформенный подход к цифровизации госорганов приобрел устойчивый тренд в мире. Платформенное мышление, в соответствии с установившейся концепцией бережливого правительства, предполагает внедрение инноваций, трансформирующих процессы взаимодействия с гражданами, на основе радикального снижения издержек.

В развитых странах оптимизировали процесс производства и транспортировки продукции, цифровизировали основные сферы жизнедеятельности общества и бизнеса. В современном мире производителям и поставщикам стоит задуматься о скорейшем внедрении цифровизации транспортной логистики, с целью минимизации расходов и увеличения уровня продаж в условиях современной экономической ситуации.

## *Список литературы*

1. *Ibino V., Berardi U., Dangelico R.M. Smart Cities: Definitions, Dimensions, Performance, and Initiatives // Journal of Urban Technology. 2015. Vol. 22(1). P. 1–18.*

2. *Подход к построению подсистем умного города / В. А. Вишняков [и др.] // Технологии передачи и обработки информации : материалы Международного научно-технического семинара, Минск, март-апрель 2023 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: В. Ю. Цветков [и др.]. – Минск, 2023. – С. 45–49.*

*3. Стырин Е.М. Государственные цифровые платформы: от концепта к реализации / Е.М.Стырин, Н.Е.Дмитриева, Л.Х.Синятулина - Вопросы государственного и муниципального управления №4, 2019. – 31с.*

*4. Кобылина Е.В. Интернет вещей в современной транспортной логистике / Е.В.Кобылина, В.М.Черняков - Экономика и бизнес: теория и практика №5-2 (87), 2022 – 58с.*

UDC 330.344.25

# SUBSYSTEMS OF ELECTRONIC GOVERNMENT, LOGISTICS OF «SMART CITY» COMPLEX

Sidorenko S.A., Usevis A.V.

*gr.267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Vishniakou U.A. – Dr. of Sci. (Tech.), Professor at the department of ICT*

**Annotation.** The report presents an analysis of the construction of public digital platforms as the basis for e-government. The efficiency of using the Internet of Things technology in transport logistics is considered. The main elements of the Internet of Things (IoT) implemented in transport logistics are described.

**Keywords:** government digital platforms, public administration, transport logistics, digitalization, Internet of things, blockchain

УДК 330.344.24

# СТРУКТУРА И КОМПОНЕНТЫ ПОДСИСТЕМ ЭНЕРГЕТИКА, ТРАНСПОРТ «УМНОГО ГОРОДА»

*Громов В.А., Кучеров С.В.*
*гр. 267041*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ*

**Аннотация.** В материалах доклада рассматривается структура и компоненты подсистем энергетики и транспорта комплекса «Умный город». Рассматривается переход от традиционной централизованной генерации энергии к децентрализованной. Рассматриваются компоненты подсистемы транспорт комплекса «Умный город», в основе которой находится интеллектуальная транспортная система.

**Ключевые слова:** «Умный город», энергетика, возобновляемые источники энергии, умные счетчики, интеллектуальные сети, CitySys, платформа IoT, интеллектуальная транспортная система.

***Введение.*** Понятие «Умный город» (УГ) можно определить как «…применение информационно-коммуникационных технологий с их воздействием на человеческий капитал/образование, социальный и реляционный капитал и экологические проблемы» [1]. Важными подсистемами УГ являются транспортная и энергетики [2]. Рассмотрим их более подробно.

***Подсистема энергетики.*** Подсистема энергетики играет ключевую роль в обеспечении

энергии для всех умных технологий и инфраструктуры в городе. Выделим основные компоненты этой подсистемы, а также их покажем их взаимосвязь.

Один из компонентов подсистемы энергетики – центральная система управления энергетикой (ЦСУЭ), которая отвечает за координацию и мониторинг энергетических потоков в городе, обеспечивает оптимальное распределение и использование ресурсов энергии. Она осуществляет также управление нагрузками и резервными источниками энергии, чтобы обеспечить стабильность и надежность подсистемы энергетики.

Другим важным компонентом в структуре подсистемы энергетики УГ являются интеллектуальные сети энергоснабжения (ИСЭ). ИСЭ используют передовые технологии связи и управления для обеспечения двусторонней коммуникации между потребителями энергии и сетевыми операторами. Это позволяет оптимизировать расход энергии, снизить потери и обеспечить эффективную интеграцию возобновляемых источников энергии.

Ещё одним компонентом является распределенная генерация и хранение энергии. В УГ стремятся увеличить долю распределенной генерации энергии и использовать различные источники, включая солнечную и ветровую энергию. Это позволяет снизить зависимость от традиционных источников энергии и уменьшить выбросы парниковых газов. Системы хранения энергии, такие как аккумуляторы и батареи, используются для сохранения избыточной энергии и обеспечения устойчивости снабжения в периоды пиковой нагрузки.

Умные счетчики позволяют потребителям отслеживать и контролировать свое энергопотребление в режиме реального времени. Они также обеспечивают возможность динамического тарифицирования, что способствует энергоэффективности и стимулирует потребителей к снижению своего энергопотребления.

«Smart grid» – концепция для модернизации энергетических систем путем интегрирования электрической и информационной технологий. Интеграция охватывает всю систему, начиная с производства, передачи и распределения до потребления (рис. 1). На низковольтном уровне такое решение часто называется «Microgrid».

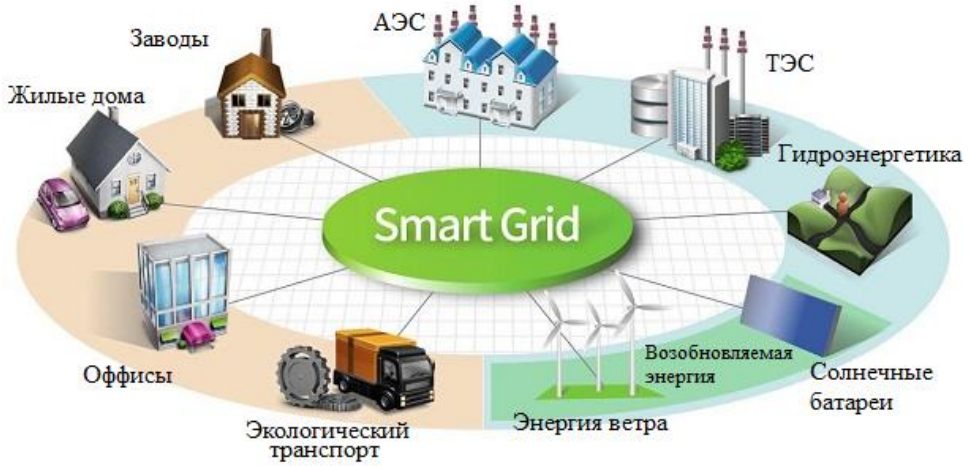



Рис. 1 – Графическое изображение топологии «умных» сетей.

С помощью распределенного интеллекта и информационно-коммуникационной технологии (ICT), а также распределенных интеллектуальных устройств (IUD) можно увеличить эффективность электроснабжения в местных электросетях или даже на уровне магистральной сети. Состояние подсистемы постоянно анализируется, производится контроль в онлайн-режиме на основании полученной информации. Подсистема оборудована управляемыми интеллектуальными устройствами, которые автоматически поддерживают баланс между поставкой и потреблением для обеспечения высокого качества электроэнергии и улучшения надежности и работоспособности.

Интеллектуальным сетям присущи следующие атрибуты [3]:

– способность к самовосстановлению после сбоев в подаче электроэнергии;
– возможность активного участия в работе сети потребителей;
– устойчивость сети к физическому и виртуальному вмешательству злоумышленников;
– обеспечение требуемого качества передаваемой электроэнергии;
– обеспечение синхронной работы источников генерации и узлов хранения электроэнергии;
– появление новых высокотехнологичных продуктов;
– повышение эффективности работы энергосистемы в целом.

Подсистему «Smart Grid» можно описать такими аспектами функционирования [4]:

*1. Гибкость, с*еть подстраивается под нужды потребителей электроэнергии.

*2. Доступность,* сеть доступна для новых пользователей.

*3. Надёжность,* сеть гарантирует защищённость и качество электроэнергии.

*4. Экономичность, э*ффективное управление и регулирование функционалом сети.

Пока электрические сети строятся по иерархическому принципу (генератор, магистральные линии, далее распределительные сети, городские сети и потребители). В большинстве случаев они состоят из радиальных линий с односторонним потоком энергии. Лишь в некоторых случаях электрические сети закольцованы. Присутствуют системы релейной защиты и диспетчерского контроля.

Подсистема «Smart Grid» предлагает новый принцип построения, в основе которой генератор, проводящая конструкция (линия) и потребитель, но он участвует в генерации и перераспределении энергии. Дефицит и стоимость органических видов топлива стимулирует развитие альтернативных источников электроэнергии. Генерирующие мощности в умной системе электроснабжения будут больше распределенными, чем концентрированными, как сейчас (рис. 2). Особенностью таких источников является их относительно небольшая мощность и нестабильность параметров генерируемой мощности. Очевидно, что для стабилизации параметров таких источников и их автоматической синхронизации с сетью необходимо использовать интеллектуальные управляющие устройства.

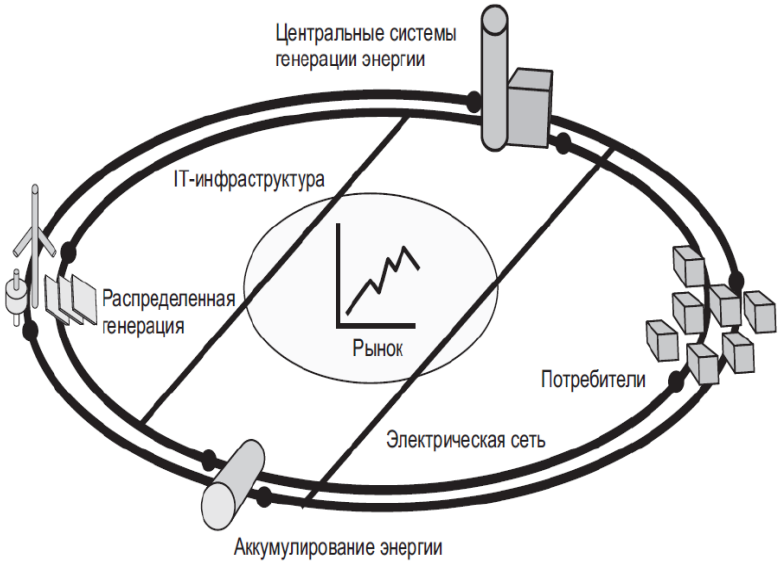



Рис. 2 – Наглядное изображение взаимосвязей в «умных» сетях

Будущая сеть уже не будет иметь иерархическую структуру и крупные потребители будут в ней перемешаны с большим количеством относительно маломощных источников энергии, а также и мощных единичных станций, регуляторов напряжения, компенсаторов реактивной мощности (рис. 3).

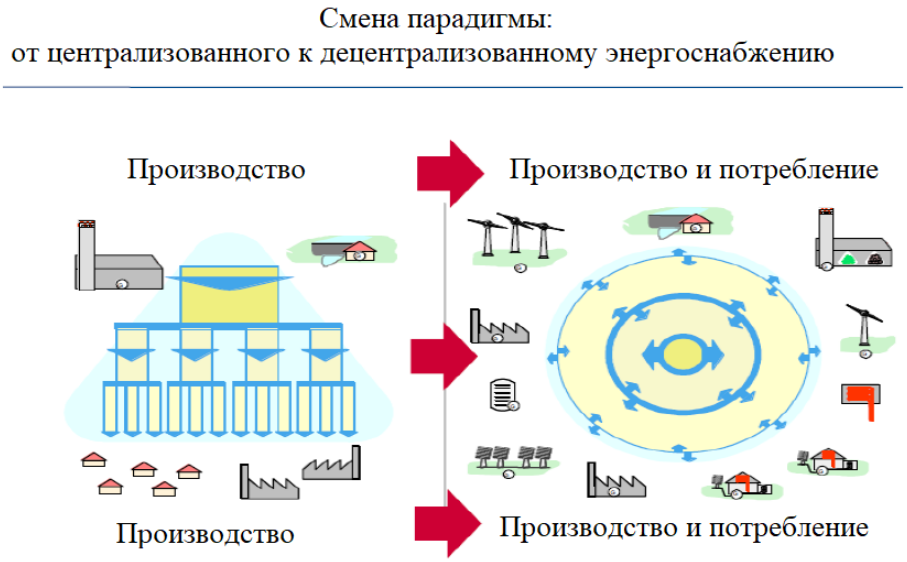



Рис. 3 – Изображение перехода от традиционной централизованной генерации к децентрализованной с потреблением

Перетоки мощности по такой сети не будут строго детерминированными. Такая сложная неструктурированная сеть должна иметь интеллектуальную управляющую систему, согласовывающую между собой работу всех многочисленных компонентов сети. Для этого все компоненты сети должны «общаться» друг с другом и с управляющим центром по специальным коммуникационным сетям.

Для надежного функционирования такой сложной подсистемы, количество отдельных многофункциональных модулей, обрабатывающих информацию, должно быть сокращено до минимума. Информация от многочисленных компонентов «Smart Grid» должна поступать по сети на мощные серверы, обрабатываться ими, и пересылаться по сети на исполнительные элементы. Вся основная функциональность системы должна обеспечиваться на аппаратно-программном уровне.

В концепции «Smart Grid» релейная защита должна быть совмещена с функциями информационно-измерительной системы. Причиной является то, что, микропроцессорные устройства релейной защиты производят измерения токов, напряжений в векторной форме. Они записывают и накапливают информацию об аварийных режимах и собственных срабатываниях. Эта информация может быть напрямую использована в будущих контрольно-информационно-измерительных узлах «Smart Grid», в которых релейной защите будут приданы дополнительные функции измерений, мониторинга и диагностики электрооборудования энергосистем. Идея «Smart Grid» реально стимулируется со стороны органов власти развитых стран. Она пока несамоокупаема и не будет самоокупаемой в ближайшем будущем. Однако таким путем, форсируется развитие «умных» технологий.

Транспортная подсистема. ***Важное значение в составе УГ отдается транспорту, подсистемы транспорта и энергетики тесно связаны друг с другом. Без развитой энергетической структуры формирование структуры умного транспорта было бы невозможно. Формирование подсистемы транспорта УГ основывается на интеллектуальной транспортной системе (ИТС) [5]. Это подразумевает интеграцию оперативного управления всеми видами транспорта и способностью реакции на события в режиме реального времени. Большое значение имеет то, что транспортная подсистема является составной частью всей системы «Умный город», и поэтому должна располагать доступными для пользователей интерфейсами.***

Для организации такой подсистемы в УГ должен быть создан единый центр управления ИТС, куда в онлайн-режиме будут передаваться данные с детекторов мониторинга транспортных потоков и дорожная обстановка с фото и видеокамер. Созданная система обязательно должна фиксировать скорость потока, наличие и количество автомобилей и общественного транспорта, учитывать погодные условия и состояние трассы. При возникновении ДТП система должна

предупреждать всех участников движения о затруднениях движения на дороге и подсказывать пути объезда. Режимы работы светофоров должны меняться в зависимости от загруженности соседних перекрестков. При действии описанной подсистемы появится возможность координировать потоки в случае заторов, отменять непопулярные маршруты и назначать новые.

Сформированная ИТС на дорогах представляет собой целый комплекс функционального оборудования, которое осуществляет сбор информации, управление транспортным потоком и информирование участников дорожного движения. Ожидаемого результата от системы можно достичь только при условии оснащения системы необходимым оборудованием и его комплексной работе можно добиться существенного улучшения ситуации на дорогах в мегаполисах [5].

Благодаря комплексному взаимодействию система позволяет одному узлу управлять десятью или даже сотнями тысяч устройств. Платформа IoT умного города содержит настраиваемые виджеты (рис. 4), механизм обработки правил и систему подключаемых модулей, которые фактически делают платформу расширяемой.

Рис. 4 – Платформа IoT настраиваемые виджеты

Общий поток данных (BigData) в умном городе обеспечивается множеством различных датчиков, отслеживающих самые разные параметры: датчики движения, датчики дорожного движения, детекторы заполнения парковочных мест, погодные станции, датчики управления отходами, датчики шума, камеры CCTV и кнопки экстренного вызова.

Представленная на рис. 5 платформа УГ CitySys представляет собой открытую платформу, объединяющую в себе множество приложений для организации подсистем. Сбор данных, передача и оценка выполняются комплексной системой управления CitySys, реализованной на платформе ThingsBoard IoT в рамках стандарта открытого исходного кода (OPC) [6].

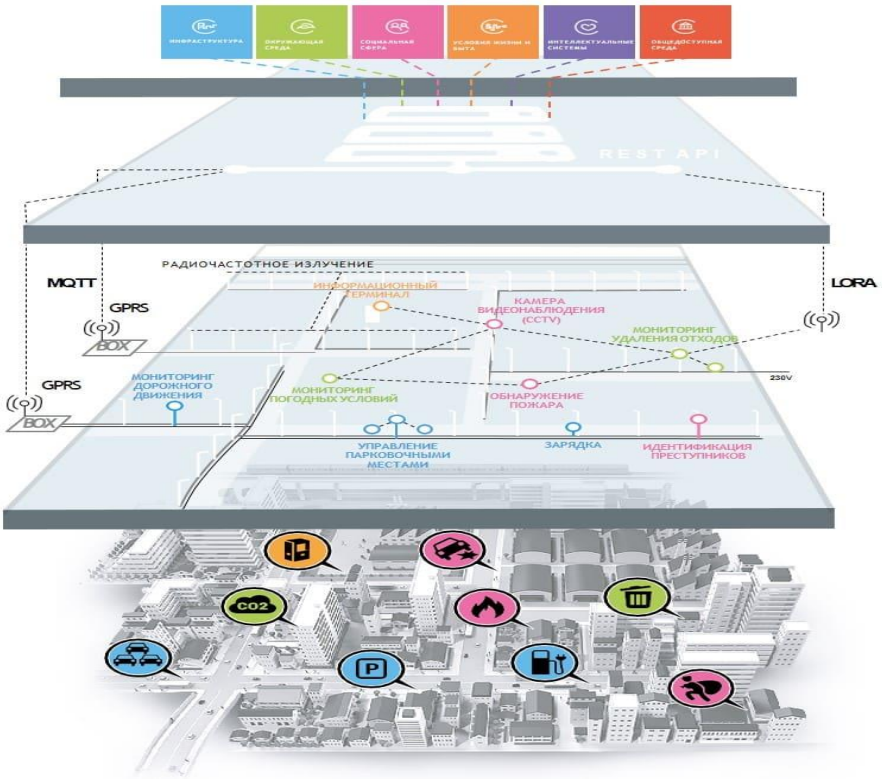



Рис. 5 – Платформа Умный город CitySys

Взаимодействие информации данной платформы с открытым исходным кодом – это серия сертификаций и спецификаций от разработчиков программного обеспечения, формирующих интерфейс между пользователями и серверами, осуществляя доступ к данным в реальном времени, постоянный мониторинг аварийных сигналов и событий, доступ к архивным данным и другие области применения. Его программные и аппаратные компоненты осуществляют прямую связь через стандартные интерфейсы и протоколы: Powerline, Bluetooth, KNX, Z-Wawe, ModBus RTU/TCP, BACnet IP, EnOcean, DMX, M-Bus, GSM.

IoT платформа CitySys имеет структуру с горизонтальной масштабируемостью и создается с использованием преимущественно технологий с открытым исходным кодом [6]. Благодаря схожести каждого узла кластера, платформа является очень надежной. Надежность и высокая эффективность являются действительно самыми важными преимуществами платформы.

CitySys позволяет напрямую управлять освещением различными способами [6]:

– использование удаленной коммутации силовых контакторов за счет функций системных кнопок;

– использование автоматической коммутации силовых контакторов за счет предустановленных профилей коммутации;

– применение профилей регулирования освещения для автоматической регулировки с использованием «умных» фонарей;

– ручная регулировка фонарей, которая возможна за счет функций системных кнопок, а также регулировка отдельных фонарей, групп фонарей или выбранных фонарей с помощью карты.

Система управления CitySys предоставляет множество функций, а также отображает состояние каждого устройства, управляемого платформой. Пользователь может просмотреть перечень электрических распределительных коробок со значениями их токов, отфильтровать и отобразить необходимые сведения. Особенно полезен информационный компонент о событиях и повреждениях, предлагающий быстрый просмотр записей о потреблении электроэнергии.

***Заключение.*** В условиях новых вызовов энергетика находится на этапе смены структурно-

технологической парадигмы. Переход к новым структурам в виде интегрированных интеллектуальных энергетических систем, объединяющих самоорганизующиеся системы электро-, тепло-, хладо-, газоснабжения и др., построенных по мультиагентному принципу обеспечит новый импульс развития энергетики, обеспечивающий удовлетворение возрастающих требований потребителей.

В связи с увеличением количества транспортных средств в мегаполисах остро встает проблема средней скорости движения и загруженности дорог. Многие города мира не первый год стоят в пробках, но лишь немногие их них смогли развязать этот «транспортный узел». Не всегда есть возможность построить новую дорогу или расширить существующую магистраль, поэтому решать проблему загруженных дорог необходимо с помощью современных технологий. Интеллектуальные транспортные системы призваны помочь в этом вопросе за счет эффективного управления светофорными объектами, средствами регулирования и мониторинга дорожного трафика, системами информирования участников движения о ситуации на дорогах и т. д.

### *Список литературы*

1. *Ibino V., Berardi U., Dangelico R.M. Smart Cities: Definitions, Dimensions, Performance, and Initiatives // Journal of Urban Technology. 2015. Vol. 22(1). P. 1–18.*

2. *Подход к построению подсистем умного города / В. А. Вишняков [и др.] // Технологии передачи и обработки информации : материалы Международного научно-технического семинара, Минск, март-апрель 2023 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: В. Ю. Цветков [и др.]. – Минск, 2023. – С. 45–49.*

3. *Куанашканов Ш. Различные подходы к организации технологии «SMART GRID» [Электронный ресурс]. – Режим доступа: https://kazatu.edu.kz/assets/i/science/sf11_energo_124.pdf - Дата доступа: 05.12.2023.*

4. *«Smart Grid» - новая идея или логичное развитие систем электроснабжения? [Электронный ресурс]. – Режим доступа: http://cons-systems.ru/smart-grid-novaya-ideya-ili-logichnoe-razvitie-sistem - Дата доступа: 04.12.2023.*

5. *Центр 2М. Интеллектуальные транспортные системы [Электронный ресурс]. - Режим доступа: https://center2m.ru/intellektualnye-transportnye-sistemy - Дата доступа: 21.02.2023.*

6. *INTELVISION. IoT платформа Умный город CitySys [Электронный ресурс]. - Режим доступа: https://www.intelvision.ru/products/platforma- umnyi- gorod - Дата доступа: 21.02.2023.*

UDC 330.344.24

## STRUCTURE AND COMPONENTS OF THE «SMART CITY» ENERGY, TRANSPORT SUBSYSTEMS

*Gromov U.A.,Kucherov S.V.*
*gr. 267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*
*Vishniakou U.A. – Dr. of Sci. (Tech.), professor at the department of ICT*

**Annotation**. The materials of the report consider the structure and components of the energy and transport subsystems of the «Smart City» complex. The transition from traditional centralized energy generation to decentralized is considered. The components of the transport subsystem of "Smart City" are considered, which is based on an intelligent transport system.

**Keywords:** «Smart City», energy, renewable energy sources, smart meters, smart grids, CitySys, IoT platform, intelligent transport system.

УДК 004.738

## МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЯХ. АНАЛИЗ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ OLSR И AODV

*Позняк А. А., Толейко К. Г.*
*гр. 163001*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*
*Научный руководитель: Полуян Т. В. – ассистент кафедры ИКТ*

**Аннотация.** В представленной статье описывается проведенный анализ протоколов маршрутизации OLSR и AODV, используемых в самоорганизующейся сети MANET, при помощи симулятора NS-3.

**Ключевые слова:** самоорганизующаяся сеть, MANET, OLSR, AODV, NS-3.

***Введение.*** В современном мире беспроводные сети становятся все более распространенными и востребованными, особенно в контексте самоорганизующихся сетей (MANET). Самоорганизующиеся сети представляют собой сети, в которых узлы могут свободно перемещаться и автоматически формировать соединения между собой без централизованного управления. Такие сети находят применение в различных областях, таких как военные операции, аварийные ситуации и мобильные коммуникации.

Одним из ключевых аспектов в самоорганизующихся сетях является маршрутизация, то есть определение маршрутов передачи данных между узлами сети. В беспроводных MANET-сетях маршрутизация является особенно сложной задачей из-за динамической природы сети, изменения топологии и ограниченной пропускной способности канала связи.

Для анализа и сравнения протоколов маршрутизации в MANET часто используются симуляторы, такие как NS-3 (Network Simulator 3). NS-3 предоставляет среду для моделирования и симуляции различных сетевых протоколов и сценариев, что позволяет исследователям изучать и оценивать производительность протоколов в реалистичных условиях.

Существует множество протоколов маршрутизации, разработанных специально для беспроводных MANET-сетей. Два из наиболее распространенных протоколов маршрутизации в MANET-сетях – OLSR (Optimized Link State Routing) и AODV (Ad hoc On-Demand Distance Vector) – заслуживают особого внимания и анализа.

***Основная часть.*** В данной работе был использован файл manet-routing-compare.cc на C++, который позволяет сравнить производительность протоколов маршрутизации в беспроводных сетях MANET. Программа генерирует топологию сети, реализует различные протоколы маршрутизации и измеряет их производительность. Результаты сравнения протоколов выводятся в отчете.

В результате моделирования были получены данные о SimulationSecond, ReceiveRate, PacketsReceived, NumberOfSinks, RoutingProtocol, TransmissionPower.

При увеличении уровня TransmitPower узлы сети могут передавать сигнал на большее расстояние, что влияет на ReceiveRate других узлов. Если TransmitPower недостаточно высок, то узлы могут не получать пакеты от удаленных источников из-за плохого качества сигнала. Однако чрезмерно высокий уровень TransmitPower может вызывать интерференцию с другими узлами и привести к потере пакетов из-за помех.

Таким образом, оптимальный уровень TransmitPower соответствует максимальному ReceiveRate для сети, обеспечивая достаточное покрытие и качество сигнала для всех узлов.

Зависимость PacketsReceived (количество полученных пакетов) от Nodes (количества узлов) в сети с протоколом AODV может быть сложной и зависит от нескольких факторов:

1 Трафик сети: чем больше узлов в сети, тем больше пакетов будет передаваться между ними. Однако с увеличением числа узлов могут возникать проблемы с коллизиями, перегрузкой сети и ухудшением производительности.

2 Эффективность маршрутизации: протокол AODV построен на принципах On-Demand маршрутизации, что означает, что маршруты устанавливаются только при необходимости. С увеличением числа узлов в сети может возникать сложность в поиске и поддержании оптимальных маршрутов, что может отразиться на количестве полученных пакетов.

3 Ресурсные ограничения: увеличение числа узлов в сети может привести к увеличению конкуренции за ресурсы, такие как пропускная способность и энергия. Это может сказаться на стабильности и надежности маршрутизации, что в свою очередь повлияет на количество полученных пакетов.

AODV является протоколом на основе запросов, который инициирует запросы маршрута

только при необходимости. Как следствие, количество полученных пакетов может быть невелико в сравнении с другими протоколами, такими как OLSR. Однако скорость приема может быть высокой, когда происходит активный обмен маршрутной информацией.

OLSR, с другой стороны, использует алгоритм состояния ссылок и поддерживает активный обмен этой информацией между узлами сети. Из-за этого OLSR может иметь большое количество полученных пакетов и обмен пакетами, что может привести к более высокой скорости приема.

Однако в ходе проведенного нами моделирования было замечено, что протокол AODV эффективнее протокола OLSR. Это возможно при следующих условиях:

1 Динамическая сетевая топология: AODV позволяет находить кратчайший путь между узлами только при необходимости, что делает его более эффективным в динамических сетевых топологиях, где состояние связей между узлами часто меняется.

2 Ограниченные ресурсы: AODV имеет меньшую нагрузку на сеть и использует меньше ресурсов, чем OLSR, что делает его более подходящим для беспроводных сетей с ограниченными ресурсами.

3 Необходимость быстрого обнаружения маршрутов: AODV выигрывает в ситуациях, когда требуется быстрое обнаружение маршрутов из-за частых изменений в топологии сети.

***Заключение.*** Результаты исследования показали, что оба протокола маршрутизации имеют свои преимущества и недостатки. Дальнейшие исследования в этой области могут включать анализ других протоколов маршрутизации, учет влияния различных факторов на производительность сети MANET, разработку новых алгоритмов маршрутизации и улучшение существующих протоколов. Это позволит создать более эффективные и надежные сети MANET, способные эффективно функционировать в различных условиях и сценариях применения.

***Список литературы***

*1. ns-3 Documentation [Электронный ресурс]. – Режим доступа: https://www.nsnam.org/docs/release/3.19/doxygen/index.html.*

*2. Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava An Overview of AODV Routing Protocol [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/profile/Gaurav-Sharma-73/publication/252068339_An_Overview_of_AODV_Routing_Protocol/links/56402a9d08ae45b5d28d37b7/An-Overview-of-AODV-Routing-Protocol.pdf.*

*3. Clausen, T. Jacquet, P. Optimized Link State Routing Protocol (OLSR) [Электронный ресурс] – 2003. – Режим доступа: https://www.rfc-editor.org/rfc/rfc3626.*

UDC 004.738

## ROUTING IN WIRELESS SELF-ORGANIZING NETWORKS. ANALYSIS OF OLSR AND AODV ROUTING PROTOCOLS

*Pazniak A. A., Taleika K. G.*
*gr. 163001*
*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*
*Paluyan T. V. – assistant at the department of ICT*

**Annotation.** The presented report analyzes the OLSR and AODV routing protocols used in the self-organizing MANET network using the NS-3 simulator.

**Keywords:** self-organizing network, MANET, OLSR, AODV, NS-3.

## Модели угроз локальной сети в учреждении образования

*Силич С.С.*
*гр.267041*
*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Шевчук О.Г. – кандидат технических наук, доцент кафедры ИКТ*

**Аннотация.** Сегодня привычным инструментом коммуникаций являются компьютерные сети, что вызывает необходимость обеспечения их безопасности, здесь рассматриваются возможные угрозы и средства обеспечения безопасности локальных сетей.

**Ключевые слова:** локальная сеть, безопасность, угроза, программное обеспечение.

***Введение.*** Настоящее время характеризуется большим количеством числа компьютеров, связанные между собой с помощью особых каналов, предназначенных для распространения информации и

Одной из основных проблем в ЛС является обеспечение их безопасности. Но, необходимо понимать, что безопасность представляет собой совокупность мер технического, организационного и административного плана, которым требуется регулярная проверка. Не менее важно, что в систему безопасности всегда включены и люди. Поэтому сеть нельзя считать безопасной при отсутствии доверияк персоналу, который с ней работает. Кроме того, абсолютная безопасность локальной сети недостижимав принципе, поскольку даже если к ней допущено крайне ограниченное число доверенных пользователей, существует вероятность, что и среди них отыщется «слабое звено».[1]

***Основная часть.*** Угрозы ЛС можно разделить следующим образом:

Техническая угроза:

- Ошибки в программном обеспечении (ПО), чем сложнее ПО, тем больше вероятность обнаружения ошибок. Большая часть не представляет никакой опасности, но некоторые могут привести к серьёзным последствиям. Действующий способ предотвращению возникших проблем является своевременная установка обновления ПО.

- Различные DoS- и DDoS-атаки. Denial Of Service (отказ в обслуживании) — особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. DoS-атака (Denial of Service) — попытка нарушения или снижения доступности ресурса, как правило, сайта, сетевого сервиса или софта. Задача в том, чтобы перегрузить целевую систему или сделать ее недоступной, приводя к отказу в обслуживании.

- Компьютерные вирусы, черви, троянские кони. Они используют для своего распространения электронную почту, уязвимость в ПО или их совокупность, выполняют функцию похищения информации и использования заряженной системы для своего распространения.

- Технические средства съема информации. Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т. д.

- Анализатор трафика, или сниффер (от англ. to sniff — нюхать) — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Человеческий фактор:

- Уволенные или недовольные сотрудники.
- Промышленный шпионаж
- Халатность.
- Низкая квалификация.

Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим. [2]

***Заключение.*** Таким образом, в настоящее время важно быть уверенным в защищённости локальной сети и вовремя выявить возможные угрозы. Знание которых совместно с уязвимыми местами защиты, которые эти угрозы обычно эксплуатируют, необходимо для выбора наиболее экономичных средств обеспечениябезопасности.

***Список литературы***

1. *Орловская Л.А., Поначугин Л.А., Поначугин А.В. Локальные вычислительные сети // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XLII междунар. Студ. Науч.-прак. Конф. – 2016. №5(41). URL:https://sibac.info/archive/techenic/5(41).pdf (дата обращения: 20.004.2018).*
2. *Абраров Р. Д., Курязов Д.А. Информационная безопасность в компьютерных сетях // Молодой ученый. – 2016. - №9.5. – С. 10-12.- URL:https:// moluch.ru/archive/113/29719/ (дата обращения: 20.004.2018).*

УДК 004.75

# МЕТОДЫ РАЗВЕРТЫВАНИЯ МИКРОСЕРВИСНЫХ ПРИЛОЖЕНИЙ В КЛАСТЕРЕ KUBERNETES

*Яцеивч К.В.*

*гр.367041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Кореневский С.А. – кандидат технических наук, доцент кафедры ИКТ*

**Аннотация.** В материалах доклада рассматриваются методы развертывания микросервисных приложений, предоставляя комлексное понимание доступых инструментов и подходов, адаптированных под различные потребности разработки и управления. Использование перечисленных методов развертывания предоставит гибкость и масштабируемость микросервисных приложений, автоматизацию процессов, а также централизованное управление развертыванием.

**Ключевые слова:** Kubernetes, helm, kubectl, gitops

***Введение.*** В современной разработке программного обеспечения микросервисная архитектура зарекомендовала себя как мощный подход к созданию масштабируемых, гибких и надежных систем. Эта модель предполагает разделение приложения на набор независимых сервисов, каждый из которых выполняет уникальную функцию и общается с другими через легковесные протоколы. Для управления жизненным циклом таких микросервисов часто применяется Kubernetes — передовая платформа для автоматизации развертывания, масштабирования и управления контейнеризированными приложениями[1].

Развертывание микросервисов в kubernetes может быть непростой задачей, учитывая динамичность и сложность современных приложений. Однако, благодаря широкому ассортименту инструментов и методик, разработчики могут выбрать подход, наиболее подходящий для их конкретных требований и предпочтений. От прямого управления ресурсами с помощью kubectl и манифестов YAML до более высокоуровневых абстракций, таких как Helm чарты, GitOps практики, операторы Kubernetes и Kustomize — каждый из этих методов предлагает свои уникальные преимущества и может быть использован в различных сценариях разработки и эксплуатации.

Эффективное использование этих инструментов и подходов позволяет командам достигать высокого уровня автоматизации, улучшать надежность и упрощать управление сложными системами, что в конечном итоге приводит к более быстрой доставке ценности для конечных пользователей.

***Основная часть.*** Одним из первых методов развертывания микросервисных приложений является командный интерфейс kubectl и YAML манифесты. Манифесты описывают желаемое состояние ресурсов в кластере. Это метод предоставляет разработчикам прямой и гранулярный контроль над компонентами системы, позволяя точно настраивать поведение и параметры каждого сервиса. К достоинствам этого метода можно отнести следующее: высокий уровень контроля и прозрачность конфигураций. Но у

этого метода есть и недостатки: управление большим числом манифестом и их зависимостями может быть трудоемким, требуется детальное понимание спецификаций ресурсов kubernetes.

Следующий метод развертывания — helm. Это пакетный менеджер для kubernetes, который значительно упрощает процесс развертывания приложений, предоставляя удобные шаблоны, который инкапсулируют набор ресурсов и их зависимости. Этот метод имеет следующие преимущества: стандартизация развертывания сложных приложений за счет шаблонов, версионирование и управление зависимостями приложений. Однако для использования этого метода необходимо освоение синтаксиса и структуры шаблонов helm.

Kubernetes operators — пользовательские котроллеры для наблюдения за состоянием ресурсов и автоматического выполнения действий для достижения желаемого результата состояний приложений. Операторы расширяют функционал кластера, позволяя разработчикам кодировать и автоматизировать задачи управления приложений. Данный метод предоставляет преимущества: автоматизация управления и обслуживания приложений, включая развертывание, обновление и восстановление. Процесс разработки специфичного оператора может быть сложным и занять достаточного времени.

Наиболее популярным методом развертывания является gitops подход. Эта методология, которая использует Git как источник истины для декларативного описания и управления инфраструктурой и приложениями. Инструменты, поддерживающие GitOps, такие как Argo CD, автоматически применяют изменения, сделанные в Git-репозитории, к кластеру Kubernetes. Этот метод выделяется данными достоинствами: обеспечение отслеживания изменений и возможность возврата к предыдущим состояниям приожений.

***Заключение.*** Выбор метода развертывания микросервисных приложений в кластере kubernetes зависит от множества факторов, включая специфику проекта, требования к масштабируемости и доступности, уровень знаний команды и предпочтительные рабочие процессы. Каждый из рассмотренных методов — использование kubectl с YAML-манифестами, helm, kubernetes operators и gitops — имеет свои преимущества и может быть наиболее эффективен в определенных сценариях.

Прямое использование kubectl с YAML-манифестами предлагает максимальный контроль и прозрачность, что делает его идеальным для обучения и экспериментов. Helm, как менеджер пакетов, значительно упрощает развертывание и управление сложными приложениями, предоставляя мощные средства для управления версиями и зависимостями. Kubernetes operators поднимают автоматизацию на новый уровень, позволяя внедрять сложные операции управления и обслуживания приложений непосредственно в кластер. Наконец, GitOps предлагает целостный подход к управлению инфраструктурой и приложениями, обеспечивая консистентность, отказоустойчивость и удобство в управлении через код.

В конечном счете, успешное внедрение микросервисов в Kubernetes требует глубокого понимания как самих методов развертывания, так и уникальных требований проекта. Иногда наиболее эффективным решением может стать комбинация нескольких подходов, например, использование helm для управления стандартными компонентами и Kubernetes Operators для специализированных микросервисов.

### ***Список литературы***

*1. The Book of Kubernetes: A Complete Guide to Container Orchestration. / Hohn Alan – No Starch Press 2022. – 430 c.*
*2. Kubernetes: Up and Running. / Brendan Burns, Joe Beda, Kelsey Hightower. – O'Reilly Media, Inc., Sebastopol 2019. – 277 c.*

UDC 004.75

**METHODS FOR DEPLOYING MICROSERVICE APPLICATIONS IN A KUBERNETES CLUSTER**

*Yatsevich K.V.*

*gr.367041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Korenevksy S.A. – Ph. D*

**Annotation**. The report examines methods for deploying microservice applications, providing a comprehensive understanding of available tools and approaches tailored to different development and management needs. Using these deployment methods will provide flexibility and scalability for microservice applications, process automation, and centralized deployment management.

**Keywords:** Kubernetes, helm, kubectl, gitops

# Анализ инструментов защиты данных пользователей на примере игровых компаний

*Бродович Б.Е.*

*гр.160801*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Рабцевич В.В. – старший преподаватель каф.ИКТ*

**Аннотация.** В материалах доклада рассматриваются проблемы безопасности игровых веб-приложений. Был проведен анализ существующих решений для защиты с учетом существующих видов атак.

**Ключевые слова:** кибербезопасность, игровое приложение, веб-приложение

***Введение.*** Создателям цифровых видеоигр постоянно приходится сталкиваться со взломом своих продуктов, который базируется на взаимодействии с исходным кодом (например, путем реверсного инжиниринга) либо других составляющих. При этом прослеживается закономерность между популярностью товара компании и его вероятностью быть взломанными [1].

***Основная часть.***

Проведем анализ различных атак на пользовательскую базу данных. Согласно принципу Керкгоффса [2] при оценке надёжности необходимо предполагать, что злоумышленник знает об используемой системе шифрования всё, кроме ключей. В данном случае ключами являются пароли пользователей, которые хранятся в виде хешей, а сама СУБД (система управления базами данных), соответственно, была взломана и целиком попала к злоумышленнику.

Самый простой метод взлома это подбор пароля. Существует два подхода: это атака по словарю и brute-force атака (простой лексикографический перебор всех возможных вариантов). Процесс подбора пароля описанными методами показан ниже на рис. 1. От данных атак сложно защититься, но есть способы сделать их менее эффективными.

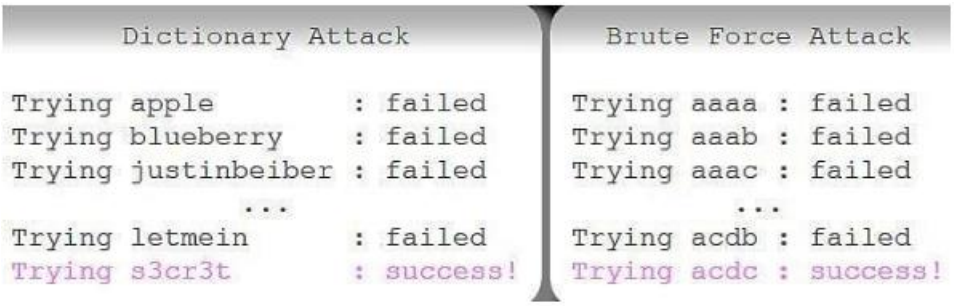



Рисунок.1. Взлом пароля с помощью атаки по словарю и brute-force атаки

Метод взлома через таблицу заключается в создании специальной таблицы, где заранее вычислены значения хешей для различных паролей. При взломе хеша происходит поиск соответствующего ему исходного пароля в этой таблице.

Обратный поиск по таблице — это эффективный метод взлома при больших объемах БД. Он позволяет злоумышленнику применять перебор паролей одновременно, создавая таблицу для поиска пользователей с соответствующими значениями хеша. Эффективность увеличивается, если несколько пользователей имеют одинаковые пароли.

Последний способ взлома – это использование так называемых радужных таблиц. Радужные таблицы – это вариант обычных таблиц, содержащих цепочки данных, полученные через хеширование и редукцию. Они требуют меньше памяти и могут взламывать пароли до восьми символов, зашифрованные с помощью MD5.

**Анализ объекта защиты и выбор инструментов для обеспечения безопасности**

Остановимся подробнее на особенностях данных, которые необходимо шифровать при разработке многопользовательской игры. В БД при регистрации нового пользователя заносится новый объект, содержащий хеш пароля, так называемую соль (затравку для функции хеширования) и токен пользователя – еще один хеш. Основная информация о пользователе — это логин, электронный адрес почты, хэш пароля (элемент passwordHash), соль хеша пароля (элемент r) и токен (элемент token).

Сейчас существует множество алгоритмов хеширования данных, каждый из которых имеет свои плюсы и минусы. Наиболее популярные из них:

1. **SHA-256 (Secure Hash Algorithm 256-bit):** этот алгоритм является наиболее часто используемым. Он создает 256-битное хеш-значение фиксированной длины и известен своей безопасностью и скоростью.
2. **SHA-1 (Secure Hash Algorithm 1):** SHA-1 также широко применяется, но стоит отметить, что он менее безопасен, так как использует 160-битное хеш-значение.
3. **MD5 (Message Digest Algorithm 5):** MD5 является одним из наиболее известных алгоритмов хеширования и широко используется для проверки целостности данных.

Для обеспечения безопасности при использовании функций хеширования рекомендуется добавлять затравку (salt), которая представляет собой случайную строку, добавляемую перед или после хешируемого сообщения (порядок не важен). Применение затравки обеспечивает ряд преимуществ, таких как: защита от атак по таблицам, усложнение перебора, повышение криптостойкости.

Таким образом, злоумышленник не может предугадать, какая затравка будет использована в каждом хеше пароля. Это влечет за собой невозможность построения радужных и иных таблиц для комбинаций всех возможных паролей со всеми возможными

затравками. Стоит также отметить, что затравку нет смысла шифровать так как это усложнит процесс аутентификации пользователей с точки зрения приложения.

Для повышения уровня защищенности при использовании пары «логин - пароль» в игровых приложениях, было решено создавать для каждого пользователя по токену. Токен в данном конкретном случае – это зашифрованная пара: логин и хеш пароля.

При регистрации пользователю выдается специальный хеш – секретный API ключ, который не следует разглашать. Этот ключ используется в каждом запросе к сервису, таким образом идентифицируя клиента.

Для обеспечения безопасности RESTful запросов используется защищенное соединение и передача токена вместо «логина-хеша пароля». Токен создается однажды: при регистрации и не меняется при смене пароля. Для его создания применяются алгоритмы с техникой «key stretching», увеличивающей криптостойкость даже слабых паролей.

Формирование политики безопасности:

1) **Минимальная длина пароля:** важно ограничивать минимальную длину пароля. В сетевых приложениях, включая игровые, слишком короткие пароли не обеспечивают надежную защиту. Обычно рекомендуется устанавливать минимум в 8 символов, что является разумным компромиссом между безопасностью и удобством для пользователей.

2) **Политика парольной защиты**:

**а) Объединение ошибок в логине и пароле**: при попытках авторизации следует рассматривать ошибку в логине и ошибку в пароле как единую пару. Это предотвращает перебор логинов и паролей через интерфейс.

**б) Восстановление пароля через временные токены**: при запросе на восстановление пароля пользователю следует предоставить ссылку с уникальным временным токеном. Токен должен быть привязан к конкретному аккаунту, чтобы злоумышленник не мог изменить чужой пароль. Время действия токена должно быть ограничено (например, 15 минутами).

**в) Аннулирование токена после успешной авторизации**: когда пользователь восстановил пароль, токен должен быть аннулирован. Это предотвращает его повторное использование.

**г) Не отправлять новый пароль по почте**: никогда не следует отправлять новый пароль пользователю по электронной почте. Вместо этого используйте временные токены для восстановления пароля.

**д) Использование новой затравки для хеширования нового пароля**: при изменении пароля рекомендуется обновлять затравку для хеширования. Это повышает безопасность хранения паролей в базе данных.

***Заключение.*** Таким образом, в статье рассматриваются проблемы повышения защищенности игрового веб-приложения с учетом различных видов атак на пользовательскую БД и проведен анализ существующих решений для обеспечения надежной парольной защиты.

## *Список литературы*

*1. Информационная безопасность в игровой индустрии [Электронный ресурс].. – Режим доступа : https://habr.com/ru/articles/695912/. – Дата доступа : 27.10.2022.*

*2. Н.Е.Губенко, А.В.Сирант Сравнительный анализ и выбор алгоритмов хеширования для организации парольной защиты игровых приложений /Н.Е.Губенко, А.В.Сирант. – Донецк: ДНТУ.*

# Analysis of user data protection tools using the example of gaming companies

*Brodovich B.E.*

*gr.160801*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Rabcevich V.V.*

**Annotation**. The materials of the report address the security issues of a gaming web application. An analysis of existing security solutions was carried out, taking into account existing types of attacks.

**Keywords:** cybersecurity, gaming application, web application

UDC 004.048

## Crimp Wheel Extraction of Iris Images during Iris Diagnosis

*Zhao Yi'an*

*gr.910101*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Вишняков Владимир Анатольевич. – Doctor of Technical Sciences, BSUIR Technology*

**Annotation**. Iris diagnostics is a method based on the recognition of patterns in the eye's iris to identify an individual's health status, genetic information and other relevant characteristics. One of the most distinctive features of the iris is the constrictor, located in the middle of the iris, surrounding the pupil. It is important for iris diagnosis because its shape, size, and other characteristics can reveal an individual's physical health.

**Keywords:** recognition of patterns, iris diagnosis, constrictor

***Crimp wheel extraction based on structural pattern*.** In pattern recognition, a method that uses basic element structures (primitives) and the structural relationships between primitives to describe patterns and complete the recognition and classification process is called structural pattern recognition [1]. Through a large number of observations of existing iris images, it can be found that there are boundary areas with drastic changes in grayscale in the iris part of the image, and most of these areas with drastic changes in grayscale exist in a few pixels. The study found that the most drastic changes in grayscale The part is around the inner edge of the iris image, which is a boundary in the iris image. However, compared with the pupil boundary edge, the grayscale of the shrink wheel shows a slowly changing trend within a certain pixel range. Compared with the non-border area There are also many pixels with large grayscale changes. As shown in Figure 1, the pupil area is between the 40th pixel and the 95th pixel, and the curling wheel area is between the 20th and 40th pixels. The curve in the figure Reflects the change in grayscale around the constriction wheel and around the pupil. In order to better find the boundary point, this paper approximately defines the center point within the boundary range as the boundary point of the image within the range, that is, using the basic element structure to count the image range with the largest change in the curling wheel texture in the iris image, and

at the same time defining Two modes: border mode and non-border mode, and use the sliding window method to count the number of times each of the two modes appears in the window, find the window containing the curling wheel texture through the rules of the number of occurrences of each mode, and complete the curling Round extraction. [2]

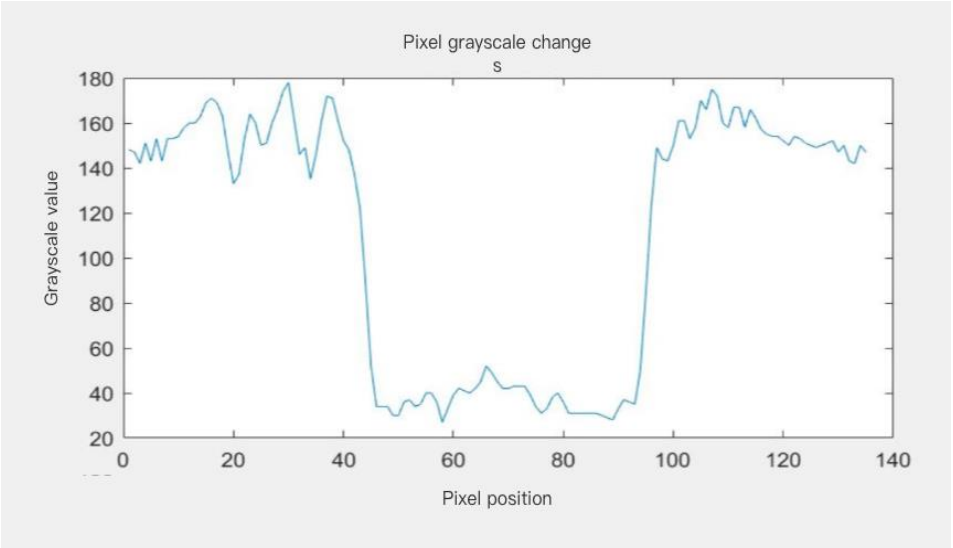



Figure 1 – Boundary area grayscale changes

***Define primitives and patterns.*** The primitive in this article is a basic unit used to describe the degree of grayscale change within a certain pixel range. Through the observation of the curling wheel part in the normalized iris image, combined with the analysis of multiple experimental results, This article defines a primitive as five consecutive pixels in the vertical direction, consisting of a central pixel and two edge pixels at the top and bottom. Its structure is shown in Figure 2, where O represents the center pixel, 1, 2, 3, 4 represent four edge pixels.

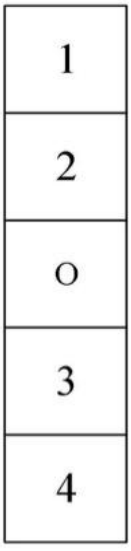



Figure 2 – Primitive diagram

In order to accurately describe the grayscale difference between each edge pixel and the center pixel in the primitive, this paper records the grayscale difference between the edge pixels 1, 2, 3, 4 and the center pixel as $q_i$=(i=1,2,3, 4), and define the threshold as a=9, b=4, and define the relationship between the absolute value of the grayscale difference between each

edge pixel and the center pixel and the threshold to define the primitive mode, recorded as P{$p_1$, $p_2$, $p_3$, $p_4$}. It stipulates three modes of 0, 1, and 2 to represent $p_i$ = (i = 1, 2, 3, 4), which represents the relationship between the absolute value of qi and the two thresholds. If the absolute value of qi is greater than a, then $p_i$ =0. If the absolute value of $q_i$ is less than b, then $p_i$=1 is recorded. If the absolute value of qi is between a and b, $p_i$=2 is recorded. When there is a large change in grayscale between the edge pixels and the center pixels, the image at this time is mostly in the boundary area, and $p_i$=0 is often present at this time. Therefore, P {0,0,0,0} can be defined as Boundary mode; Similarly, when the edge pixels have almost no change compared with the center pixels, the image at this time is mostly in the non-border area, that is, $p_i$=1, and the non-edge mode can be defined as P {1,1,1,1}. It would be too simple to consider just using the above two modes as the judgment conditions for boundary areas and non-boundary areas. In order to find out the boundary area of the crimping wheel as completely as possible, this article adds several more types that often appear in boundary areas and non-boundary areas. The mode of the non-boundary area is used to determine whether the image is at the boundary, that is, let P {2,0,0,0}, P {0,2,0,0}, P{0,0,2,0}, P{ 0,0,0,2} to jointly serve as the boundary determination mode, let P{2,1,1,1}, P{1,2,1,1}, P{1,1,2,1}, P{1,1,1,2} to jointly define the non-boundary mode. [3]

***Crimping wheel extraction implementation.*** Select a 15*15 window and slide it along the direction of Figure 5 on the normalized image. In the same window, if the boundary mode appears more often, the non-border mode will appear less often, and vice versa. In order to achieve an accurate description, the boundary point on a certain column is determined by using the quotient of the number of occurrences of the boundary pattern within the window and the number of occurrences of the non-border pattern within the window, and the quotient is recorded as B. [4]

The extraction steps of the crimping wheel are as follows, and the extraction flow chart is shown in Figure 4.

(1) Use a 15×15 window to slide on the normalized image in the direction as shown in Figure 3, count all B, record the maximum value, and save the center point of the window where the maximum value of the quotient is located, which is the boundary point of the column.

(2) Move the window one pixel to the right and repeat the above steps until the image is traversed and all boundary points are found.

(3) Connect all the boundary points and map them to the original image, which is the calibrated shrinking wheel.

Figure 3 – Window sliding direction

***Experimental results and analysis.*** The results of the curling wheel extraction are shown in Figure 5. It can be seen from the figure that the curling wheel outline extracted by this algorithm covers the entire curling wheel area, basically outlines the outline shape of the curling wheel, and is not affected by the eyelashes above the iris. interference.

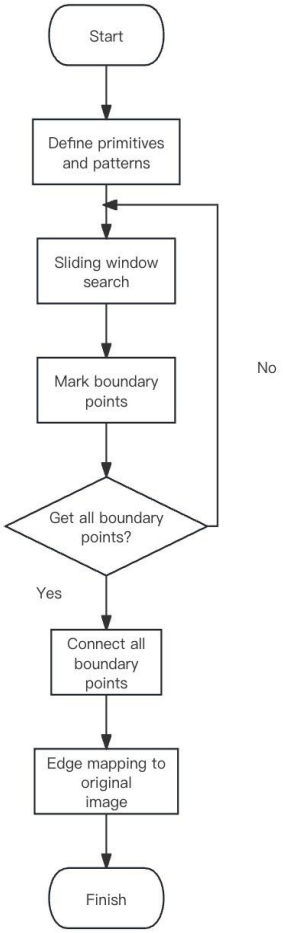



Figure 4 – Curled round extraction flow chart

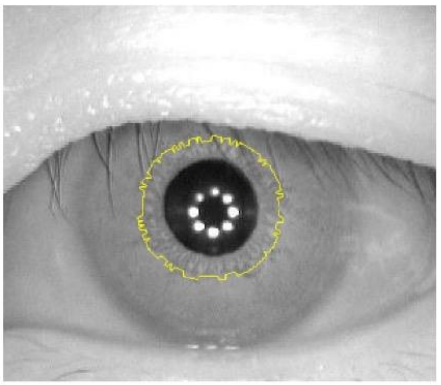


Figure 5 – Curled round extraction

***Conclusion.*** As a combination of traditional Chinese medicine visual examination and western medicine iridology, iris diagnostics plays a huge role in the field of human sub-health evaluation and disease prevention. It has gradually been valued by various countries in the world. As a subject that has attracted widespread attention from the world, iris diagnostics has developed a An iris-assisted diagnosis system based on this discipline has become an inevitable trend. Crimping wheel extraction is a key step in the iris diagnosis process. Deep learning algorithms can quickly and automatically identify and extract key features such as crimping wheels from a large number of iris images, significantly improving the speed of

analysis and batch processing. The use of deep learning to extract crimped wheels in iris diagnosis is not only a technological advancement, but its practical significance and application value involve many aspects such as medical health, safety certification, and technological innovation. It is an important step in the current and future field of artificial intelligence. one of the research directions.

## *REFERENCES*

*[1] Xin Guodong, Wang Wei. Research on iris constriction wheel extraction method [J]. Computer Engineering and Design, 2008, 29(9): 2290-2292.*

*[2] Yuan Weiqi, Ye Bingwen, Sun Xiao, Teng Hai. Iris curling wheel detection method based on gradient extreme value[J]. Computer Engineering, 2014,40(2):162-165.*

*[3] Dong Feixia. Eye syndrome differentiation and iris diagnosis [J]. Journal of Changchun University of Traditional Chinese Medicine, 2010, 26(1):8-9.*

*[4] Gao Yuan. Research on feature extraction method of iris texture[D]. Shenyang University of Technology, 2015.*

УДК 004.75

## СИСТЕМА АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

*Грищук А.А. Клепцов Ю.В Грибович А.А*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Цветков В.Ю. – д.т.н., доктор, заведующий кафедры ИКТ*

**Аннотация.** В настоящее время радиочастотная идентификация (RFID) является одной из быстро развивающихся технологий в области беспроводных коммуникаций быстрого действия и одной из базовых технологий Интернета вещей. На данный момент радиочастотную идентификацию внедрили во многие сферы жизни, не только корпоративной, но и повседневной.

**Ключевые слова:** радиочастотная идентификация, штрихкодирование, индивидуальное сканирование

***Введение.*** Технология RFID становится все более популярной в области почтовой связи, ведь главное ее преимущество – скорость – очень важно при оказании услуг.
RFID-технология используется в Системе UNEX (система измерения качества почтовых услуг) на протяжении последних 17 лет. Более того, данная система внедрена уже в 46 странах – порядка 340 рабочих и складских помещений операторов почтовой связи сегодня оборудованы более чем 1500 RFID-считывателей.

***Основная часть.*** По данным IDTechEx, озвученным на II Московском ID-Форуме, в 2014 году общий объем мирового рынка RFID составил 8,9 млрд долл., а в 2015-м рынок превысил 9,6 млрд долл. Сейчас 13% продаж приходится на считывающие устройства; все остальные доходы формируются от поставок меток различных видов. Основная масса меток используется для оснащения средств контроля доступа и в розничной торговле, далее с большим отрывом следуют «умные» билеты и производство.
Сейчас технологии радиочастотной идентификации более всего востребованы в ретейле, логистике, медицине и некоторых производственных процессах, однако в ближайшем будущем ожидаются заметные перемены: активность сместится в сферу легкой промышленности, оборонного сектора и почты.
Даже при наличии систем штрихкодирования процесс отслеживания перевозимых грузов

может быть достаточно сложным. Основная проблема заключается в том, что Barcode или QR-code каждой этикетки необходимо сканировать индивидуально, обеспечив при этом прямую видимость этикетки сканером штрихкода. Описанные выше особенности сильно замедляют логистические процессы и повышают влияние человеческого фактора, как следствие, возникновение ошибок.
Система, построенная на основе технологии радиочастотной идентификации (RFID) актуальна в логистике и на складах, так как лишена этого недостатка – сканирование целой группы товаров может производиться одновременно бесконтактным образом. Использование системы, построенной на основе оборудования RFID и меток RFID, значительно оптимизирует логистические процессы. Наши метки RFID в сочетании с RFID-считывателем позволяют отслеживать, учитывать и сортировать даже большие группы предметов одновременно. Индивидуальное сканирование конкретного товара тоже возможно. Благодаря технологии RFID управление логистическими процессами становится проще, чем когда-либо. Влияние человеческого фактора значительно минимизируется, что приводит к меньшему количеству ошибок, например, при доставке товара.

Почта России давно прорабатывала возможность маркировки RFID-метками писем и бандеролей, и сейчас эти работы входят в завершающую фазу. Также в рамках развития общих процедур Таможенного союза начат проект по маркировке изделий легкой промышленности, чтобы взять под контроль их оборот. Что касается военной промышленности, то здесь радиочастотные технологии используются для идентификации специфических изделий.
Республиканское унитарное предприятие «Белпочта» стремится не только выполнять свою главную миссию - предоставление услуг почтовой связи для населения, органов государственного управления, предприятий и организаций, руководствуясь девизом «Быстрота. Надежность. Доступность», но также и стремится облегчить труд своих работников. РУП «Белпочта» постоянно повышает уровень обслуживания и внедряет новые услуги, а также совершенствует существующие услуги и производственные процессы. Работать на опережение потребностей своих клиентов — один из главных принципов предприятия.
РУП «Белпочта» на сегодняшний день является технически оснащенным предприятием, которое успешно использует различные технологии, в том числе и информационные, для эффективной работы предприятия. Так на смену уже ставшему традиционным штрих-кодированию постепенно приходит новая технология - радиочастотная идентификация.
Технология RFID позволяет вывести учет на новый уровень, на котором вмешательство человека минимально или не требуется вовсе. Появилась возможность полностью автоматизировать учет.
Внедрение технологии RFID в почтовую связь позволит повысить эффективность работы в целом, усилить контроль над прохождением отправлений по всему пути следования, а также ускорить регистрацию и слежение почтовых отправлений в системе. Применение данной технологии ведет к увеличению безопасности почтовых отправлений, снижению потерь времени, повышению производительности и более эффективному использованию оборудования и персонала.

***Заключение.*** В данной исследовательской работе был проведен анализ перспектив внедрения технологии радиочастотной идентификации (RFID) для автоматизации учета в объектах почтовой связи. Существенно сокращается время на получение информации о движении объектов и повышается ее достоверность и безопасность. Внедрение автоматизированной системы, построенной на основе радиочастотных технологий, позволит достигнуть следующих результатов:

– уменьшить затраты на оплату труда за счет сокращения численности работников, исключить ошибки персонала, автоматизировать значительную часть работы;

– усовершенствовать обработку информации за счет исключения ручного ввода и связанных с этим ошибок

– снизить потери времени от поиска почтового отправления, быстро и точно проводить инвентаризацию.

Преимущества использования радиочастотной идентификации позволяют заключить, что штрих-код постепенно будет заменен на более эффективный способ автоматической идентификации на разных этапах обработки почтовых отправлений, что позволит улучшить качество оказания услуг почтовой связи.

### *Список литературы*

1 RFID [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/RFID. – Дата доступа: 21.05.2023

2 Частотные диапазоны [Электронный ресурс]. – Режим доступа: https://erfid.ru/ baza-znanij/frequency/. – Дата доступа: 20.05.2023

3 Автоматизация идентификации объектов. Штрих-кодирование [Электронный ресурс]. – Режим доступа: https://studref.com/304474/filosofiya/avtomatizatsiya_identifikatsii _obektov_shtrih_kodirovanie. – Дата доступа: 21.05.2023

4 Как выбрать RFID-метки [Электронный ресурс]. – Режим доступа: https://go-rfid.ru/novosti-i-statiy/novosti-oborudovaniya/kak-vibrat-rfid-metki. – Дата доступа: 05.07.2023

## AUTOMATIC OBJECT IDENTIFICATION SYSTEM

*Hryshchuk A.A. Klepcov U.V. Gribovich A.A.*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Tsvetkov V.Yu. – Doctor of Technical Sciences, Doctor, Head of the Department*

**Annotation**. Currently, radio frequency identification (RFID) is one of the rapidly developing technologies in the field of fast-acting wireless communications and one of the basic technologies of the Internet of Things. At the moment, radio frequency identification has been introduced into many areas of life, not only corporate, but also everyday.

**Keywords**: radio frequency identification, bar coding, individual scanning

УДК 004.75

# АНАЛИЗ СЕТЕВОГО ТРАФИКА. МЕТОДЫ СБОРА СЕТЕВЫХ ПРИЗНАКОВ И ПРЕДУПРЕЖДЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

*Грибович А.А., Клепцов Ю.В., Грищук А.А. магистранты гр.267041*

*Белорусский государственный университет информатики и радиоэлектроники[1]*
*г. Минск, Республика Беларусь*

*Медведев С.А. – канд. технич. наук*

**Аннотация**. Рассматривается задача сбора и анализа сетевых признаков и предупреждений для выявления аномалий и вредоносной активности, улучшения диагностики, восстановления и устранения причинных факторов. Рассмотрена концепция сетевого мониторинга безопасности (NSM) и методы сбора данных.

**Ключевые слова**. Сетевой мониторинг безопасности, сбор сетевых данных, обнаружение на конечных точках.

**Введение.** В современном мире безопасность сетей становится все более приоритетной, особенно в условиях нарастающих угроз в интернете. Эффективные

методы сбора данных о сетевой активности играют решающую роль в обнаружении и реагировании на потенциальные атаки.

Концепция сетевого мониторинга безопасности (NSM) включает в себя сбор, анализ и реагирование на признаки вторжений [1]. Необходимость сбора сетевых данных обусловлена выявлением аномалий и вредоносной активности, что предоставляет ценную информацию о возможных угрозах. Каждый из методов сбора данных имеет свои преимущества и недостатки, и их выбор зависит от конкретных требований и целей. В данной работе мы рассмотрим каждый из них в контексте обеспечения безопасности сети.

Важно отметить, что мониторинг сетевых данных и активности пользователей играет важную роль в обеспечении безопасности сети. Постоянное обновление политик безопасности и тщательная проверка конфигураций конечных точек являются неотъемлемой частью защиты сети от вредоносных атак.

**Основная часть.** Мониторинг сетевой безопасности (NSM) - это сбор, анализ и эскалация признаков и предупреждений для обнаружения и реагирования на вторжения. Данный подход неявно обращается к планированию деятельности или попыткам сопротивления вторжениям. Все четыре фазы цикла безопасности – планирование, сопротивление, обнаружение и реагирование необходимы при защите сети организации от угроз. Первым шагом в построении операционной модели является описание взаимосвязей между планированием, сопротивлением, обнаружением и реагированием, как показано на рисунке 1.

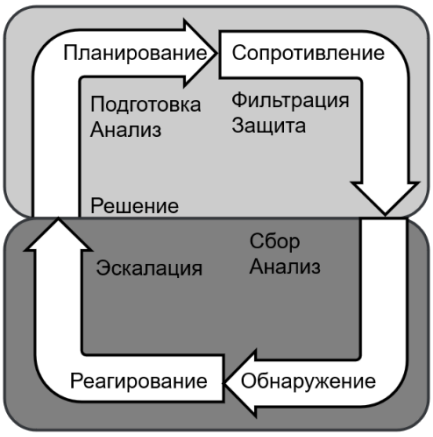



Рисунок 1 – Цикл обеспечения безопасности

IT-команды и команды по безопасности планируют новые защитные меры, в то время как существующие компоненты противодействия отражают некоторых злоумышленников. В то время как одна группа занимается обнаружением одних злоумышленников, реагируя на них, команды инцидентного реагирования по безопасности уже реагируют на других злоумышленников, уже проникших в организацию.

Фаза планирования. Команды IT и безопасности подготавливаются и анализируют текущую ситуацию, нацеливаясь на оптимальное сопротивление вторжениям и уязвимостям. В рамках этой фазы проводятся бюджетирование, аудит, проверка соответствия, обучение и разработка безопасного программного обеспечения. К примерам работы по оценке относятся симуляция атак, тестирование на проникновение и практика проведения атакующих операций.

Фаза сопротивления. Команды IT и безопасности осуществляют фильтрацию и защиту данных. Здесь применяется автоматизированное противодействие, такое как брандмауэры, антивирусное программное обеспечение и защита от утечки данных. Также проводятся обучение по безопасности и управление конфигурацией и уязвимостями.

Фазы обнаружения и реагирования включают в себя сбор, анализ и эскалацию, которые являются основой цикла безопасности предприятия. Аналитики занимаются обнаружением и реагированием на вторжения.

Сбор данных, которые нам необходимы для принятия решения о том, является ли деятельность нормальной, подозрительной или вредоносной. Включает в себя различные процессы, которые собирают информацию, как техническую, так и не техническую.

Технические процессы включают в себя сбор данных с конечных точек или хостов (таких как компьютеры, серверы, планшеты, мобильные устройства и т. д.), сети и логов (созданных приложениями, устройствами и другими источниками).

Нетехнические процессы сбора включают запись информации от сторонних лиц (внешних участников, таких как партнеры, правоохранительные органы, разведывательные агентства и т. д.) и пользователей. Индикатор компроментации (IOC) – это признак компрометации, который указывает на наличие инцидента безопасности или активности злоумышленников в сети или системе. IOC может включать в себя различные типы данных, такие как IP-адреса, URL-адреса, хэши файлов, паттерны сетевого трафика, аномальные действия пользователей и другие сигналы, которые могут указывать на наличие угрозы безопасности.

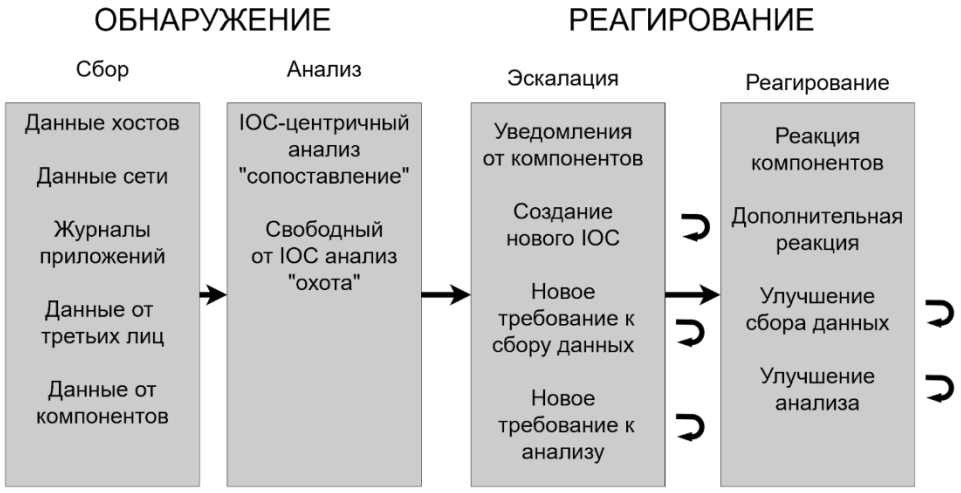



Рисунок 2 – Процесс сетевого управления безопасностью

Сбор данных происходит с помощью комбинации аппаратных и программных средств, которые используются для генерации и сбора данных для обнаружения и анализа NSM [2].

Большинство организаций можно отнести к одной из трех категорий:

- Организации без установленной инфраструктуры NSM, которые только начинают определять свои потребности в сборе данных.
- Организации, которые уже занимаются обнаружением вторжений, но никогда подробно не изучали данные, которые они собирают.
- Организации, которые вложили много времени в определение своей стратегии сбора данных и постоянно совершенствуют эту стратегию в рамках цикла NSM.

Сбор сетевых данных может помочь выявить закономерности, и необходим для обнаружения аномальной или вредоносной активности в сети. Предоставляет полезную информацию о вторжениях для улучшения диагностики, восстановления и устранения причинных факторов. Вот несколько методов:

1. Захват пакетов: Используйте инструменты захвата пакетов, такие как Wireshark, tcpdump или Snort, для захвата сетевых пакетов, проходящих по сети. Захват пакетов

позволяет вам осмотреть содержимое отдельных пакетов, включая исходные и конечные IP-адреса, порты, протоколы и данные полезной нагрузки.

Процесс сниффинга пакетов включает в себя взаимодействие программного и аппаратного обеспечения и состоит из трех этапов:

Сбор данных: Сначала сниффер пакетов собирает сырые двоичные данные с провода, переключая выбранный сетевой интерфейс в режим promiscuous. Это позволяет прослушивать весь трафик на сегменте сети.

Преобразование: Захваченные двоичные данные преобразуются в читаемый формат. Большинство продвинутых снифферов ограничиваются этим этапом, оставляя анализ для пользователя.

Анализ: Сниффер пакетов анализирует захваченные данные, проверяя протокол сетевых данных и выявляя его особенности [3].

PCAP представляет собой формат файла, используемый для хранения данных, захваченных при сниффинге пакетов. PCAP - это важный инструмент для системных администраторов и команд по безопасности, предоставляющий глубокое понимание сети [4]. Он увеличивает видимость сети, позволяет мониторить в реальном времени и прост в использовании. Однако есть и недостатки:

- Не обнаруживает угрозы, не связанные с сетью, такие как атаки на аппаратный уровень.
- Не преодолевает шифрование, что делает невозможным анализ зашифрованных коммуникаций.
- Расположение сниффера пакетов влияет на видимость, так как он не может видеть всю активность по сети.

2. Анализ сетевого потока: Собирает данные сетевого потока, которые предоставляют краткую информацию о потоках сетевого трафика. Данные потока включают в себя такие детали, как исходные и конечные IP-адреса, порты, протоколы и метки времени. Инструменты, такие как NetFlow, sFlow или IPFIX, могут использоваться для экспорта данных потока из маршрутизаторов, коммутаторов или сетевых устройств.

Строго говоря, поток – это серия пакетов, которые имеют одни и те же исходные и конечные IP-адреса, исходные и конечные порты, а также IP-протокол [5]. Это также называется пятикратным IP-потоком. Термин "поток" иногда также используется для обозначения агрегации отдельных потоков. Запись потока – это сводная информация о потоке, записывающая, какие хосты общались с какими другими хостами, когда происходила эта связь, как трафик передавался, и другая основная информация о сетевом общении. Система анализа потока собирает информацию о потоках и предоставляет вам систему для поиска, фильтрации и печати информации о потоках. Записи потока подводят итоги каждого соединения в вашей сети.

Архитектура потоковой системы включает три компонента:

- Сенсор (зонд): Устройство, которое прослушивает сеть и захватывает данные о трафике. Это может быть коммутатор, маршрутизатор или программное обеспечение, которое слушает сетевой трафик. Сенсор отслеживает сетевые соединения и передает данные после завершения соединения или по истечении тайм-аута.
- Коллектор: Программное обеспечение, которое получает записи сенсора и сохраняет их на диск. Коллектор является критической частью инфраструктуры управления потоками, хотя формат хранения данных может отличаться.
- Система отчетности: Читает файлы коллектора и создает удобные для анализа отчеты. Система должна быть совместима с форматом файла, используемым коллектором.

3. Обнаружение вторжений (IDS) - это процесс мониторинга событий в компьютерной системе или сети и анализа их на наличие признаков вторжений, таких как попытки компрометации конфиденциальности, целостности и доступности данных, а также обход механизмов безопасности [6]. Эти события могут быть вызваны злоумышленниками, получающими доступ из Интернета, авторизованными пользователями, пытающимися получить несанкционированные привилегии, или авторизованными пользователями, злоупотребляющими своими привилегиями.

Цели использования IDS:

- Предотвращение проблемного поведения путем увеличения риска обнаружения и наказания злоумышленников.
- Обнаружение атак и других нарушений безопасности, которые не удается предотвратить другими мерами безопасности.
- Обнаружение и реагирование на предвестники атак, такие как сетевые запросы и другие аномалии.
- Документирование существующих угроз для организации.
- Контроль качества проектирования и администрирования безопасности, особенно в крупных и сложных предприятиях.

4. Управление информацией и событиями безопасности (SIEM). SIEM используется для централизации и корреляции журнальных данных с различных сетевых устройств и средств безопасности. Платформы SIEM собирают журналы от брандмауэров, маршрутизаторов, коммутаторов, сенсоров IDS/IPS, серверов и других сетевых устройств, и применяют правила корреляции для выявления потенциальных инцидентов безопасности.

5. Журналирование на DNS и DHCP серверах для мониторинга разрешений доменных имен и выделений IP-адресов. Анализ журналов DNS и DHCP может помочь выявить подозрительные доменные имена, IP-адреса или имена хостов, связанные с злонамеренной деятельностью.

6. Журналы прокси-серверов и веб-серверов. Используются для мониторинга веб-активности пользователей и доступа к внешним сайтам. Журналы прокси-серверов и веб-серверов могут предоставить информацию о шаблонах веб-трафика, поведении пользователей и потенциальных угрозах безопасности, таких как доступ к вредоносным веб-сайтам или загрузка подозрительных файлов. Включите журналирование на сетевых устройствах, таких как брандмауэры, маршрутизаторы и коммутаторы, чтобы записывать события и активности.

6. Сетевые тапы/Зеркалирование портов сети. Используется для копирования сетевого трафика с одного сегмента сети на другой. Это позволяет вам мониторить сетевой трафик, не нарушая поток данных. Сетевые тапы и зеркалирование могут быть особенно полезны для захвата трафика на высокоскоростных или критически важных сетевых каналах.

7. Обнаружение и ответ на события на конечных точках (EDR). Интегрируются решения безопасности конечных точек с возможностями мониторинга сети для сбора данных с конечных точек о сетевых подключениях, трафике и связи. Решения EDR предоставляют информацию о сетевой активности конечной точки и могут помочь выявить аномальное или злонамеренное поведение, свидетельствующее о угрозах безопасности.

По мере присоединения, изменения и выхода устройств из наших сетей, они приобретают динамичные характеристики, сравнимые с фильмом, а не статичным снимком [7]. Наш подход к сети, особенно к ее периметру, должен быть адаптивным и постоянно ориентированным на динамическую природу сети. Это требует от нас не только моментальных снимков, но и всестороннего обеспечения доверительности всех подключаемых к нам конечных точек.

С учетом разнообразия методов подключения устройств к нашим сетям, конечная точка становится ключевым периметром, который необходимо защитить. Хотя у нас есть сетевые брандмауэры, контролирующие широкомасштабный доступ к сети, основная угроза исходит от мелких нарушений доступа, таких как небольшие вирусы, попадающие в сеть через пользовательские конечные точки.

Путем анализа данных с этих сетевых источников организации могут обнаружить и оперативно реагировать на аномальную или вредоносную активность на своих сетях, чтобы минимизировать потенциальные угрозы безопасности.

Как минимум, предпочтительно избежать следующего: вирусов, червей, незаконного программного обеспечения, шпионских программ, неавторизованных пользователей, неавторизованных конечных точек [8].

Каждая конечная точка должна выполнять следующее: обеспечить целостность операционной системы, проверить конфигурацию системы, быть удаленно управляемой.

Успешное удаленное управление требует строгой политики, которая обеспечивает соблюдение минимальной конфигурации для всех подключенных конечных точек, независимо от возражений пользователей. Это важно, поскольку даже одна несоответствующая система может привести к серьезным проблемам в сети.

На рисунке 3 показан процесс коррекции наших правил, включая в них принципы восстановления и компартментализации. Важно понять, может ли сеть может доверять каждой из конечных точек.

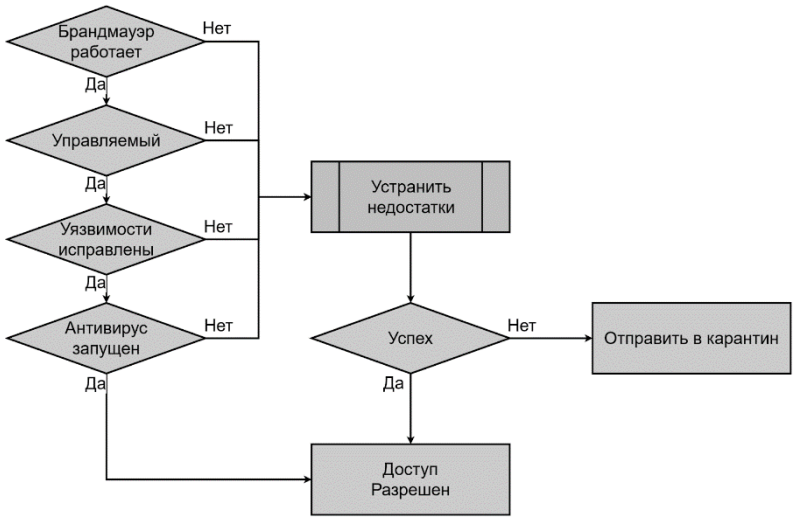



Рисунок 3 – Конечная точка должна быть помещена в карантин, если не проходит четыре простых теста

**Заключение.** В современном мире, где угрозы в интернете продолжают расти, мониторинг сетевых данных и активности пользователей играет ключевую роль в обеспечении безопасности сети. Разнообразные методы сбора данных имеют свои преимущества и недостатки, и выбор конкретного метода зависит от требований и целей организации. Однако, независимо от выбранного метода, важно понимать необходимость постоянного обновления политик безопасности и строгой проверки конфигураций конечных точек, хостов и других узлов сети, как неотъемлемой части защиты от вредоносных атак.

***Список использованных источников:***

1. *Richard Bejtlich // The Practice of Network Security Monitoring: Understanding Incident Detection and Response, 2013. P. 185-189.*
2. *Chris Sanders, Jason Smith, and Liam Randall // Applied Network Security Monitoring: Collection, Detection, and Analysis, 2014. P. 74-75.*
3. *Крис Сандерс // Анализ пакетов: Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 2017. P. 23-26.*
4. *What Is PCAP? Packet Capture Explained [Electronic resource]. URL: www.forbes.com/advisor/business/software/what-is-pcap. (date of access: 05.02.2024).*
5. *Michael W. Lucas // Network Flow Analysis, 2010. P. 10-12.*

6. Rebecca Bace, Peter Mell // Intrusion Detection Systems, 1999. P. 5-6.
7. Mark Kadrich // Endpoint Security, 2007. P. 15.
8. Mark Kadrich // Endpoint Security, 2007. P. 73-74.

*УДК 004.738.5*

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ LORAWAN И SIGFOX

*Клепцов Ю.В., Грищук А.А., Грибович А.А.*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Хмелев А.Г. – д.э.н., профессор, кафедры ПОИТ*

**Аннотация.** Данная научная статья проводит сравнительный анализ двух популярных протоколов передачи данных для интернета вещей (IoT) – LoRaWAN и SigFox. В статье рассматриваются технические характеристики обоих протоколов, их преимущества и недостатки, а также возможности применения в различных сценариях. Исследование позволяет выявить основные отличия между LoRaWAN и SigFox, что поможет разработчикам и инженерам выбрать наиболее подходящий протокол для конкретного проекта IoT.

**Ключевые слова:** LoRaWAN, SigFox, протокол передачи данных, интернет вещей, сравнительный анализ

***Введение.*** С развитием интернета вещей (IoT) становится все более актуальным вопрос выбора подходящего протокола передачи данных для обеспечения связи между устройствами. Два из наиболее популярных протоколов в этой области – LoRaWAN и SigFox – предлагают различные подходы к передаче данных и имеют свои особенности. В данной статье будет проведен сравнительный анализ этих двух протоколов с целью выявления их технических характеристик, преимуществ и недостатков.

***Основная часть.*** По словам Донны Мур, председателя совета директоров LoRa Alliance, из всех приложений IoT около 75% приходится на сети с низким энергопотреблением и большим охватом (LPWAN), и только 25% требуют высокой пропускной способности и малой задержки сигнала. Ожидается, что в ближайшие годы рынок LPWAN будет быстро расти в результате резкого увеличения спроса на маломощные глобальные соединения для устройств Интернета вещей.
Сегодня LPWAN используются в нескольких секторах: транспорт, логистика, энергетика, здравоохранение и сельское хозяйство. По состоянию на 2022 год более 90% мирового рынка LPWAN делят между собой три технологии: LoRaWAN, SigFox и NB-IoT. В рамках данной статьи будут рассмотрены первые две из них.

Общим в обеих технологиях является работа в нелицензируемом диапазоне частот ISM, схожая топология сети, крайне низкое энергопотребление конечных устройств, широкая зона покрытия (Таблица 1). Однако, если рассматривать обе технологии как радиоканал для передачи данных, имеются существенные различия.

LoRaWAN (Long Range Wide-Area Networks) – это MAC-протокол для высокоемких сетей с большим радиусом действия и низким собственным потреблением мощности, который организация LoRa Alliance стандартизировала для маломощных глобальных радиальных сетей (Low Power Wide Area Networks, LPWAN) типа звезда. LoRa – это набор методов модуляции, запатентованных компанией Semtech. Модуляция LoRa является физическим уровнем. Это достаточно новый метод модуляции с расширением спектра посредством линейной частотной модуляции (CSS) и одноименная сетевая технология.

Протокол LoRaWAN оптимизирован для малобюджетных сенсоров с работой от батарей, представляет собой открытый протокол связи и включает в себя различные классы узлов. Тем самым обеспечивается компромисс между скоростью доставки информации и временем работы устройств, что особенно важно ввиду использования питания от батарей/аккумуляторов. Скорость передачи данных по протоколу LoRaWAN в системе LoRa находится в диапазоне 0,3-11 кбит/с. Протокол обеспечивает полную двустороннюю связь, а архитектура (посредством специальных методов шифрования) обеспечивает общую надежность и безопасность всей системы. Архитектура LoRaWAN в том числе была разработана с целью облегчить обнаружение мобильных объектов, что является одним из наиболее быстро растущих приложений на уровне Интернета вещей.

LoRaWAN-сеть включает конечное устройство, шлюзы, сетевой сервер и сервер приложений. Используется топология типа «звезда», где каждый модуль или счетчик передает данные по радиоканалу напрямую на базовую станцию без применения промежуточных ретрансляторов. Базовая станция принимает сигналы от всех устройств в радиусе своего действия, оцифровывает и передает на удаленный сервер, используя доступный канал связи, например Ethernet, WiFi, сотовую связь. LoRaWAN используется для передачи небольших по объему пакетов данных на дальние расстояния. Такая сеть была разработана специально для распределенных сетей телеметрии, межмашинного взаимодействия (M2M) и Интернета вещей (IoT). Чтобы продлить срок службы батареи/аккумулятора в конечном устройстве и общую пропускную способность сети, сетевой сервер LoRaWAN управляет скоростью передачи данных и радиочастотным выходом каждого конечного устройства по отдельности. Управление осуществляется с помощью алгоритма адаптивной скорости передачи данных (Adaptive Data Rate, ADR).

Архитектура сети LoRaWAN обеспечивает полную конфиденциальность данных. Она сохраняется в процессе прохождения всей цепочки задействованных устройств. Содержимое пакета данных на всех стадиях процесса остается доступным только отправителю (конечному устройству) и получателю (приложению), которому оно предназначается.

К несомненным достоинствам технологии LoRaWAN можно отнести: безопасность сети и данных — как на уровне сети, так и на уровне приложений, широкий выбор и низкая стоимость конечных устройств и шлюзов, быстрота развертывания сети, высокая масштабируемость сети (до 5000 конечных узлов/км2), высокая помехозащищенность, большой радиус действия в плотной городской застройке и энергоэффективность, адаптивная скорость передачи данных (ADR). К недостаткам LoRaWAN относят сравнительно низкую пропускную способность, некоторую задержку передачи данных от датчика до конечного приложения, риски зашумленности спектра частот диапазона ISM, ограничение мощности сигнала.

22 декабря 2023 года Федеральное агентство по техническому регулированию и метрологии Российской Федерации (Рстандарт) утвердило национальный стандарт протокола LoRaWAN для интернета вещей (IoT). Ожидается, что это будет способствовать развитию экосистемы отечественных устройств, таких как умные счетчики и датчики, оборудование для транспорта, сферы ЖКХ, промышленных предприятий и пр.

Таблица 1

| Технология | Пропускная способность | Дальность на открытой местности | Дальность в городской застройке | Энергопотребление | Частоты, МГц | Время работы сенсоров |
|---|---|---|---|---|---|---|
| LoRaWAN | От 0,3 до 50 кбит/сек | 10-20 км | 2-5 км | от 0,1 мкА до 120 мА | 433, 470, 868, 915 | До 10 лет на одной батарейке АА |
| SigFox | В среднем 100 бит/сек | 20-50 км | 5-10 км | 25 мкА во время передачи данных и около 1 мкА во время ожидания | 868, 915 | До 20 лет на двух батарейках АА |

В Республике Беларусь технология LoRaWAN представлена целым рядом компаний, преимущественно занимающихся сбором и анализом данных приборов учета электроэнергии, газа,

воды и тепла. Некоторые из них, например, IOTANS, предлагают готовые решения, предоставляя широкий выбор оборудования от датчика до платформы для сбора и отображения данных, монтажа и сервисного обслуживания. Зона покрытия LoRaWAN-сетей индивидуальна и рассматривается в каждом конкретном проекте. Чаще всего это новые микрорайоны многоквартирной жилой застройки, где применяются поквартирные приборы учета воды и тепла.

SigFox — это односкачковая радиальная, звездообразная сеть со шлюзами, которые служат контроллерами этой сети. В некотором роде она похожа на LoRa, но использует иной способ достижения аналогичных целей. Система развернута с использованием возможностей современных сотовых сетей. Подобно LoRa, SigFox имеет большой диапазон покрытия и ей свойственно низкое энергопотребление. Используется технология Ultra Narrow Band (UNB), которая изначально предназначена для связи на низких скоростях передачи данных.

Протокол SigFox достаточно прост. Он не требует квитирования (обмена сигналами для установления связи, т. е. процедуры представления или взаимного опознавания партнеров по связи при установлении соединения) и передает пакеты всего по 12 байт (плюс дополнительные данные, такие как идентификатор радиосвязи и время). Как уже было сказано, передача ведется в очень узкой полосе частот, при этом используется D-BPSK-модуляция (дифференциальная двоичная фазовая манипуляция) со скоростью 100 или 600 бит/с со шестисекундными циклами передачи. Однако такая низкая скорость и узкий частотный спектр позволяют экономить энергию батарей и обеспечивают большой радиус покрытия технологии.

Sigfox использует дифференциальную двоичную фазовую манипуляцию (DBPSK) и гауссову частотную манипуляцию (GFSK) в нелецинзируемом диапазоне ISM. Широкополосный сигнал свободно проходит через твердые объекты и требует небольшое количество энергии. SigFox-сеть имеет топологию «звезда» с одним переходом и требуется, чтобы оператор мобильной связи передавал генерируемый трафик. Сигнал также можно использовать для покрытия больших территорий и достижения подземных объектов.

Из-за узкой полосы пропускания приемники могут иметь очень низкий уровень собственного шума, т. е. высокую чувствительность, достигающую порядка –140 дБм. Это означает, что при применении технологии SigFox без кодирования для «Интернета вещей», т. е. с помощью процессоров с небольшой вычислительной мощностью, при низкой мощности передатчика (14 дБм), низких скоростях передачи данных, коротких и нечастых, не более 140 сообщений в день, можно достичь большей зоны покрытия и более продолжительного времени автономной работы узла сети. Технология использует шифрование AES с HMACs с закрытым ключом, который встроен в прибор, плюс некоторый порядковый номер. Благодаря всем этим характеристикам SigFox может быть самым эффективным решением из всех технологий построения LPWAN в определенных обстоятельствах.

В настоящее время сеть Sigfox действует в 75 странах и регионах, охватывая 6 млн квадратных километров. В этой сети зарегистрировано более 11 млн активных устройств, которые передают свыше 80 млн сообщений в сутки. Широкое применение SigFox получила в сельском хозяйстве, логистике, системах «Умный город», энергетической отрасли, медицине и пр.

К достоинствам SigFox можно отнести большое покрытие, высокую проникающую способность в городской застройке (до 10км), сверхнизкое потребление (до 20 лет работы сенсора от двух батарей AA), низкую стоимость сенсоров, совместимость протокола SigFox с существующими трансиверами. Среди недостатков выделяют низкую скорость передачи данных, зависимость от сотовой инфраструктуры, ограниченную помехоустойчивость. Данная система изначально спроектирована с участием централизованной базы данных для идентификации устройств, управляющей компанией Sigfox, что в некоторых случаях идет в разрез с законодательной базой в отдельных странах.

***Заключение.*** Перспективы развития мирового рынка LPWAN позволяют спрогнозировать

рост капитализации с 14.31 млрд долларов США в 2023 году до 704.95 млрд долларов США к 2030 году при среднегодовом темпе роста 74.50 % в течение прогнозируемого периода. Значительную долю рынка (по состоянию на 2022 год около 59 %) занимают технологии LoRaWAN и SigFox. Сравнительный анализ протоколов передачи данных LoRaWAN и SigFox позволил выявить их основные отличия и может помочь пользователям и инженерам выбрать наиболее подходящий протокол для конкретного проекта IoT.

В результате проделанной работы удалось установить, что технология LoRaWAN является одной из наиболее перспективных беспроводных технологий на современном рынке IoT. По состоянию на середину 2020 года LoRaWAN со 105 млн. устройств де-факто самая распространённая технология LPWAN. Решения LoRa применяются в обслуживании систем HVAC и электронике, в учете электроэнергии и водоснабжении, контроле окружающей среды, управлении подачей электроэнергии, прогнозной очистке помещений. В LoRa Alliance уже входит свыше 500 компаний, среди которых производители программного обеспечения, микроэлектроники, операторы связи: IBM, Semtech, Cisco, Inmarsat, Swisscom и другие.

Во многом основные функции LoRaWAN сравнимы с SigFox, например, небольшой объем полезных данных, большая дальность передачи, высокий срок службы сенсоров. Тем не менее, LoRaWAN предлагает лучшую пропускную способность, а также значительно лучшую задержку.

К сожалению, несмотря на ряд преимуществ и широкое распространение в мире, протокол SigFox не получил распространение на территории Республики Беларусь и в Российской Федерации. Причиной этого в первую очередь можно назвать отсутствие стандартизации, в отличие от LoRaWAN.

### *Список литературы*

1 Официальный сайт SigFox [Электронный ресурс]. – Режим доступа: https://www.sigfox.com/what-is-sigfox/
2 Официальный сайт LoRaWAN [Электронный ресурс]. – Режим доступа: https://lora-alliance.org/about-lorawan/
3 Анализ рынка LPWAN [Электронный ресурс]. – Режим доступа: https://exactitudeconsultancy.com/ru/reports/32172/lpwan-market/
4 Архив журнала Control Engineering Russia №3(75)2018 [Электронный ресурс]. – Режим доступа: https://controlengrussia.com/magazine/
5 Сравнительный анализ стандартов связи для сетей IoT [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/msw/articles/720518/
6 LoRaWAN: один из путей Интернета вещей [Электронный ресурс]. – Режим доступа: https://www.connect-wit.ru/lorawan-odin-iz-putej-interneta-veshhej.html
7 Википедия. SigFox [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Sigfox

**UDC 004.738.5**

## COMPARATIVE ANALYSIS OF DATA TRANSMISSION PROTOCOLS LORAWAN AND SIGFOX

*Kleptsov Y.V., Hryshchuk A.A., Gribovich A.A.*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Scientific supervisor: Khmelev A.G. – Doctor of Economics, Professor, Department of POIT*

**Annotation**. This scientific article provides a comparative analysis of two popular data transfer protocols for the Internet of Things (IoT) – LoRaWAN and SigFox. The article discusses the technical characteristics of both protocols, their advantages and disadvantages, as well as the possibilities of application in various scenarios. The study reveals the main differences between LoRaWAN and SigFox, which will help developers and engineers choose the most suitable protocol for a specific IoT project.

**Keywords**: LoRaWAN, SigFox, data transfer protocol, Internet of things, comparative analysis

УДК 004.777

**СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ К ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА БАЗЕ УПРАВЛЯЕМЫХ КОММУТАТОРОВ HUAWEI И CISCO.**

*Кривко Д.Н., магистрант*
*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Пулко Т.А. – канд. техн.наук, доцент*

**Аннотация.** В материалах доклада рассматриваются шаги разработки алгоритма, направленного на управление коммутационным оборудованием производителей Cisco и Huawei. Итогом данной работы должна стать централизованная система, позволяющая оптимизировать рабочий процесс администратора сети в области предоставления доступа к локальной сети, а также направленная на повышение общего уровня информационной безопасности в применяемом сегменте.

**Ключевые слова:** локальная вычислительная сеть, алгоритм управления доступом, коммутатор, маршрутизация, Access Control List, язык Python.

Расширение локальных вычислительных сетей, а также их регулярное усложнение за счет реализации новейших методов обеспечения информационной безопасности зачастую приводит к тому, что в рамках одной локальной вычислительно сети используются передовые коммутаторы различных вендоров. Данный факт в значительной степени усложняет работу специалистов ответственных за администрирование сети, поскольку различные производители в своих решениях не всегда используют единые подходы к их реализации. Чем сложнее и разнообразнее становится диапазон применяемых команд управления сетевым оборудованием, тем выше шанс ошибки со стороны администратора, что в свою очередь может негативно сказаться как на информационной безопасности данной сети, так и на её функционировании в целом. Создание систем позволяющих решать подобного рода проблемы является востребованной, поскольку с их помощью с администратора снимается функция непосредственного ввода команд управления, что позволяет в большей степени сконцентрировать внимание на более актуальных вопросах. Целью данной работы является написание алгоритма управления доступом к локальной вычислительной сети, позволяющего идентифицировать сетевое коммутационное оборудование производителей Cisco и Huawei, с применением необходимого набора команд, характерных каждому из производителей.

Для разработки итогового алгоритма необходимо разобрать пул команд управления коммутаторов Cisco и Huawei, с целью определения закономерностей их применения, а также отличительных особенностей их синтаксиса. Получив данную информацию, необходимо описать логику работы алгоритма, уделив внимание вопросу идентификации оборудования, а также последовательности действий по генерированию команд управления. Только после этого можно будет приступать к кодированию данного алгоритма с использованием языка программирования и созданию централизованной системы управления доступом к локальной вычислительной сети. На данном этапе необходимо реализовать следующий набор функций:

– централизованная система учета IP-адресов используемых в ЛВС;
– поиск по системе учета, в соответствии с известными параметрами;
– разграничение доступа к системе централизованного управлений по паролю;
– введение логирования всех действий, выполняемых посредством системы централизованного управления;
– автоматическое определения вендора коммутационного оборудования в ЛВС до момента исполнения отдельных команд;
– автоматическое выполнение команд, необходимых для управления доступом к ЛВС;
– реализация автоматического определения mac-адреса для каждого ip-адреса активного

оборудования, используемого в ЛВС;
– реализация функционала, позволяющего производить разрешения/ограничение прохождения трафика по ЛВС для конкретных ip-адресов посредством статической маршрутизации, а также используя ACL-листы;
– реализация функционала отвязки/привязки mac-адреса к конкретному ip-адресу;
– наладить взаимодействие с сервером антивирусного обеспечения, с целью отображения наиболее актуальной информации, относящейся к антивирусной защите для конкретного ip-адреса;
– автоматическая синхронизация вносимой информации в систему учета с системой учета вышестоящей организации.

Для решения поставленных задач необходимо определиться с пошаговым алгоритмом взаимодействия всех взаимосвязанных элементов: базы данных, коммутационного оборудования, системы антивирусной защиты.

На начальных этапах разработки необходимо описать структуру базы данных, с целью максимальной оптимизации данных которые потребуются для дальнейшей работы, избегая избыточности данных, которые не должны дублироваться, а при необходимости, из одних данных получать другие уже непосредственно в процессе работы программы, без постоянного их хранения.

Для реализации поставленных целей принято решение об использовании в работе языка программирования Python. Данное решение обусловлено тем, что данный язык программирования легкий в освоении с простым и понятным синтаксисом. Это позволяет в перспективе упростить процесс сопровождения итогового решения, в случае смены разработчика. Также Python имеет одну из самых больших библиотек, включая библиотеки для работы с сетевыми протоколами, такими как urllib3, telnetlib, pynetbox и т. д.

Библиотеки значительно облегчают разработку сетевых приложений и управление сетевыми устройствами, они могут использоваться для управления различными сетевыми устройствами, включая маршрутизаторы, коммутаторы, межсетевые экраны, серверы и т. д., а также могут быть использованы для мониторинга сетевой активности, анализа данных и создания пользовательских интерфейсов, предоставляет возможности для автоматизации управления. Он может использоваться для написания сценариев, которые выполняют повторяющиеся задачи. Это позволяет администратора сети сэкономить время и улучшить эффективность своей работы.

Была разработана схема взаимодействия сетевых сервисов, которая наглядно показывает процесс взаимодействия между отдельными сетевыми сервисами, работа которых направлена на обеспечение отдельных элементов информационной безопасности. Объединение их в одну единую систему позволит в значительней степени повысить оперативность принятия решений в области защиты информации, а также упростит процесс управления доступом к локальной вычислительно сети (рисунок 1).

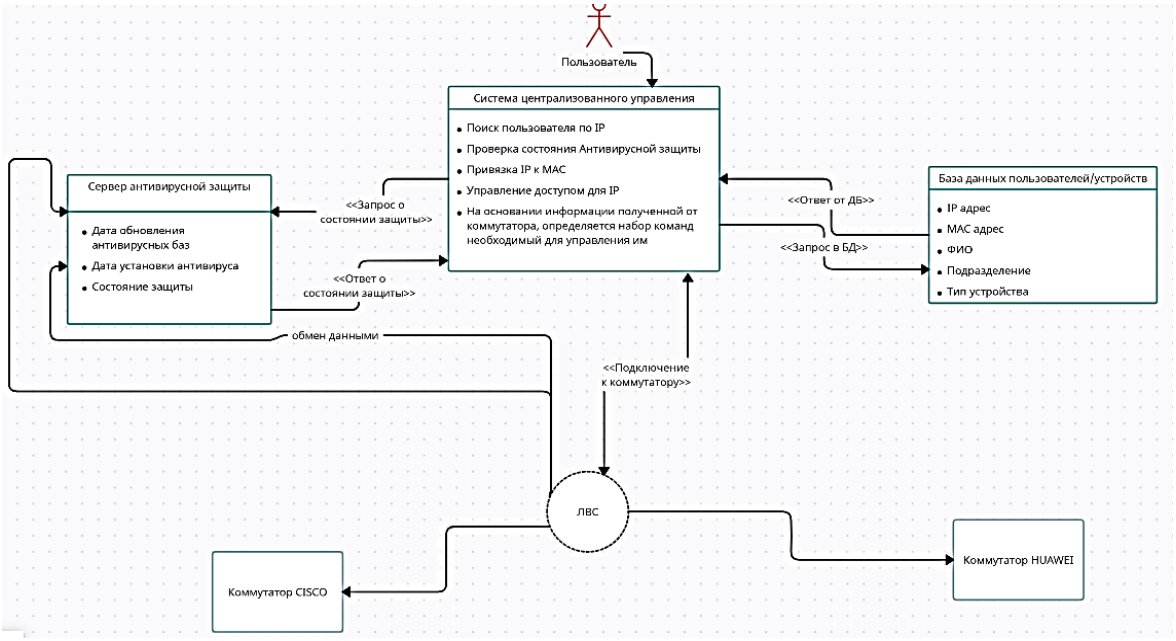


Рисунок 1 – Общая схема взаимодействия сетевых сервисов

Использование разработанной системы централизованного управления доступом к локальной вычислительной сети позволит повысить эффективность работы специалистов ответственных за организацию информационной безопасности, в рамках предоставления доступа к ресурсам локальной вычислительной сети валенного сегмента, а также более оперативно реагировать на возникающие угрозы.

Данная система разрабатывается на языке программирования Python, что в перспективе позволит более оперативно внедрять необходимые изменения в систему, а также позволит расширять её конечный функционал.

**Список использованных источников:**

1. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство – 2008. – 994 с.
2. Бэрри Пол Изучаем программирование на Python. – Эксмо, 2020. – 624 с.
3. Жан Вальран Парех Шьям Коммуникационные сети. Краткое введение - ДМК Пресс, 2023.- 268с.

УДК 621.397.42

## ИССЛЕДОВАНИЕ 4/8 КАНАЛЬНОГО ГИБРИДНОГО 5 В 1 ВЕДИОРЕГИСТРАТОРА И 2/4 AHD КАМЕР ВИДЕРНАБЛЮДЕНИЯ С ИК ПОДСВЕТКОЙ НА ОСНОВЕ СТЕРЕОСКОПИЧЕСКОГО СПОСОБА ОПРЕДЕЛЕНИЯ ДАЛЬНОСТИ ДО ОБЪЕКТА

*Черепова Е.В., Михалёнок К.А., Тиханкова П.И., Лобан В.В.*
*гр.162901*

*Белорусский государственный университет информатики и радиоэлектроники,*
*г. Минск, Республика Беларусь*

*Научный руководитель: Зорько М.И. – ассистент кафедры ИКТ*

**Аннотация.** В материалах доклада рассматриваются два варианта экспериментальной установки системы видеонаблюдения на основе комплекта с использованием четырех или восьмиканального (4/8) гибридного 5 в 1 видеорегистратора к которому подключены первоначально две AHD камеры (720p & 960p & 1080p несжатый видеопоток), две аналоговые камеры (960H несжатый видеопоток) видеонаблюдения с ИК подсветкой и две IP видеокамеры (IP сжатый видеопоток) и т.д. Результаты исследований будут использоваться в лабораторном практикуме по учебной дисциплине Системы прикладного телевидения, а также Системы телевизионного и звукового вещания в седьмом семестре периода обучения студентов по специальности 6-05-0611-06 Системы и сети инфокоммуникаций по профилю Телевизионные и мультимедийные системы в соответствии с описанием и порядком выполнения лабораторных работ, посвященных исследованию основных вопросов построения и функционирования цифровых телевизионных систем.

**Ключевые слова:** Система видеонаблюдения, видеокамера, формат кадра, видеорегистратор, ИК подсветка, стереоскопический способ, определение дальности объекта.

***Введение.*** Актуальность исследования обусловлена необходимостью внедрения инновационных технологий в учебный процесс с практической точки зрения совершенствования целевых компетенций студентов в области защиты объектов и территориальных районов.

Данная статья предназначена для изучения принципов проектирования, построения и

эксплуатации стереоскопических систем в приложении к технологиям видеонаблюдения. Предлагаемая полезная модель лабораторной установки обладает преимуществами, выявленными в ходе сравнения четырех и восьми-камерной версии, а также файловой системой хранения данных и опцией распознавания лиц в ракурсной системе регистрации объектов в поле видения комбинированных оптико-электронных преобразователей. Также присутствует функция видеоконтроля за мобильными объектами в условиях экстремальной освещенности и возможность просмотра динамических изображений на экранах дополнительных видеоконтрольных устройств, которые располагаются в пределах досягаемости на основе стереоскопического способа определения дальности до объекта штатными оптико-электронными преобразователями видеокамер в зоне действия системы видеонаблюдения.

В рассматриваемых вариантах предлагаемой установки используются способы определения дальности до объекта от места расположения видеокамер с базилярным разнесением последних до полутора метров во всех направлениях наблюдения с перекрытием азимутальных плоскостей в круговой зоне видеонаблюдения.

***Основная часть.*** Предметом исследований являются вопросы обработки стереоскопических изображений. Они основаны на использовании технических средств, позволяющих получить от пространственно-разнесенных видеокамер изображения с учетом прогнозируемой дальности наблюдаемых объектов. При этом, их положение в пространстве может носить динамический характер по признаку детекции движения, что позволит наблюдателю выбирать ракурс с учетом приоритета наведения конкретной видеокамеры по важности контролируемых элементов и признаков деталировки на изображении с целью повышения их разборчивости и масштаба фоновых элементов кадра.

На рисунке 1 показан фрагмент лабораторной установки, а именно форматирование кадра на экране устройства отображения с учетом использования четырех проводных, а также двух видеокамер, работающих по стандарту H.265+ с доступом к просмотру изображений по Wi-Fi сети, например, в мобильном приложении.

Рисунок 1 – Форматирование кадра на экране устройства отображения

Кроме того, справа на экране видна лента видео аналитики, учитывающая перемещение объекта в контролируемой зоне наблюдения.

Учитывая масштабируемость видеорегистратора с точки зрения количества технических средств и направлений видеоконтроля (до двенадцати направлений контроля) можно гарантировать, что увеличение числа используемых опций в составе установки приведет к выбору контролируемого пространства на высотах, преобладающих над точками подвеса видеокамер в купольной области для рассматриваемого ранее варианта, а именно применения дополнительных камер с опцией, в том числе, тепловизинного контроля над местом размещения видеооборудования, контролирующего в реальном времени наземную часть особо охраняемого объекта. При этом использование видеокамер с разрешением 1280x720 (1Мп), 1920x1080 (2Мп) и 2592x1944 (5Мп) обеспечит кратное увеличение формируемых кадров в соотношении их активных площадей кадра для сравнения 1 Мп к 2 Мп равным коэффициенту масштабируемости в 2,25 раза, а для случая учета соотношений – 2 Мп к 5 Мп равным коэффициенту масштабируемости в 2,43 раза соответственно. Тем самым у наблюдателя появится возможность контролировать большее объектовое пространство, с учетом увеличения числа беспроводных каналов видеоконтроля посредством Wi-Fi до четырех штук.

Данное решение уменьшит «слепые» зоны в местах развертывания гибридной системы видеонаблюдения.

Дальнейшее совершенствование лабораторной установки возможно с учетом дополнения ее каналом звукового сопровождения в контролируемых зонах, а также IP коммутатором, роутером, интернет и выходом в облачный сервис с последующим контролем на экранах компьютера, смартфона или планшета.

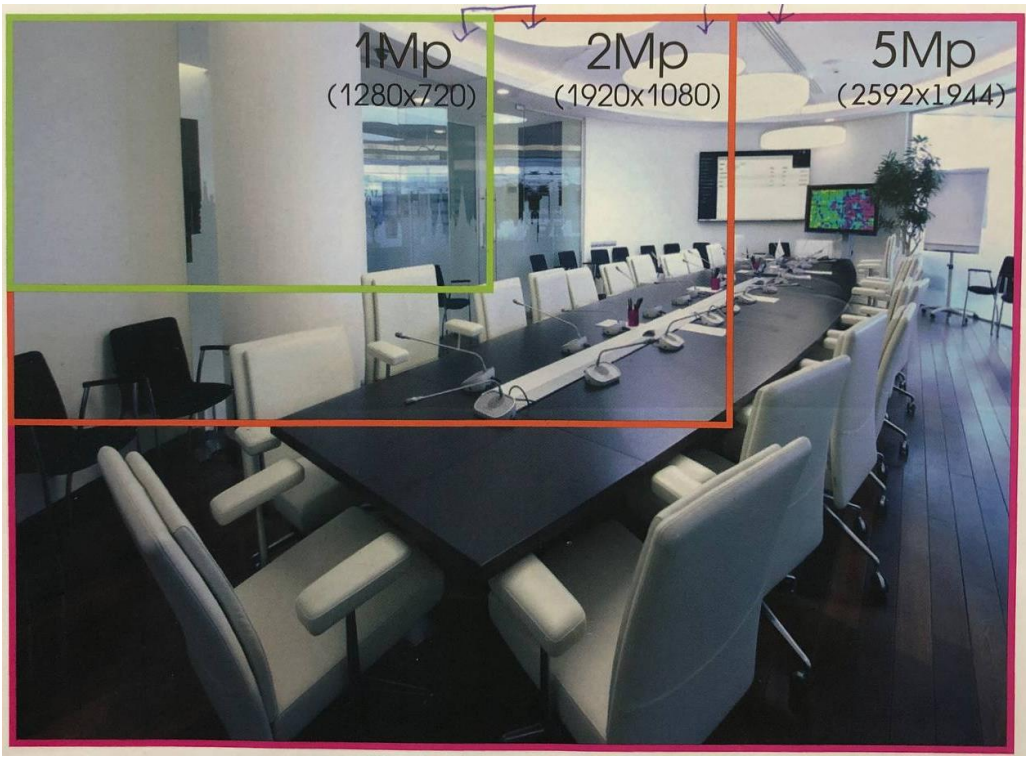



Рисунок 2 – Масштабирование кадра контролируемого изображения.

***Заключение.*** Лабораторная установка функциональна и допускает бюджетное расширение опций на основе пользовательских запросов, в части, подробного изучения стереоскопических способов на основе формирования пространственных образов виртуальных моделей стереоизображений определения дальности до объекта с обработкой реальных видео сюжетов в рамках учебного процесса по дисциплинам Системы прикладного телевидения, а также Системы телевизионного и звукового вещания для специальности 6-05-0611-06 Системы и сети инфокоммуникаций по профилю Телевизионные и мультимедийные системы. Финансирование на поддержание работоспособности не требуется. Срок годности неограничен.

## *Список литературы*


*1. Системы видеонаблюдения. Основные задачи. [Электронный ресурс]. ? Электронные данные. ? Режим доступа :http://www.telemultimedia.ru/.*

*2. Справочник по технике видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек; пер. с нем. ? М.: Техносфера, 2010. – 544 с.*

*3. Видеокамеры. [Электронный ресурс]. – Электронные данные. – Режим доступа: http://ru.wikipedia.org/wiki.*

*4. Гедзберг, Ю. М. Охранное телевидение / Ю. М. Гедзберг. – М. : Горячая Линия – Телеком, 2006. – 312 с.*

*5. YCC365Plus Smart HD Camera.*

*6. Комплект видеонаблюдения GINZZU HK-440N.*

*7. IP-камера IMILAB Home Security Camera Basic 1080p (CMSXJ16A).*


UDC 621.397.42

## THE STUDY OF A 4/8-CHANNEL HYBRID 5 IN 1 DVR AND 2/4 HD VIDEO SURVEILLANCE CAMERA WITH IR ILLUMINATION BASED ON A STEREOSCOPIC METHOD FOR DETERMINING THE DISTANCE TO AN OBJECT

*Cherepova E.V. Mihalionok K.A., Tikhankova P.I., Loban V.V.*

*gr.162901*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Zorko M.I. – assistant of the ICT department*

**Annotation**. The materials of the report consider two options for the experimental installation of a video surveillance system based on a kit using a four or eight-channel (4/8) hybrid 5 in 1 DVR to which two AHD cameras (720P & 960p & 1080p uncompressed video stream), two analog cameras (960H uncompressed video stream) video surveillance with IR illumination and two IP video cameras are connected (IP compressed video stream), etc. The results of the research will be used in a laboratory workshop on the academic discipline of Applied television systems, as well as television and audio broadcasting systems in the seventh semester of the student's study period in the specialty 6-05-0611-06 Infocommunication systems and networks in the profile of Television and multimedia systems in accordance with the description and procedure of laboratory work devoted to the study of the main issues of the construction and functioning of digital television systems.

**Keywords:** Multimedia technologies, video surveillance system, video camera, frame format, DVR, IR backlight.

УДК 004.75

## РЕАЛИЗАЦИЯ НЕЗАВИСИМОЙ СИСТЕМЫ КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ

С.П. СПОСОБ[1], Л.С. ЛАЗУТА[2], П.В. БУТЬКО[3]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», старший преподаватель*
[2]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, аспирант*
[3]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, магистр*

Современная образовательная система сталкивается с возрастающей потребностью в разработке инновационных методов контроля знаний студентов, особенно на фоне распространения онлайн-образования и дистанционных форм обучения. В данных условиях проблема оценки знаний приобретает новые измерения, что требует применения новаторских подходов, направленных на повышение эффективности и объективности оценочного процесса.

Применение передовых технологий, таких как искусственный интеллект и блокчейн, является ключевым направлением в разработке систем контроля знаний. Искусственный интеллект способствует автоматизации процесса оценки, минимизации субъективных факторов и обеспечению более точной и объективной оценки студенческих работ. Блокчейн-технологии гарантируют безопасность и надежность данных, предотвращая возможные манипуляции и фальсификации результатов. Важно подчеркнуть, что современное образование нацелено на повышение качества обучения и совершенствование образовательного процесса. Внедрение новейших технологий в системы контроля знаний улучшает использование образовательных ресурсов, мотивацию студентов и развитие их учебных навыков.

Первым этапом реализации системы является создание пользовательского интерфейса, включающего в себя несколько ключевых элементов. В интерфейсе предусмотрена страница для ознакомления с системой, которая обеспечивает первичное введение пользователя в функционал и возможности системы. Также разрабатывается окно авторизации, позволяющее идентифицировать пользователей и предоставлять доступ к соответствующим уровням системы. Личный кабинет реализован с возможностью выбора ролей: учащегося, преподавателя и администратора системы. Каждая из этих ролей обладает индивидуальными правами доступа к функциям и ресурсам, что способствует эффективной и безопасной работе с системой в соответствии с задачами и полномочиями каждого пользователя.

Следующим этапом в реализации системы является интеграция с крупным сервисом, использующим технологию GPT, который поддерживает обработку запросов через API. Для обеспечения качественной обработки запросов требуется разработка специализированных промпт-инструкций. Эти инструкции должны четко определять процедуры обработки, оценки и формирования рекомендаций по экзаменационным ответам. Промпт-инструкции представляют собой детализированные указания, которые настраивают алгоритмы GPT на выполнение специфических задач в контексте анализа студенческих ответов. Это включает в себя точную интерпретацию вопросов, адекватную оценку ответов и генерацию конструктивных предложений для улучшения учебного процесса.

Тщательно разработанные промпт-инструкции способствуют повышению точности и объективности оценок, что является критически важным для образовательных учреждений, стремящихся к обеспечению высоких стандартов образовательной деятельности. Внедрение такой системы позволяет автоматизировать процесс оценки, снижая человеческий фактор и время, затрачиваемое на коррекцию и оценку студенческих работ.

Веб-интерфейс должен соответствовать всем требованиям, предъявляемым к процессу сдачи экзамена. Это включает в себя предоставление детального описания

процесса сдачи, доступ к полному списку экзаменационных вопросов и интеграцию таймера для ограничения времени на ответ. Кроме того, интерфейс должен включать функции контроля за действиями пользователей в системе, что позволит администраторам получать отчёты о возможных попытках нарушения правил сдачи.

Необходимо обеспечить, чтобы веб-интерфейс поддерживал высокий уровень безопасности и прозрачности. Функциональность должна быть реализована таким образом, чтобы обеспечивать точное отслеживание действий каждого пользователя, включая вход в систему, перемещение между вопросами и совершение попыток ответа. Эти данные следует анализировать для выявления аномалий или поведения, которое может указывать на попытки манипуляции или нечестной сдачи.

В соответствии с установленным порядком работы с моделями GPT для экзаменационных систем, каждый экзаменационный вопрос должен включать три основных компонента: формулировку вопроса, ожидаемый ответ и детали нюансов оценки. Такой подход позволяет установить чёткие и объективные критерии для оценки ответов, обеспечивая таким образом качественное и последовательное измерение уровня знаний студентов.

Формулировка вопроса должна быть ясной и точной, чтобы минимизировать вероятность неправильного толкования задания студентами. Ожидаемый ответ должен чётко описывать, какие элементы ответа считаются корректными и полными, облегчая процесс проверки и уменьшая субъективность оценки. Нюансы оценки описывают специфические аспекты ответа, которые нужно учитывать при оценке, включая степень детализации ответа, точность и соответствие общепринятым научным или практическим нормам.

Такая структурированная подготовка вопросов способствует повышению эффективности образовательного процесса и обеспечивает более высокий уровень справедливости и объективности при оценке экзаменационных работ.

В качестве итога сдачи экзамена студент и преподаватель должны получить развернутый отчет по результатам проверки. Данный документ будет включать в себя подробное изложение действий студента во время экзамена, а также анализ предоставленных ответов. Отчет предоставит объективную оценку выполненных заданий, отражая точность и полноту ответов, соответствие предварительно установленным критериям оценки и любые замеченные отклонения от нормы.

Компонент отчета, касающийся действий студента, будет содержать хронологию и контекст совершенных операций в системе во время экзамена, включая время ответов, переходы между заданиями и возможные нарушения регламента. Обзор ответов предоставит детализированный анализ каждого ответа, включая оценку его правильности, полноты и соответствия установленным требованиям. Также будут указаны рекомендации для улучшения знаний студента и указания на типичные ошибки.

Широкий спектр требований к процедуре сдачи экзаменов и возможности искусственного интеллекта обеспечивают основу для интенсивной интеграции различных инструментов, способствующих проведению экзаменационных процессов. В области безопасности может быть реализована интеграция блокчейн-технологий, что обеспечивает повышенную защиту данных и прозрачность в документации процессов оценки. Это позволяет достигнуть необходимого уровня надежности и снизить риск манипуляций результатами.

Для проведения специализированных экзаменов предусмотрена возможность интеграции в интерфейс экзаменационного окна дополнительных полей, таких как инструменты для решения математических задач, построения графиков, создания

графических изображений, а также веб-интегрированная среда разработки для выполнения программных заданий. Это позволяет студентам демонстрировать свои умения в различных дисциплинах и обеспечивает преподавателю комплексные данные для оценки.

Результатом разработки и интеграции данной системы является создание комплексной платформы, обеспечивающей эффективное проведение и оценку экзаменов с использованием передовых технологий. Эта система объединяет функциональные возможности искусственного интеллекта и блокчейн-технологий, что позволяет значительно улучшить точность, безопасность и надежность процесса экзаменации.

Интеграция искусственного интеллекта способствует автоматизации административных задач и оценки ответов, что снижает возможность субъективного влияния и повышает объективность оценок. Блокчейн, в свою очередь, вносит в процесс неизменяемость и прозрачность регистрации результатов, предотвращая фальсификацию данных и обеспечивая верифицируемость записей.

Кроме того, разработанная система обладает адаптивностью к различным академическим дисциплинам и может поддерживать разнообразные форматы ответов, включая текстовые ответы, графические изображения и программный код. Это делает платформу универсальным инструментом для проведения экзаменов в образовательных учреждениях и профессиональных сферах, где требуется демонстрация конкретных умений и знаний.

УДК 004.75

## МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЦЕЛОСТНОСТИ СЕТИ ИНТЕРНЕТ ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

*Лазута Л.С., аспирант,*

*Белорусская государственная академия связи*
*г. Минск, Республика Беларусь*

*Карпук А.А. – канд. техн. наук*

Аннотация. Осуществлен анализ методов обеспечения безопасности и целостности сети Интернет вещей с использованием технологии блокчейн. Основное внимание уделено ключевым аспектам блокчейна, таким как децентрализация, неизменяемость и прозрачность данных, которые способствуют повышению безопасности данных в сетях IoT. Особое внимание уделено необходимости разработки и внедрения эффективных механизмов консенсуса и умных контрактов для обеспечения безопасности, управления и сохранения целостности данных.

Сеть Интернет вещей (Internet of Things, IoT) [1] определяется как глобальная инфраструктура для информационного общества, обеспечивающая продвинутое взаимодействие между физическими и виртуальными объектами через использование информационных и коммуникационных технологий. Концепция IoT [2] включает в себя широкий спектр устройств, от бытовых приборов до сложных промышленных инструментов, которые собирают, обмениваются и обрабатывают данные в реальном времени. Эти устройства оснащены датчиками и актуаторами и связаны через сетевые технологии, позволяющие им действовать автономно и кооперативно для достижения общих задач и улучшения качества жизни и операционной эффективности.

Эти понятия формируют фундамент, на котором строится архитектура Интернета вещей, обеспечивая его функциональность, масштабируемость и безопасность. Поскольку системы IoT включают множество устройств, обменивающихся данными и выполняющих различные функции, они сталкиваются с серьезными проблемами безопасности и целостности данных [3]. Неизбежные сбои программного и аппаратного обеспечения,

несанкционированный доступ и атаки вредоносного ПО делают системы уязвимыми. Для решения этих проблем применяются механизмы защиты, направленные на обнаружение и нейтрализацию угроз, а также восстановление системы после инцидентов. Однако, учитывая объем и разнообразие данных, обрабатываемых устройствами IoT, существующие методы часто оказываются недостаточными для обеспечения адекватной защиты [4]. Это требует внедрения более продвинутых технологий, таких как блокчейн, которые могут предложить дополнительные уровни защиты благодаря своим свойствам децентрализации и неизменяемости данных. Таким образом, для повышения безопасности и устойчивости систем IoT необходимо использовать комплексные и интеллектуальные подходы, включающие современные методы машинного обучения для анализа и обработки данных, собираемых с разнообразных устройств.

Технология блокчейн предлагает ряд методов для повышения безопасности и целостности данных в сетях IoT. Во-первых, система аутентификации устройств IoT на базе блокчейна позволяет надежно верифицировать каждое устройство в сети, используя децентрализованный и неизменяемый реестр, что значительно снижает риск несанкционированного доступа. Во-вторых, система отслеживания состояния устройств IoT обеспечивает постоянный мониторинг и запись всех изменений состояний устройств в блокчейн, что упрощает процесс обнаружения аномалий и неисправностей в режиме реального времени. Третий метод, система управления доступом к данным IoT, использует блокчейн для контроля и регулирования доступа к данным, предоставляя устойчивую к взлому платформу для хранения и обмена данными.

Авторизация представляет собой передовой метод обеспечения контроля доступа к ресурсам и управления ими [5]. Этот метод использует уникальные свойства блокчейна, такие как децентрализация, неизменяемость и прозрачность, для создания надежной системы авторизации. В блокчейне каждое устройство IoT может иметь уникальный идентификатор, ассоциированный с соответствующими ключами доступа, что позволяет точно контролировать и верифицировать права доступа без необходимости центрального управляющего узла [6].

При использовании блокчейна для авторизации, все запросы на доступ и изменения прав доступа записываются в надежный и немодифицируемый реестр, что обеспечивает полную прозрачность и отслеживаемость всех операций. Такой подход значительно усложняет несанкционированное изменение или удаление прав доступа, поскольку любые изменения в блокчейне требуют консенсуса между участниками сети. Этот метод также обеспечивает высокий уровень безопасности, поскольку изменение данных в блокчейне требует согласия большинства участников сети, что снижает риск возможных атак или мошенничества. Благодаря использованию уникальных идентификаторов устройств IoT, связанных с соответствующими ключами доступа, система обеспечивает точную верификацию прав доступа, что повышает безопасность и управляемость доступа к ресурсам.

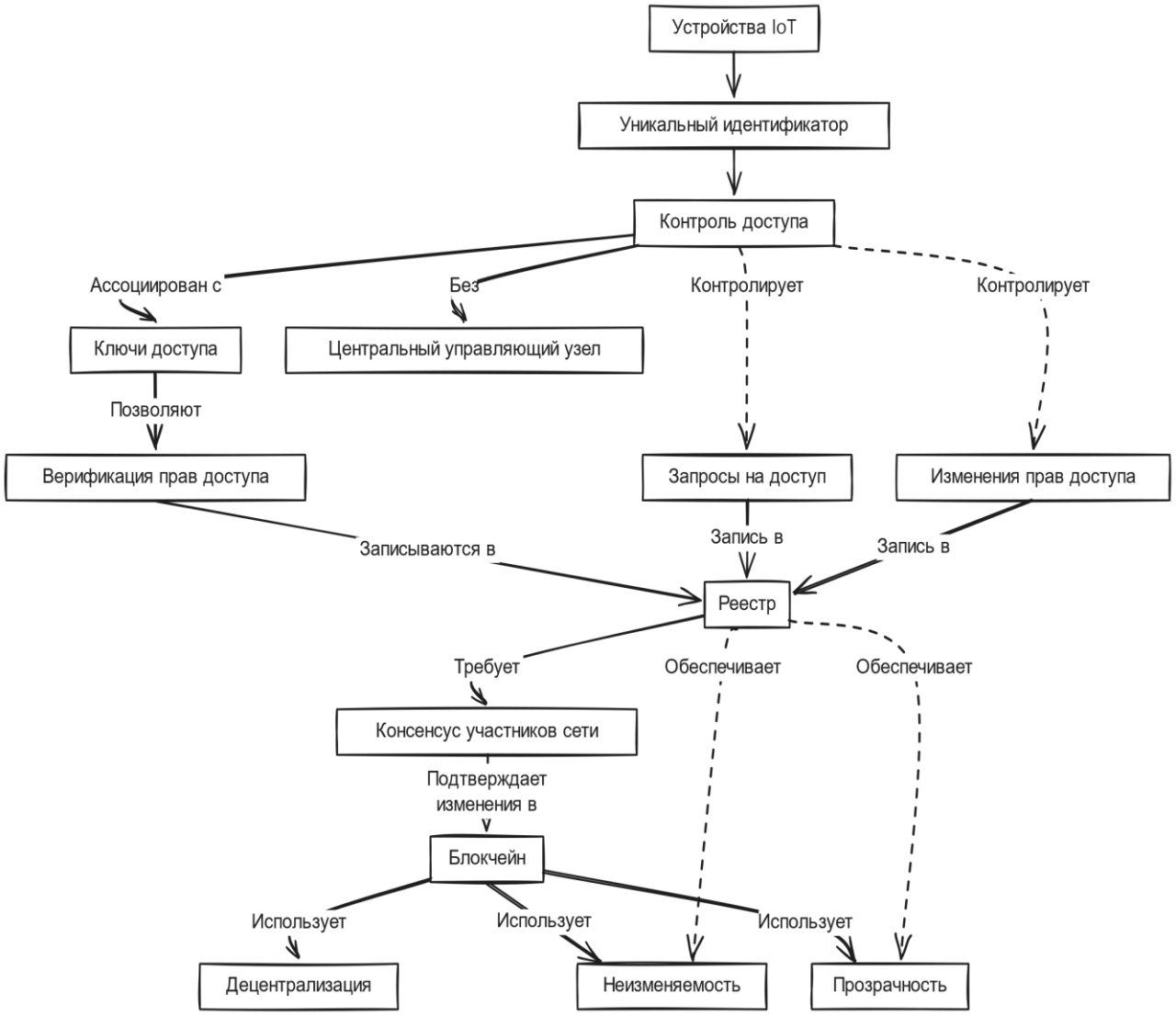



Рисунок 1 – Авторизации на основе блокчейна для управления доступом устройств IoT

Мониторинг и обновление систем в рамках IoT являются критически важными процессами для поддержания безопасности, стабильности и функциональности устройств. Эти процессы включают сбор и анализ данных о состоянии устройств, что позволяет оперативно выявлять неисправности или уязвимости. Системы мониторинга должны обеспечивать непрерывное слежение за параметрами работы устройств, такими как использование памяти, загрузка процессора, температура и сетевая активность. Данные, собранные в процессе мониторинга, анализируются для определения отклонений от нормы, которые могут указывать на возможные сбои или попытки безопасностных нарушений. Процесс обновления включает разработку и распространение патчей или новых версий программного обеспечения, что обеспечивает исправление обнаруженных уязвимостей и добавление новых функций. Обновления должны распространяться автоматизированно и безопасно, чтобы минимизировать перерывы в работе и предотвратить возможность внедрения вредоносного кода в процессе их установки. Важно, чтобы процедуры мониторинга и обновления были интегрированы в единую систему управления, что позволяет обеспечить централизованное контролирование и управление всеми аспектами работы устройств IoT.

***Список использованных источников:***

*1. Aliu, O.G. "A Survey Of self Organisation in Future Cellular Networks." IEEE Communications Surveys Tutorials. Vol. 15. 2013. P. 336-361.*

*2/ Klaine P.V. "A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks." IEEE Communications Surveys Tutorials. Vol. 19, no. 4. 2017. P. 2392–2431.*

*3. Аверченко, И.Б. "Блокчейн технологии в индустрии интернета вещей." Гарвардское бизнес-ревью. 2017. № 3. С. 45-49.*

*4. Джонсон, Д. "Блокчейн технологии для интернета вещей." IoT Solutions World Congress. 2016.*

*5. Дориан, Н. "Blockchain: Blueprint for a New Economy." Sebastopol: O'Reilly Media, 2015. 152 p.*

*6. Бутерин, В.Э. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." GitHub. 2014.*

# СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ»

УДК 53.089.6

## МЕТОДИКА ОПРЕДЕЛЕНИЯ АБСОЛЮТНОЙ ПОГРЕШНОСТИ ИЗМЕРЕНИЙ РАССТОЯНИЙ ОПТИЧЕСКИМ РЕФЛЕКТОМЕТРОМ MTP 6000

*Ковалев Д.В., Орехов А.К.*

*гр.267041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белошицкий А.П. – кандидат технических наук, доцент*

**Аннотация.** В материалах доклада рассматривается разработанная методика определения абсолютной погрешности измерения расстояний до мест неоднородностей и соединений оптического волокна (ОВ) с помощью оптического рефлектометра MTP 6000. Приводятся функциональные возможности этого прибора и принцип его работы.

**Ключевые слова:** Оптический рефлектометр, измерения расстояний, погрешность, методика.

***Введение.*** Для достижения требуемых параметров передачи волоконно-оптических линий связи (ВОЛС) и их высоких эксплуатационных качеств большую роль имеет метрологическое обеспечение (МО) строительства и технической эксплуатации ВОЛС. Одной из важных задач МО является контроль метрологических характеристик (МХ) используемых измерительных приборов. На разных стадиях жизненного цикла приборов этот контроль осуществляется при проведении государственных испытаний, поверки, калибровки и метрологической экспертизы. Эти работы по метрологической оценке выполняются с использованием специально разработанных научно-обоснованных методик.

В докладе рассматривается разработанная методика определения абсолютной погрешности оптического рефлектометра MTP 6000 при измерении расстояний до мест неоднородностей и соединений ОВ.

***Основная часть.*** Прибор MTP 6000 [1] предназначен для измерения характеристик оптических волокон и волоконно-оптических компонентов и может выполнять функции следующих приборов:

— оптического рефлектометра;

— источника непрерывного оптического излучения;

— измерителя мощности оптического излучения;

— источника видимого излучения.

При работе в режиме оптического рефлектометра прибор МТР 6000 позволяет измерять затухания в ОВ и их соединениях, длины ОВ и волоконно-оптических линий, расстояния до мест неоднородностей и соединений ОВ.

Принцип работы оптического рефлектометра МТР 6000 основан на измерении сигнала обратного рэлеевского рассеяния при прохождении по ОВ мощного одиночного оптического импульса. Слабый сигнал обратного рассеяния регистрируется чувствительным оптическим приемником, преобразуется в цифровую форму и многократно усредняется для уменьшения влияния шумов аппаратуры. В результате обработки этого сигнала формируется рефлектограмма, по которой определяются параметры ОВ и ВОЛС.

Для генерации непрерывного оптического излучения в приборе МТР 6000 используются те же лазерные диоды и оптический разветвитель, что и для рефлектометра. Выходом источника непрерывного излучения является оптический разъем рефлектометра. Мощность излучения стабилизируется с помощью внешнего фотодиода и схемы стабилизации мощности.

Для определения абсолютной погрешности измерения расстояний оптическим рефлектометром МТР 6000 в качестве эталонного средства был выбран оптический генератор ОГ-2-1. Метрологические характеристики ОГ-2-1 [2] полностью удовлетворят требованиям решаемой задачи.

Определение погрешности проводят при минимальных значениях разрешения (интервала дискретизации сигнала обратного рассеяния), допустимых для данного диапазона измеряемых расстояний. Одновременно проверяют значения диапазонов измерения расстояний.

Для определения погрешности измерения расстояний необходимо соединить выход генератора ОГ-2-1 со входом рефлектометра МТР 6000 и включить генератор. С помощью кнопки F2 на передней панели рефлектометра выбрать окно «Параметры измерения» показанное на рисунке 1.

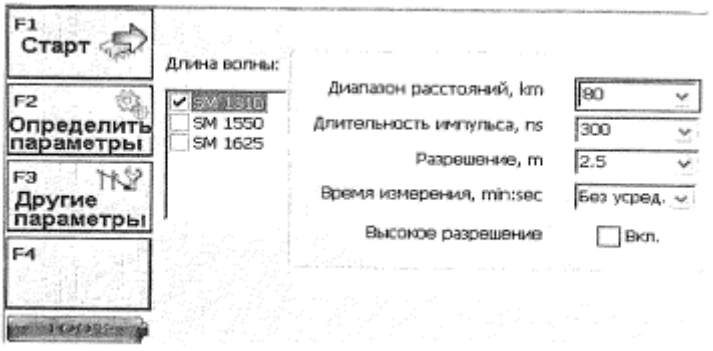



Рисунок 1 – Изображение окна «Параметры измерения» на дисплее рефлектометра МТР 6000.

В появившемся окне «Параметры измерения» установить следующие значения параметров:

длина волны - минимальная из 1310, 1490, 1550, 1625 нм для одномодовых рефлектометров или минимальная из 850, 1300 нм для многомодовых рефлектометров;

диапазон расстояний: 2 км;

длительность импульса: 100 нс;

разрешение: 0,16 м;

время измерения: без усреднений;

остальные параметры — по умолчанию.

После установки параметров измерения нажать кнопку ENTER.

Затем с помощью кнопки F3 выбрать окно «Дополнительные параметры измерения». В этом окне установить следующие значения параметров:

коэффициент обратного рассеяния, ВС: -80,0 dB для длины волны 1310нм, -81 dB, для длин волн 1490, 1550, 1625 нм, -72 dB, для длины волны 850 -75 dB, для длины волны 1300 нм.

Показатель преломления, n: 1,47500.

Остальные параметры — по умолчанию.

Затем установить в меню" Параметры" управляющей программы оптического генератора ОГ-2-1 значение показателя преломления, равным 1,475.

Нажать кнопку «Расстояние» управляющей программы оптического генератора ОГ-2-1, при этом откроется окно «Проверка шкалы расстояний», в нем следует установить:

диапазон измеряемых расстояний — 2 км;

длину волны - в соответствии с выбранной длиной волны рефлектометра;

длительность измерительного импульса - 100 м;

число измерительных импульсов - 5;

положение 1-го измерительного импульса - 400 м.

Нажать кнопку «Зафиксировать параметры импульсов», затем нажать кнопку «Допустимая погрешность» и установить параметры для расчета допустимой погрешности прибора:

$\Delta L_0$= 0,5м

$\Delta L_{sample}$= dL, м (минимальной разрешающей способности прибора для заданного диапазона измеряемых расстояний);

SL = 0,00003.

Запустить прибор МТР 6000 на измерение в режиме без усреднения.

С помощью аттенюаторов оптического генератора ОГ-2-1 установить амплитуду импульсов на экране прибора на 2-5 дБ ниже верхней границы вертикальной шкалы прибора. Горизонтальную линию, имитирующую сигнал обратного рассеяния на рефлектограмме, устанавливают на уровне (11±1) дБ ниже плоской части вершины импульса, для многомодовых рефлектометров, и на уровне (15±l) дБ ниже плоской части вершины импульса, для одномодовых рефлектометров.

После завершения работы прибора МТР 6000 в этом режиме передвинуть маркер: «В» в крайнее правое положение и прочитать максимальное значение шкалы расстояний, это значение является диапазоном измерения расстояний.

С помощью маркеров прибора МТР 6000 измерить расстояния от начала координат до точки пересечения горизонтальной линии, имитирующей сигнал обратного рассеяния, и переднего фронта каждого импульса. При этом используется максимальная растяжка масштаба по шкале затухания и шкале расстояний.

Занести полученные значения в соответствующий столбец ("Рефлектометр") в окне «Проверка шкалы расстояний» управляющей программы оптического генератора, для дальнейшего автоматического расчета погрешностей по формуле:

$$\Delta l_i = 1.1 * \sqrt{\Delta L_0^2 + \left(L_j - L_{0j}\right)^2} \quad (1)$$

где $\Delta L_0$, м — пределы допускаемой основной абсолютной погрешности при

воспроизведении расстояния оптического генератора ОГ-2-1

$L_j$, м- расстояние до j-го импульса, измеренное по экрану прибора МТР 6000,

$L_{0j}$, м- расстояние до j-го импульса, задаваемое оптическим генератором ОГ-2-1.

П о в т о р и т ь измерения для всех диапазонов расстояний, указанных в таблице 1 для данного прибора, по описанной выше методике. Устанавливать длительности и положение первого измерительного импульса согласно таблице 1.

Т а б л и ц а 1

| Длительность измерительного импульса, м | Положение первого измерительного импульса, м | Диапазоны измерения расстояний, км | |
|---|---|---|---|
| | | Многомодовый рефлектометр | Одномодовый рефлектометр |
| 100 | 400 | 2 | 2 |
| 300 | 400 | 10, 20, 40 | 10, 20, 40 |
| 1000 | 400 | 80 | 120, 240 |

Р е з у л ь т а т ы проверки считают удовлетворительными, если:

- максимальные значения шкалы расстояний соответствуют диапазонам измеряемых расстояний таблицы 1;
- полученные значения пределов погрешностей в столбце «Погрешность» не превышают пределов допустимой абсолютной погрешности измерения расстояния, указанных в столбце «Допуск» в окне «Проверка шкалы расстояний» управляющей программы оптического генератора, т. е. удовлетворяют условию:

$$\Delta L_j \leq dl + dL + 3 * 10^{-5} * L_{0j} \quad (2)$$

г д е допустимое значение начального сдвига dl 0,5 м;

$dL$ - установленное значение разрешения (интервала дискретизации сигнала обратного рассеяния), м;

$L_{0j}$— расстояние, задаваемое оптическим генератором ОГ-2-1, м.

***Заключение.*** Разработанная методика позволяет определить абсолютную погрешность измерения расстояний до мест неоднородностей и соединений ОВ с помощью оптического рефлектометра МТР 6000.

### *Список литературы*

1. *Руководство по эксплуатации оптического рефлектометра МТР 6000*
2. *Руководство по эксплуатации оптическим генератором ОГ-2-1.*

UDC 53.089.6

**METHODOLOGY OF DETERMINATION OF ABSOLUTE ERROR OF DISTANCE MEASUREMENTS BY OPTICAL REFLECTOMETER MTR 6000**

*Kovalev D.V., Orekhov A.K.*

*gr.267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Supervisor: A.P. Beloshitsky - Candidate of Technical Sciences, Associate Professor.*

**Annotation**. In the materials of the report the developed technique of determination of absolute error of measurement of distances to the places of inhomogeneities and connections of optical fiber (OF) with the help of optical reflectometer MTR 6000 is considered. The functional capabilities of this device and the principle of its operation are given.

**Keywords**: information memorization, web application, Leitner's method

УДК 631.317.08

## МЕТОДИКА ОЦЕНИВАНИЯ НЕОПРЕДЕЛЕННОСТИ РЕЗУЛЬТАТОВ ИЗМЕРЕНИЙ, ВЫПОЛНЕННЫХ С ПОМОЩЬЮ ЭТАЛОНА ЕДИНИЦЫ ОСЛАБЛЕНИЯ ЭЛЕКТРОМАГНИТНЫХ КОЛЕБАНИЙ

*Маскей М. Ш. гр.367041, Касперович М. М. научный сотрудник центра 1.9*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белошицкий А. П. – кандидат технических наук, доцент*

**Аннотация.** В материалах доклада рассматривается разработанная методика оценивания неопределенности результатов измерений, выполненных с помощью эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.

**Ключевые слова:** методика, неопределенность, эталон, ослабление, электромагнитные колебания

***Введение.*** В последнее время достигнут существенный прогресс на пути промышленного освоения миллиметрового диапазона волн. Это обстоятельство стимулировало ускоренное создание разнообразных средств измерений (СИ) этого диапазона, в том числе скалярных и векторных анализаторов цепей и измерительных аттенюаторов [1]. Для проведения работ по метрологической оценке этих СИ в Республике Беларусь отсутствует соответствующее эталонное оборудование. Научно-образовательным инновационным центром сверхвысокочастотных (СВЧ) технологий и их метрологического обеспечения (Центр 1.9) БГУИР ведутся работы по созданию национального эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц. В докладе приводится описание методики оценивания неопределенности результатов измерений ослабления, выполненных с помощью указанного эталона.

***Основная часть.*** Для проведения измерений ослабления при помощи эталона необходимо собрать измерительный тракт и выполнить калибровку эталона на измеряемой частоте. После чего подключить объект измерений и выполнить измерения. Количество измерений выбирают в зависимости от требуемой точности. Для высокоточных измерений рекомендуется провести не менее 10 повторных наблюдений.

Для оценки неопределенности результатов измерений ослабления с использованием эталона необходимо учитывать не только точность самого измерения, но и степень точности самого эталона. При этом важно провести анализ всех возможных источников ошибок и учитывать их в расчетах. Для составления модели измерения ослабления с помощью эталона были проанализированы и выявлены источники неопределённости измерений. Основными источниками неопределённости измерений для данной измерительной задачи являются: неопределенность измерения ослабления на промежуточной частоте, неопределенность измерения ослабления из-за недостаточной развязки измерительного канала, неопределенность измерения ослабления из-за нелинейности входных цепей и неопределенность измерения ослабления из-за рассогласования

измерительного тракта. При правильном учете данных неопределенностей в модели измерения можно достаточно точно определить значение ослабления.

Для оценки неопределенности была предложена следующая модель измерения:

$$A = A_{\text{и}} + \delta_{\text{ПЧ}} + \delta_{\text{н}} + \delta_{\text{из}} + \delta_{\text{расс}}, \quad (1)$$

где $A$ – результат измерений, дБ;

$A_{\text{и}}$ – измеренное значение ослабления, дБ;

$\delta_{\text{ПЧ}}$ – неопределенность измерения ослабления на промежуточной частоте ПЧ), дБ;

$\delta_{\text{из}}$ – неопределенность измерения ослабления из-за недостаточной изоляции (развязки) измерительного канала, дБ; $\delta_{\text{н}}$ – неопределенность измерения ослабления из-за нелинейности входных цепей, дБ;

$\delta_{\text{расс}}$ – неопределенность измерения ослабления из-за рассогласования измерительного тракта, дБ.

Входная величина типа А неопределенности характеризуется нормальным видом распределения с оценкой величины в децибелах. Оценка величины представлена результатами нескольких наблюдений, а стандартная неопределенность определяется из выражения:

$$u(A_{\text{и}}) = \sqrt{\frac{1}{n(n-1)} \sum_{i=1}^{n} (A_{\text{и}i} - \bar{A}_{\text{и}})^2}, \text{ дБ} \quad (2)$$

Неопределенность величины $\delta_{\text{ПЧ}}$ классифицируется как тип В и характеризуется прямоугольным видом распределения, с оценкой величины, соответствующей 0 дБ. Интервал, в котором находится значение входной величины, определяется пределами допускаемой основной абсолютной погрешности измерения ослабления на ПЧ $d_1$, а стандартная неопределенность равна:

$$u(\delta_{\text{ПЧ}}) = \frac{d_1}{\sqrt{3}}, \text{ дБ} \quad (3)$$

Неопределенность величины $\delta_{\text{н}}$ также имеет тип В, при этом она характеризуется прямоугольным видом распределения и оценкой величины, соответствующей 0 дБ. Интервал, в котором находится значение входной величины, определяется нелинейностью входных цепей $d_2$, а стандартная неопределенность определяется соотношением:

$$u(\delta_{\text{н}}) = \frac{d_2}{\sqrt{3}}, \text{ дБ} \quad (4)$$

Неопределенность величины δиз имеет тип В и описывается прямоугольным видом распределения с оценкой величины 0 дБ. Интервал, в котором находится значение входной величины, определяется значением паразитного сигнала вследствие недостаточной изоляции $d_3$, а стандартная неопределенность определяется из выражения:

$d_3$

$$u(\delta_{из}) = \frac{}{\sqrt{3}}, \text{ дБ} \quad (5)$$

Неопределенность величины $\delta_{расс}$ имеет тип В, но характеризуется распределением в форме арксинусоидальной кривой, с оценкой величины 0 дБ. Интервал, в котором находится значение входной величины, зависит от максимально возможного рассогласования в измерительном тракте $d_4$, а стандартная неопределенность равна:

$$u(\delta_{расс}) = \frac{d_4}{\sqrt{2}}, \text{ дБ} \quad (6)$$

*Неопределенность случайной составляющей.* Сигнал с выхода объекта измерений, имеет небольшие колебания амплитуды в процессе измерения. Такие колебания приводят к некоторой неопределенности в измерении ослабления. Помимо тепловых шумов с увеличением частоты флуктуации значительно увеличиваются также из-за эффекта фазового 60-я научная конференция аспирантов, магистрантов и студентов

шума. В эталоне предусмотрена возможность снижения случайной неопределенности измерения путем усреднения.

*Неопределенность измерения ослабления, обусловленная нелинейностью входных цепей.* Нелинейность присуща многим устройствам, входящим в состав эталона, однако нелинейность преобразователей частоты (смесителей) и предварительных усилителей превалирует настолько, что нелинейностью остальных устройств можно пренебречь. Уровень сигнала на СВЧ-входе смесителя должен поддерживаться как минимум на 30 дБ ниже уровня гетеродина, чтобы добиться наименьшей ошибки из-за нелинейности. Измерения должны проводиться на малых уровнях сигнала, чтобы обеспечить работу смесителей в своей линейной области.

*Неопределенность измерения ослабления из-за недостаточной развязка (изоляция) измерительного канала.* Развязка измерительного канала важна из-за паразитных сигналов, которые могут искажать результаты измерений. Влияние развязки измерительного канала проявляется в виде присутствия на входе смесителя измерительного канала паразитного сигнала с постоянной (или медленно дрейфующей) амплитудой и фазой. Пока полезный сигнал остается много больше этого паразитного сигнала, влияние последнего пренебрежимо мало. Но при уменьшении амплитуды входного измерительного сигнала с ростом измеряемого ослабления паразитный сигнал начинает искажать результат измерения, векторно (с учетом амплитуд и фаз) складываясь с полезным сигналом. Одним из наиболее часто встречающихся источников этого паразитного сигнала является наводка входного и усиленного сигнала опорного канала в измерительный канал. Поэтому изоляцией или развязкой каналов принято называть просачивание мощности из опорного в измерительный канал и выражать ее в децибелах.

Поскольку в общем случае угол при векторном суммировании полезного и паразитного сигналов неизвестен, для оценки интервала ошибки необходимо использовать наихудший случай – синфазное детектирование. В таком случае для границы интервала можно записать

$$d_3 = -20 \cdot \lg\left(1 - 10^{-\frac{A_{из} - A_x}{20}}\right), \quad (7)$$

где $A_{из}$, $A_x$ – ослабления объекта измерения и развязка между опорными измерительными каналами СВЧ тракта эталона соответственно, дБ.

*x*

$$A_{из}-A_x=20\cdot(\frac{x}{x_{из}}), \quad (8)$$

где $x$, $x_{из}$ – амплитуды сигнала через объект измерения и сигнала утечки соответственно, дБ.
*Неопределенность измерения ослабления на промежуточной частоте.* По принципу действия эталон производит перенос значения измеряемой величины на ПЧ и осуществляет сравнение его значения с низкочастотным эталонным значением (ослабление на ПЧ), которое в свою очередь имеет свою неопределенность при его определении. Эта неопределенность зависит от погрешности измерения ослабления приемником сигналов ПЧ входящим в состав эталона.
*Неопределенность измерения из-за рассогласования измерительного тракта.* Значение величины $d_4$ для расчета этой неопределенности по формуле (6) можно определить из выражения:

$$d_4=8{,}2\ [\Gamma_г\cdot\Gamma_c\cdot(K^2+1)+\Gamma_г\cdot\Gamma_1+\Gamma_c\cdot\Gamma_2], \quad (9)$$

где $\Gamma_1$, $\Gamma_2$ – коэффициентов отражения от входа и выхода объекта измеряемого устройства;

$\Gamma_Г$, $\Gamma_С$ – модули коэффициентов отражения тракта СВЧ по обе стороны (со стороны входа и выхода) измеряемого устройства; К – модуль коэффициента передачи измеряемого устройства.

***Заключение.*** Разработанная методика позволяет оценить неопределенность результатов измерения ослабления, выполненных с помощью эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.

### *Список литературы*

*1. Богуш, В. А. Векторные анализаторы цепей сантиметрового и миллиметрового диапазонов длин волн/ В. А. Богуш [и др.]. – Москва: Горячая линия – Телеком, 2019. – 328 с.*

UDC 631.317.08

## METHODOLOGY FOR ESTIMATION OF UNCERTAINTY OF THE RESULTS OF MEASUREMENTS PERFORMED USING THE STANDARD OF THE UNIT OF ATTENUATION OF ELECTROMAGNETIC OSCILLATIONS

*Maskey M.S. gr.367041, Kasperovich M.M. Research Associate of the Center 1.9*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Beloshitsky A. P. – Cand. Sc. (Tech.), associate professor*

**Annotation.** In the materials of the report the developed methodology of estimation of uncertainty of the results of measurements made with the help of the standard of the unit of attenuation of electromagnetic oscillations in the frequency range from 37.5 to 178.4 GHz is considered.

**Keywords:** methodology, uncertainty, standard, attenuation, electromagnetic oscillations

УДК 681.7.069

# МЕТОДИКИ ВЫПОЛНЕНИЯ ИЗМЕРЕНИЙ ЗАТУХАНИЯ ОПТИЧЕСКИХ ВОЛОКОН И КАБЕЛЕЙ ОПТИЧЕСКИМ ТЕСТЕРОМ ОТ-2-8

*Орехов А.К. магистрант гр.267041*

*Ковалёв Д.В. магистрант гр.267041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белошицкий А.П. – кандидат технических наук, доцент*

**Аннотация.** Доклад посвящён разработке методик выполнения измерений затухания смонтированного оптического кабеля (ОК) и оптического волокна (ОВ) с использованием оптического тестера ОТ-2-8. Приводятся описание методов измерения, метрологические характеристики оптического тестера, порядок проведения измерений.

**Ключевые слова:** оптический кабель, оптическое волокно, оптический тестер, измерение, затухание, методика.

***Введение.*** Для достижения высоких эксплуатационных показателей волоконно-оптических линий связи (ВОЛС) большую роль играет метрологическое обеспечение (МО) при их строительстве и эксплуатации. Одной из важных задач МО является разработка методик выполнения измерений (МВИ) позволяющих определять показатели качества ВОЛС с необходимой точностью и достоверностью.

В докладе рассматриваются МВИ вносимого и собственного затухания ОВ входящих в ОК смонтированной ВОЛС с использованием метода вносимых потерь, а также МВИ собственного затухания ОВ находящихся на катушке.

***Основная часть.*** Измерение затухания оптического кабеля проводится с помощью оптического тестера ОТ-2-8 методом относительных измерений. Частными случаями метода относительных измерений являются метод вносимых потерь и метод обламывания.

Основные метрологические характеристики оптического тестера представлены в таблице 1.

Таблица 1 – Основные характеристики оптического тестера ОТ-2-8

| Длина волны калибровки, нм | Стандартный диапазон измерений мощности | Высокий диапазон измерений мощности | Пределы допустимой относительной погрешности оптического излучения |
|---|---|---|---|
| 650 | от -30 до +3 дБм (от 1 мкВт до 2 мВт) | от -10 до +3 дБм (от 100 мкВт до 2 мВт) | ±12% (±0,49 дБ) |
| 850 | от -60 до +3 дБм (от 1 нВт до 2 мВт) | от -40 до +3 дБм (от 100 нВт до 2 мВт) | ±8 % (±0,33 дБ) |
| 1310, 1550 1490, 1625 | от -70 до +7 дБм (от 100 пВт до 5 мВт) | от -50 до +10 дБм (от 10 нВт до 10 мВт) | ±5 % (±0,22 дБ) |

*Метод вносимых потерь* применяется для измерения затухания обладающих уже смонтированных ОК, в которых ко входу и выходу ОВ подключены оптические соединители. Измерения затухания ОК проводят по схеме, представленной на рисунке 1.


Рисунок 1 – Структурная схема измерения затуханий ОК методом вносимых потерь

Метод вносимых потерь основан на последовательном измерении мощности оптического излучения на выходе измеряемого i-го волокна оптического кабеля $P_1$, мВт и на выходе вспомогательного оптического волокна (оптического патч-корда) $P_2$, мВт.

За результат измерений вносимого затухания i-го ОВ входящего в ОК принимается значение рассчитанное по формуле 1:

$$A_{iOB} = 10 \lg \frac{P_1}{P_2} - A_{\text{вс}}, \quad (1)$$

где: $A_{iOB}$ – затухание i-го ОВ, дБ,

$P_1$ – мощность оптического излучения на выходе измеряемого волокна, мВт.

$P_2$ – мощность оптического излучения на выходе вспомогательного оптического волокна, мВт.

Собственное затухание i-го ОВ определяется из выражения:

$$A_{iOB}^{c} = A_{iOB} - A_1 - A_2 \quad (2)$$

Затухание входного ($A_1$) и выходного ($A_2$) оптических соединителей, которые подключены к ОВ оптического кабеля, а также затухания вспомогательного ОВ ($A_{\text{вс}}$) должны быть указаны в технической документации на эти элементы.

*Метод обламывания* применяется для измерения затухания ОВ к которым не подключены оптические соединители. Измерения затухания ОВ проводят по схеме, представленной на рисунке 2.

Измерение $P_1$


Измерение $P_2$

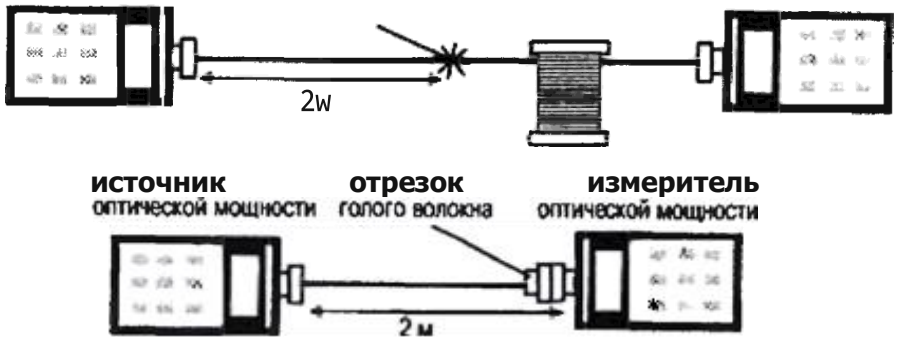



Рисунок 2 – Структурная схема измерения затуханий ОВ методом обламывания

Метод обламывания основан на сравнении значения мощности оптического излучения, измеренного на выходе измеряемого отрезка ОВ $P_1$, мВт, со значением мощности, измеренным на выходе его короткого участка, образованного за счет обламывания ОВ около 2 м от начала измеряемого образца, $P_2$, мВт. После регистрации мощности $P_1$ и $P_2$ затухание $A_{ов}$, дБ определяется по формуле 2:

$$A_{OB} = 10lg \frac{P_1}{P_2} \quad (3)$$

где: $A_{ОВ}$ – затухание ОВ, дБ;

$P_1$ – мощность оптического излучения на выходе измеряемого волокна, мВт;

$P_2$ – мощность оптического излучения на выходе короткого участка волокна, образованного за счет обламывания, мВт.

При измерении методом обламывания принципиально важно обеспечить постоянство мощности, вводимой в исследуемое волокно, и неизменность модового состава излучения. Соответственно необходимо, чтобы в процессе измерений соблюдалось постоянство условий ввода оптического излучения и сохранялось строго неизменным положение волокна в юстировочном устройстве.

***Заключение.*** Разработанная методика обеспечивает выполнение измерений затухания оптического волокна с применением метода вносимых потерь при использовании оптического тестера ОТ-2-8 (источника оптического излучения ОТ-2-8/ИИ и измерителя оптической мощности ОТ-2-8/ИМ, конструктивно объединенных в одном корпусе) и может быть распространена на аналогичные средства измерения с учетом их действительных значений погрешности.

### *Список литературы*

*1. Руководство по эксплуатации оптического тестера ОТ-2-8.*

UDC 681.7.069

## METHODS OF MEASUREMENT OF OPTICAL FIBERS AND CABLES ATTENUATION BY OPTICAL TESTER OT-2-8

*Orekhov A.K. Master student of gr.267041*

*Kovalyov D.V. Master student of gr.267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Supervisor: A.P. Beloshitsky - Candidate of Technical Sciences, Associate Professor.*

**Annotation**. The report is devoted to the development of methods for measuring the attenuation of mounted optical cable (OC) and optical fiber (OF) using optical tester OT-2-8. The description of measurement methods, metrological characteristics of optical tester, order of measurements are given.

**Keywords**: optical cable, optical fiber, optical tester, measurement, attenuation, methodology.

УДК 621.317.3

## МЕТОДИКА ПОВЕРКИ ИЗМЕРИТЕЛЯ ПАРАМЕТРОВ КАБЕЛЬНЫХ ЛИНИЙ ДЕЛЬТА-ПРО+

*Валова И.Н.*

*гр. 267041*

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь*

*Научный руководитель: Белошицкий А. П.. – кандидат технических наук, доцент кафедры ИИС*

**Аннотация.** В материалах доклада рассматривается разработанная методика поверки рефлектометра, входящего в состав измерителя параметров кабельных линий ДЕЛЬТА-

ПРО+. Приводятся метрологические характеристики поверяемого рефлектометра и выбранных эталонных средств поверки, схемы поверки и значения поверяемых точек.

**Ключевые слова:** поверка, методика, измеритель, кабельные линии

***Введение.*** Кабельные линии связи, которые еще недавно составляли основу телекоммуникационной сети нашей страны, и сейчас используется для предоставления простых, но востребованных услуг телефонии и передачи данных посредством организации прямых связей МЧС, МВД и других государственных организаций, а также для небольших частных компаний и фирм, не имеющих возможности проложить оптическую линию связи. Для качественного обслуживания кабельных телекоммуникационных сетей необходимо правильно организовать их метрологическое обеспечение (МО).

Метрологическое обеспечение означает совокупность подходов к организации измерений, конкретных методик, обработки результатов, а также измерительных приборов необходимых для контроля за эффективной работой кабельных телекоммуникационных систем. В свою очередь контроль метрологических характеристик (МХ), используемых измерительных приборов – одна из важнейших задач МО. Этот контроль осуществляется при проведении государственных испытаний, поверки, калибровки и метрологической экспертизы средств измерений с помощью специально разработанных и научно-обоснованных методик.

В докладе рассматривается разработанная методика поверки (МП) рефлектометра, входящего в состав измерителя параметров кабельных линий ДЕЛЬТА-ПРО+. МП разработаны в соответствие с требованиями [1].

***Основная часть.*** Импульсный рефлектометр измерителя ДЕЛЬТА-ПРО+ предназначен для определения расстояния до места изменения волнового сопротивления всех типов кабелей. Принцип работы рефлектометра основан на известном физическом явлении отражения зондирующих импульсов от неоднородностей волнового сопротивления исследуемого кабеля. С помощью рефлектометра можно измерить расстояние до места повреждения кабеля, определить характер повреждения, измерить расстояние между неоднородностями волнового сопротивления, определить длину кабеля и измерить коэффициент укорочения.

При поверке рефлектометра определяются его следующие основные МХ: погрешность частоты следования калибровочных меток, погрешность измерения расстояния рефлектометром, диапазон перекрываемого затухания.

Для определения вышеперечисленных МХ при поверке прибора были выбраны следующие эталонные средства поверки: частотомер Ч3-85, имеющий следующие метрологические характеристики: диапазон измерений: $1 \cdot 10^{-2}$-$2 \cdot 10^{8}$ Гц, погрешность измерения частоты менее ±0,05 %; два резистора С2-29-0,25 сопротивлением 60 Ом, погрешность ±0,5 %; ступенчатый аттенюатор API/Weinschel 115A-119A, имеющий пять стандартных диапазонов ослабления: 0-9 дБ, 0-69 дБ и 0-99 дБ с шагом 1 дБ, а также 0-60 дБ и 0-90 дБ с шагом 10 дБ.

Определение МХ поверяемого прибора

1. Определение погрешности частоты следования калибровочных меток.

Данную операцию поверки выполняют при включенном приложении «Рефлектометр» в режиме работы прибора «Калибровочные метки». В данном режиме рефлектометр вырабатывает калибровочные метки с частотой следования $f_к$=1024 кГц. Схема соединения

приборов для данной операции поверки приведена на рисунке 1.

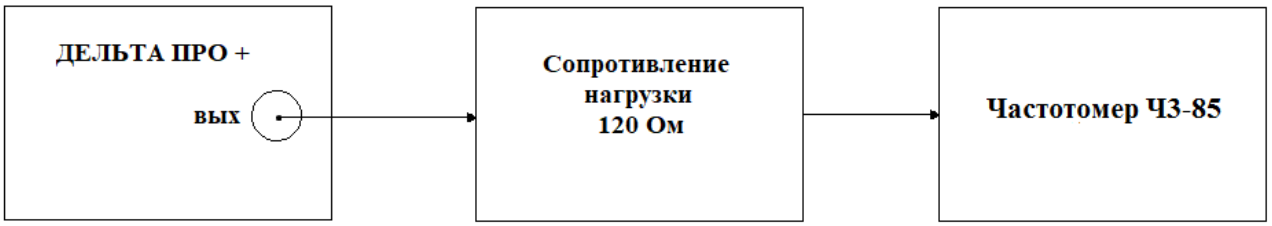



Рисунок 1 – Схема соединения приборов при определении частоты следования калибровочных меток

Сигнал с выхода прибора через нагрузочные сопротивления 120 Ом (два последовательно соединенных резистора с сопротивлением 60 Ом) подается на вход частотомера Ч3—85. С помощью частотомера измеряется частота следования калибровочных меток.

Погрешность следования калибровочных меток определяют по формуле (1):

$$\Delta f = f_{изм} - f_k, \text{ Гц}, \quad (1)$$

где Δf – абсолютная погрешность; $f_{изм}$ – частота, измеренная частотомером; $f_k$ – частота следования калибровочных меток.

Результат поверки считается удовлетворительным, если частота следования калибровочных меток находится в пределах 1024±0,5 кГц.

2. Определение погрешности измерения расстояния рефлектометром.

Операцию поверки выполняют при включенном приложении «Рефлектометр» в режиме работы прибора «Калибровочные метки».

Определение погрешности измерения расстояния проводится с помощью встроенного калибратора при установленных разрешениях: 2 м, 38 см. К выходу прибора необходимо подключить нагрузочное сопротивление 120 Ом (два последовательно соединенных резистора с сопротивлением 60 Ом). Диапазон расстояний в данном режиме по умолчанию равен 1 км. Устанавливается коэффициент укорочения 1,50 и разрешение по оси X равное 2 м. Внутреннее схемотехническое устройство прибора обеспечивает передачу калибровочных меток с выхода рефлектометра на его вход. Данные метки являются эталонными расстояниями. Изображение калибровочных меток на экране прибора показано на рисунке 2.

Нулевой курсор устанавливается на пересечении центра фронта первой метки, измерительный курсор совмещается с центром спада первой метки, и снимаются показания расстояния между курсорами $l_{12}$.

Затем измерительный курсор переводится на центр фронта второй метки, нулевой курсор переводится на пересечение центра фронта первой метки. Снимаются показания расстояния между курсорами $l_{13}$.

Переводя измерительный курсор на центр спада второй метки, при установке нулевого курсора на пересечении центра фронта первой метки, измеряется расстояние $l_{14}$.

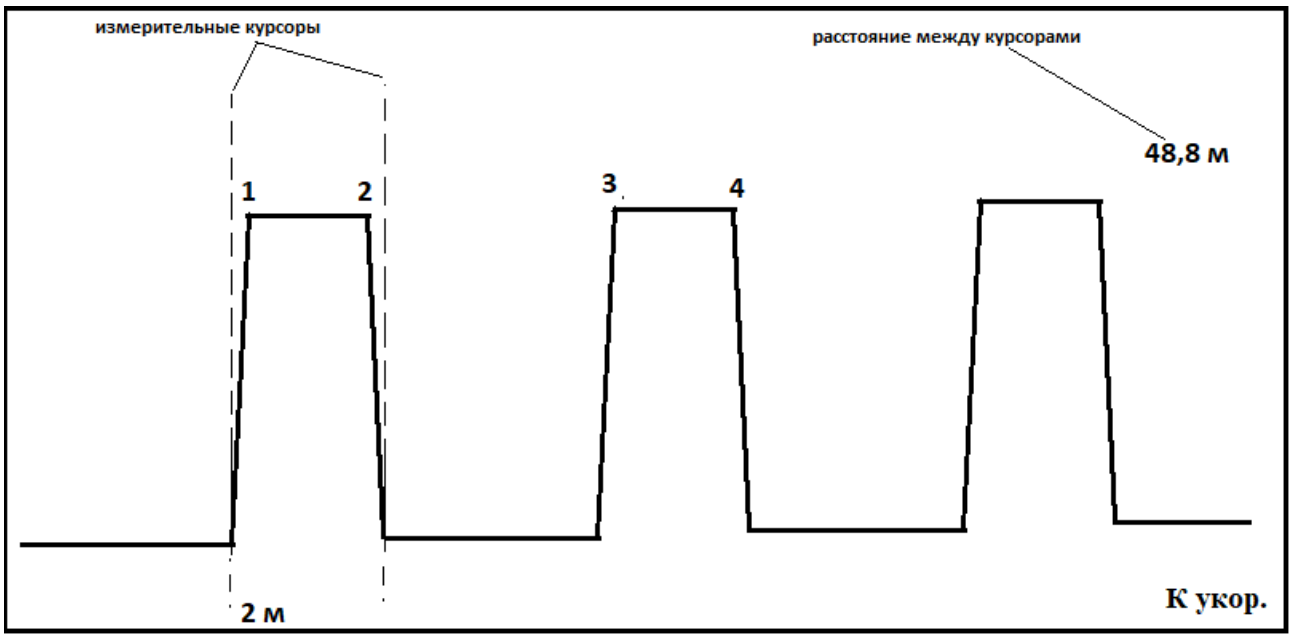



Рисунок 2 – Изображение на экране прибора калибровочных меток

Вычисляется разность между измеренными расстояниями и эталонными *lэ* расстояниями, указанными в таблице 1, по формулам 2, 3, 4:

$$\Delta l_{12}=l_{и12}-l_{э12}; \quad (2)$$
$$\Delta l_{13}=l_{и13}-l_{э13}; \quad (3)$$
$$\Delta l_{14}=l_{и14}-l_{э14}. \quad (4)$$

Полученные результаты Δ*l* не должны превышать пределы погрешности, указанные в таблице 1.

Приведенные выше операции по определению Δ*l*, необходимо повторить для разрешения равного 38 см.

Таблица 1 – Пределы допускаемой погрешности измерения расстояния рефлектометром

| Метки | 1-2, ($l_{и12}$) | 1-3, ($l_{и13}$) | 1-4, ($l_{и14}$) |
|---|---|---|---|
| Эталонное расстояние (*lэ*), м | 48,8 | 97,7 | 146,5 |
| Предел допускаемой погрешности (Δ*l*), м | ±0,2 | ±0,2 | ±0,2 |

Результаты поверки считаются удовлетворительными, если полученные значения абсолютной погрешности Δ*l* для разрешения 38 см не превышают значений, указанных в таблице.

3. Проверка перекрываемого затухания.

Операцию поверки выполняют при включенном приложении «Рефлектометр», установив тип входа «Раздельный».

На первом этапе выход прибора соединяют с его входом. Установив диапазон в 1 км и ширину импульса 4 мкс. Подавая сигнал с выхода рефлектометра на его вход, необходимо убедиться в наличии импульса на экране прибора.

На втором этапе между входом и выходом измерителя ДЕЛЬТА-ПРО+ включают

аттенюатор API/Weinschel 115A-119A, как показано на рисунке 3. На аттенюаторе устанавливают затухание равное 90 дБ.

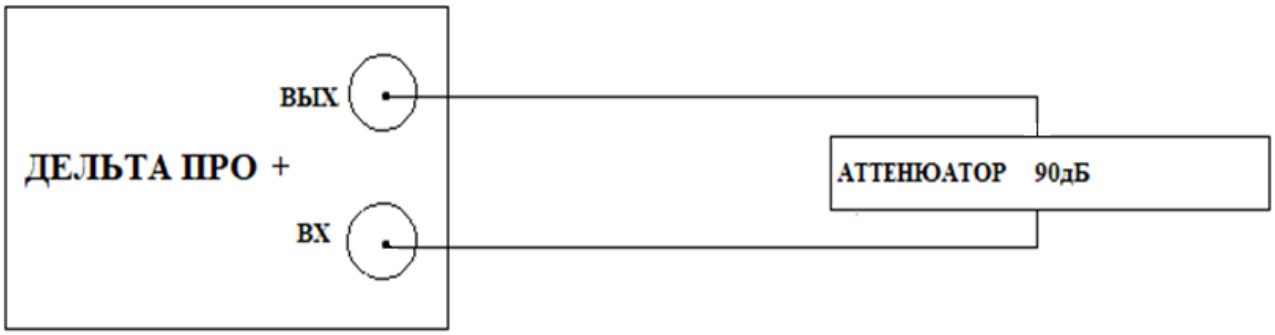



Рисунок 3 – Схема соединения приборов при проверке перекрываемого затухания

Результат поверки считается удовлетворительным, если при таком затухании на экране прибора можно наблюдать ослабленный зондирующий импульс

***Заключение.*** Разработанная методика поверки прибора ДЕЛЬТА-ПРО+ позволяет контролировать соответствие прибора заявленным метрологическим характеристикам и своевременно выявить неисправность в работе прибора.

## *Список литературы*

*4. Постановление Госстандарта №40 от 21.04.2021г. «Об осуществлении метрологической оценки в виде работ по государственной поверке средств измерений»..*

*5. Руководства по эксплуатации измерителя параметров кабельных линий ДЕЛЬТА-ПРО+.*

UDC 621.317.3

## THE METHOD OF CHECKING THE METER PARAMETERS OF CABLE LINES THE DELTA-PRO+

*Valova I.N.*

*master's student gr.267041*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Beloshitsky A.P. – Ph.D. (Tech.), Associate Professor at the department of IMS*

**Annotation**. The article discusses the method of checking the meter parameters of cable lines the DELTA-PRO+. The article presents the metrological characteristics of the device being tested and the selected reference means of verification. Verification schemes and values of verifiable points, as well as methods for estimating measurement errors.

**Keywords:** verification, methodology, measurer, cable lines

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Сборник материалов 60-ой научной конференции аспирантов, магистрантов и студентов*

Ответственный за выпуск *В.И. Брилевский*

Компьютерная верстка *Михальцова Ю.В.*

Дизайн обложки *Кайдак Д.Н.*