Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Белорусское инженерное общество

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XXII Белорусско-Российской научно-технической конференции
(Минск, 12 июня 2024 г.)

Минск БГУИР 2024

УДК 004.056.5
ББК 32.972.5
Т38

Технические средства защиты информации : тез. докл. Т38 XXII Белорусско-Российской науч.-техн. конф. (Республика Беларусь, Минск, 12 июня 2024 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2024. – 104 с.
ISBN 978-985-543-513-7

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

УДК 004.056.5
ББК 32.972.5

ISBN 978-985-543-621-9

ОГЛАВЛЕНИЕ

Assanovich B., Baniukevich E. Using wavelet scattering transform to create voiceprint of a password 7
Sudani H.H. IoT security of edge computing 8
Абросимов М.Б., Жаркова А.В., Лобов А.А., Моденова О.В., Саяпина А.А., Улитин И.В. Анализ результатов XXII международной олимпиады по криптографии SarCrypt 8
Авдеев Н.А., Гавришев А.А. Обеспечение физической безопасности избирательного участка ... 9
Авсейкова Ю.В. Организация безопасной передачи данных с использованием бессерверных технологий 10
Алефиренко В.М., Асиненко А.М. Анализ возможности применения спектрограмм для отслеживания конфиденциальности информации 11
Алефиренко В.М., Денскевич А.Д. Выбор акустических сейфов для защиты мобильных телефонов от несанкционированной активации 12
Альбино Родригес Э.Д., Гиль М.Н., Лобунов В.В. Криптографический модуль в PoS-терминалах ... 13
Артюх М.Е. Алгоритм «Априори» как способ поиска ассоциативных правил 14
Ахапкина А.М., Божко Р.А., Федоренко В.А. Концепция единого информационного пространства систем и сетей связи военного назначения 15
Баженова И.В. Анализ сложных сигналов СВЧ диапазона 16
Баженова И.В. Следящий измеритель направления 17
Батура А.А., Будник А.В. Методика оценки эффективности функционирования электронных систем безопасности 17
Бахар М.П. Технические средства и методы обеспечения информационной безопасности 18
Богачёва А.Ю., Салей И.М. Система для контроля посещаемости студентов 19
Бойправ О.В., Белоусова Е.С. Конструкции электромагнитных экранов СВЧ-диапазона на основе углеродосодержащих волокнистых материалов и связующих веществ 20
Борботько Т.В. Формирование кадрового потенциала для обеспечения кибербезопасности Республики Беларусь 21
Боровиков С.М. Модели прогнозирования класса работоспособности изделий электронной техники на основе преобразования их информативных параметров в дискретный код 22
Боровиков С.М. Прогнозирование надежности изделий электронной техники по постепенным отказам методом имитационных воздействий 23
Бураков Д.И., Лещенко Е.А. Правовые аспекты криптографической защиты информации: обзор законодательства и правовых норм 24
Воробьева А.И., Уткина Е.А. Формирование наноразмерных пленок Fe на поверхности пористого оксида алюминия для элементов электроники 25
Высоцкий Е.О., Кадан А.М. Реализация безопасного электронного голосования по протоколу двух агентств Нурми-Саломаа-Сантин 26
Гавришев А.А. Возможные угрозы безопасности передачи данных по беспроводным каналам связи, описанные в банке данных угроз безопасности информации ФСТЭК России 27
Гайкевич Е.В., Рогов М.Г. Средства антивирусной защиты 28
Галузо В.Е., Пинаев А.И., Гурский М.С. Параметры системы противодымной защиты 29
Гапоненко Н.В., Лашковская Е.И., Зайцев В.А., Насонова Н.В. Люминесцентные покрытия на стеклах и тканях для визуализации применения лазерного излучения для несанкционированного доступа к информации 30
Гурский М.С. Подходы к повышению качества подготовки специалистов технических вузов 31
Давыдов Г.В., Попов В.А., Потапович А.В. Измерение выталкивающей силы вибрационных преобразователей 32

Даревский Д.И., Буйвидович П.А., Оникийчук Н.Д. Использование технологии блокчейн для реализации безопасной электронной зачетной книжки учащихся 33
Деликатный А.М. Обучающий модуль «Исследование стойкости криптосистемы RSA»..... 34
Демидова Ю.А., Воробьев И.М. Назначение и использование механизма Cross-Origin Resource Sharing 35
Довгун В.А., Марцинкевич В.А. Нормативно-правовое регулирование процесса аттестации информационных систем на соответствие требованиям защиты информации 36
Дробот С.В., Русакович В.Н., Сацук С.М. Требования к содержанию отчета по обоснованию безопасности атомной электростанции..... 37
Зайкова С.А. Защита специальных данных пациентов в медицинском центре..... 38
Качинский М.В., Станкевич А.В., Шемаров А.И. Использование динамически изменяющихся ключей для повышения криптостойкости алгоритмов блочного шифрования..... 39
Качинский М.В., Станкевич А.В., Шемаров А.И. Конвейерная реализация хэш-функции SHA-512 на базе FPGA 40
Кваченюк Я.Д., Николайчик А.С., Рогов М.Г. Использование нейронных сетей в сфере криптографии..... 41
Киевец Н.Г. Применение теста «стопка книг» для оценки качества работы генераторов случайных чисел..... 42
Козлов В.С., Цаладонов А.Д., Биран С.А., Короткевич А.В. Модуль Юнга пленочных структур на основе анодного оксида алюминия..... 43
Колосовский Е.В., Марков А.Н. Обзор законодательства и нормативных требований в области аттестации информационных систем 43
Крамаренко А.К., Кулик А.Д. Проблемы и решения в контексте подготовки специалистов по информационной безопасности 44
Крамаренко А.К., Матиевская А.В. Новый подход к технической защите информации: использование локальных бинарных шаблонов для изображений с целью обеспечения инвариантности размеров и ориентации..... 46
Крищенович В.А. Биометрические технологии в электронных медицинских картах 47
Кушнир В.Н., Прищепа С.Л. Смягчение фононного спектра в сверхпроводящих пленках наноразмерной толщины 48
Лазарук С.К., Клюцкий А.Ю., Долбик А.В., Лешок А.А., Ковальчук Н.С., Лабунов В.А. Кремниевые лавинные светодиоды с внутренней модуляцией оптического сигнала для интегральной фотоники..... 49
Лазарук С.К., Сасинович Д.А., Долбик А.В., Дудич В.В., Томашевич Л.П., Ефименко С.А., Козлов А.А., Лабунов В.А. Защитные покрытия на основе алюминиевых сеток, встроенных в анодный оксид алюминия..... 50
Либорас В.А., Буневич М.А. Применение SDR-приемопередатчиков для оценки побочных магнитных излучений и наводок от средств вычислительной техники..... 51
Линцевич К.Д. Подготовка специалистов в области защиты информации: вызовы и перспективы..... 52
Логин В.М. Подготовка бакалавров по специальности «Информационные системы и технологии» 52
Логин В.М. Технические средства защиты телефонных линий от перехвата передаваемой по ним информации 53
Маликов В.В. Исследование незадекларированных возможностей прикладного программного обеспечения 54
Мартинкевич Д.Л., Насонова Н.В. Создание системы защиты информации коммерческого предприятия 55

Матюшенко А.К., Снигирь П.А. Обеспечение безопасности передачи данных на канальном уровне на основе оборудования Huawei 56
Метельский А.Д., Гусаков П.Б. Подготовка специалистов в области защиты информации.... 57
Митюхин А.И., Мурашкина З.Н. Защита пространственных данных полигональных объектов..... 58
Мищенко В.Н., Матусевич П.А., Митрофанов А.Д., Сурвило И.С. Исследование особенностей физического процесса переноса носителей заряда в графене, входящем в состав гетероструктурного полупроводникового прибора 58
Мищенко В.Н., Матусевич П.А., Митрофанов А.Д., Сурвило И.С. Моделирование из первых принципов транспортных свойств носителей заряда в графене, модифицированном атомами водорода 59
Мокеров В.С., Белоусова Е.С., Бойправ О.В. Двухслойные углесодержащие поглотители электромагнитного излучения на основе полиуретановой мастики и поливинилацетатной дисперсии 60
Мокеров В.С. Поглотители электромагнитного излучения на основе модифицированных углей 61
Недбайлик С.В., Гусаков П.Б. Криптографическая защита информации в приложении Telegram..... 62
Николайчук А.Н. Использование полей заголовка IP-пакета для методов сетевой стеганографии..... 63
Одинец Д.Н., Кулеш В.Л., Алуев Е.А. Концепция построения модуля защиты web-приложения на основе имитации и анализа сетевых атак..... 64
Осипов Р.Д., Герасимов А.С. Программные средства защиты информации..... 65
Песняк Н.В. Интеграция системы полиграфии в мобильные приложения iOS: технологии и безопасность 65
Петриченко И.А., Лещенко Е.А. Методы и средства криптографической защиты в распределенных информационных системах 66
Петров А.Д. Особенности политики информационной безопасности в учреждениях системы высшего образования..... 67
Петров С.Н., Булавин К.С., Ворожцов А.О. Уязвимости идентификатора RFID-меток..... 68
Петров С.Н., Смотрук Г.С. Сложности эксплуатации SIEM-систем при обработке большого объема событий безопасности 68
Поблагуев А.П., Ильющенко А.И. Google Dorking как метод анализа защищенности веб-ресурсов..... 69
Поляков К.Б., Скиба И.Г. Актуальные аспекты нормативно-правового регулирования в области защиты персональных данных..... 70
Пронин И.В., Романюк М.В. Роль многофакторной аутентификации в криптографической защите информации: технологии и реализации 71
Пулко Т.А., Лах А.А., Румас С.С. Актуальность биометрической аутентификации пользователей по поведенческим характеристикам 72
Путилин В.Н. Технические средства защиты информации ядерных электростанций 73
Пухир Г.А., Колбун В.С., Камил И.А.К. Разработка защитных конструкций для подавления утечки информации по каналам ПЭМИ..... 74
Розина В.А., Бегляк Е.В. Безопасность облачных решений: типовые подходы крупных вендеров 75
Рощупкин Н.А. Автоматизация инструмента Nmap для сканирования корпоративной сети с межсетевым экраном pfSense 76
Савельева М.Г. Математическая модель стеганографической системы для растровых документов-контейнеров 77

Савельева М.Г., Песецкий И.А., Песецкий Н.А. Устойчивость стеганографических преобразований к методам стегоанализа 78
Салей И.М., Богачёва А.Ю. Создание учебных видеоматериалов с использованием нейронных сетей 79
Сацук С.М., Дробот С.В., Русакович В.Н. Многофункциональная среда для управления информационным справочником показателей безопасной эксплуатации Белорусской АЭС 80
Серый А.И. Использование камертона оператором радиотехнической разведки 81
Серый А.И. Прямые и обратные физические эффекты в технических средствах и методах защиты информации 82
Способ С.П., Макаренко К.Е. Нормативно-правовое регулирование в сфере защиты информации 83
Тимофеев А.М., Корчинский А.А., Телипко Д.А. Аутентификация пользовательских данных и их отправителя на основе алгоритма ГОСТ 28147-89 84
Тимофеев А.М., Шишпаренок А.Н., Юруть В.Е. Исследование криптостойкости алгоритмов симметричного типа 85
Тимошенко М.В. Программное средство для реализации криптографических операций 85
Типун А.Ф., Хацкевич О.А. Использование машинного зрения для оценки 3D-позы человека 86
Титович Н.А., Мурашкина З.Н. Оценка изменения времени задержки логических элементов под действием радиопомех 87
Тучковский А.К., Врублевский И.А. Монодисперсные шаровые полимерные гранулы с проводящим слоем меди для экранирования электромагнитного излучения 88
Урбан Н.А. Программное обеспечение для реализации криптографических алгоритмов в контексте требований безопасности к средствам криптографической защиты информации 89
Утин Л.Л. Возможности киберподразделений стран НАТО по проведению специальных операций, направленных на дезорганизацию управления 90
Уткина Е.А., Воробьева А.И., Меледина М.В., Ходин А.А. Электрохимическое осаждение буферного слоя на основе оксисульфидов цинка-олова для фотоэлектрических преобразователей 91
Фильченков П.А. Критерии для выбора и разработки средств аудита безопасности информационных систем учреждений здравоохранения 92
Фильченкова Т.М. Смешанное обучение на английском языке по учебной дисциплине «Теория электрической связи» для иностранных студентов 93
Хартанович А.А. Комбинирование каскадной модели и стеганографического метода для размещения информации в файлах изображений 94
Хиль В.М., Шаронова Е.И. Нормативные аспекты защиты информации государственных и коммерческих организаций 95
Цыркунович П.И. Усовершенствованный скрытый канал ABC-Channel на основе блокчейн 96
Шитик Е.А. Атака отравления протоколов LLMNR/NBT-NS и противодействие ей 97
Шутько Н.П. Математическая модель мультиключевой системы текстовой стеганографии на основе использования цветовых координат HSL 98
Якушев А.В., Ревенько Д.В., Биран С.А., Короткевич А.В. Изолированные токопроводящие каналы на подложках из анодного оксида алюминия 99
Ярмольчик А.А., Способ С.П. Технические средства защиты информации 99
Ярмош А.Д., Тарасюк И.С. Разработка и внедрение методов контроля целостности данных в информационных системах 100
Сидоренко А.В., Высотская Е.А. Шифрование данных с использованием дискретной квантовой карты 101
Сидоренко А.В., Сергеев И.В. Шифрование изображений на основе хаотических отображений 102

USING WAVELET SCATTERING TRANSFORM TO CREATE VOICEPRINT OF A PASSWORD

B. Assanovich, E. Baniukevich

Educational Establishment "Grodno State University named after Yanka Kupala", Grodno, Belarus

Today, new biometric technologies are increasingly being used in various protocols and interfaces that implement user identification and verification. Voice identification, which implements text-dependent and text-independent speech recognition, is widely exploited in the human-machine interface. An example is the ID R&D developer [1], owned by the Mitek group of companies, which offers an AI-based speaker recognition product IDVoice that combines three-modal biometric capture with liveness detection, digital ID issuance, and mobile authentication. The developed SDK of ID R&D produces so-called a "voiceprint" that is a template analogous to someone's fingerprint and capable to perform user verification. Usually Shallow and Deep Neural Networks (DNN) are used in these technologies.

However, it is known [2] that for such tasks of user verification with voice signal, it must be digitized, and then a series of transformations should be performed to identify the main speech characteristics, which can then be applied to train neural networks. In recent years, several approaches to speech processing using Mel Frequency Cepstral Coefficients (MFCC) [3] and Gaussian Mixture Model (GMM) and Time-Delayed Neural Network (TDNN) that learn features from audio samples and converts them to fixed dimension vectors have been widely used.

Besides, applying these methods researches sometimes do not considered the properties of sound waves that have rich physical characteristics. The promising approach has been become the use of SincNet filters that are actually band pass filters which are derived from parameterized sinc functions [3]. The developed by authors model resulted in a significant improvement in EER score of 8.2 % with the use of vanilla SincNet with DNN fusion technique. However, recently the research interest turned again to a known promising technique that was proposed by Mallat [2] named as Wavelet Scattering Transform (WST). The process involves capturing multi-scale and invariant representations of the voice data, making it suitable for biometric applications like authentication. To evaluate the similarity for a user, the extracted features from WST can be compared using different similarity metrics.

In this work, we propose to use WST as a transformation that takes the main frequency properties of voice signal into its biometric characteristics and can possibly be used to convert voice data into a passphrase. This approach can provide to organize both the text-dependent and text-independent two-channel user identification using fusion techniques. We carried out a series of experiments where voice messages corresponding to spoken numbers in English from available dataset [4], were used as a passphrase. The range of correlation values between different voice samples versions of one user was 0.67–0.97. This proves the possibility of using WST to build single-factor or multi-factor biometric verification.

References

1. Internet Resource. Human Verification [Electronic resource]. – Access mode: https://www.idrnd.ai. – Date of access: 07.05.2024.

2. Joakim, A. Deep Scattering Spectrum / A. Joakim, S. Mallat// IEEE Trans. Signal Proc. – 2013. – Vol. 62. – P. 4114–4128.

3. M. Tripathi, D.Singh, S. Susan. Speaker Recognition Using SincNet and X-Vector Fusion. In Artificial Intelligence and Soft Computing. ICAISC 2020. Lecture Notes in Computer Science, vol 12415. Springer, Cham. 2020.

4. Internet Resource. Free Spoken Digit Dataset (FSDD). [Electronic resource]. – Access mode: https://https://github.com/Jakobovski/free-spoken-digit-dataset. – Date of access: 07.05.2024.

IoT SECURITY OF EDGE COMPUTING

H.H. Sudani

Iraqi Ministry of Science and Technology, Baghdad, Iraq

IoT is a mesh of physical things or objects that are connected to the Internet. These objects interconnect with external and internal environments with the help of embedded technology. Physical things analyze sense, control, and decide independently or in alliance with other things by way of two-way communication and high-speed control. This is also essential for the smart grid [1]. IoT results from current progress in embedded processing, wireless, and sensing technologies. IoT-based smart grids need six fundamental technologies, which include software-defined objects, model protocols, edge computing-based analysis, intelligent sensing, low cost, and network information security. One of the vital challenges for IoT is managing the large amount of data produced by sensors. Sending this massive amount of data directly to the cloud will create problems of latency, security, privacy, and high bandwidth utilization. On the other hand, its hasty development leads to the neglect of security threats to a large extent in edge computing platforms and their enabled applications.

Edge computing (EC) is the major technology to attain real-time demand response for IoT-based smart grids [2]. EC carries out computation at the edge of the network. It emphasizes being near the user and the data source. It is real-time, reliable, and faster.

Thus, privacy protection needs to be considered in edge computing, and effective privacy-preserving mechanisms such as local differential privacy and differential privacy with high utility [3] need to be designed to protect the privacy of users in the edge computing-based IoT environment. IoT gateways and security solutions help address the security issues of IoT edge devices. By moving security functionality to the network edge and providing security directly to IoT devices, these solutions help to identify and block potential threats there, improving the overall security posture. In order to provide reliable protection against security threats and attacks, a light-weight authentication scheme needs to be modeled where the EC servers authenticate the end devices without any time delay.

References

1. Meng, W. Smart Grid Neighborhood Area Networks: a Survey / W. Meng, R. Ma, H. H. Chen // IEEE Network. – 2014. – Vol. 28, no. 1. – P. 24–32.

2. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing / S. H. Chen [et al.] // IEEE Access. – 2019. – Vol. 7. – Article ID 74089.

3. On Binary Decomposition Based Privacy-Preserving Aggregation Schemes in Real-Time Monitoring Systems / X. Yang [et al.] // IEEE Trans. Parallel Distrib. Syst. – 2016. – Vol. 27, no. 10. – P. 2967–2983.

АНАЛИЗ РЕЗУЛЬТАТОВ XXII МЕЖДУНАРОДНОЙ ОЛИМПИАДЫ ПО КРИПТОГРАФИИ SARCRYPT

М.Б. Абросимов, А.В. Жаркова, А.А. Лобов,
О.В. Моденова, А.А. Саяпина, И.В. Улитин

ФГБОУ ВО Саратовский научный исследовательский государственный университет имени Н.Г. Чернышевского, Саратов, Россия

XXII Международная олимпиада по криптографии SarCrypt проводилась в 2023–2024 учебном году. Традиционно первый тур олимпиады проводится в первую полную неделю декабря и является отборочным. На второй тур попадают победители

первого тура, то есть участники, занявшие 1–3 место. Второй тур традиционно проводится на базе факультета компьютерных наук и информационных технологий Саратовского научного исследовательского государственного университета имени Н.Г. Чернышевского в последнее воскресенье января. Олимпиада проводится для трех категорий участников: учеников 6–8 классов, 9–11 классов и студентов. На решение задач дистанционного тура дается одна неделя, а на решение задач очного тура – 3 часа. Ученикам 6–8 классов предлагается 6 задач, ученикам 9–11 классов – 8 задач, студентам – 10 задач по криптографии, теории кодирования, комбинаторике и другим разделам математики и информатики.

В отборочном туре приняли участие 56 учеников 6-8 классов, 79 учеников 9–11 классов и 56 студентов из городов России, Республики Беларусь, Республики Молдовы и Республики Казахстан. Все участники I–II туров получили электронные дипломы, а их руководители – грамоты. Итоги обоих туров олимпиады можно посмотреть на сайте [1].

В докладе обсуждаются задачи, которые предлагались участникам, и анализируются итоги олимпиады. Сравниваются изменения в подготовке участников по сравнению с предыдущими олимпиадами SarCrypt [2].

Список литературы

1. Олимпиады по криптографии [Электронный ресурс]. – Режим доступа: https://www.sgu.ru/structure/computersciences/theorcompsafe/olimpiady-po-kriptografii. – Дата доступа: 30.04.2023.

2. XXI международная олимпиада по криптографии SarCrypt / М. Б. Абросимов [и др.] // Технические средства защиты информации : тез. докл. XXI Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 6 июня 2023 года). – Минск : БГУИР, 2023. – С. 12.

ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ИЗБИРАТЕЛЬНОГО УЧАСТКА

Н.А. Авдеев[1], А.А. Гавришев[2]

[1]Национальный исследовательский университет «МЭИ», Москва, Россия

[2]Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Известно [1], что выборы и референдум являются высшим непосредственным выражением принадлежащей гражданам власти. Однако количество увеличивающихся криминальных и иных видов угроз различным объектам, в том числе и избирательным участкам, ставит вопрос об обеспечение их безопасности, в том числе и физической.

В данном докладе, на основе проведенного анализа литературы [1–4], разработаны обобщенные рекомендации по обеспечению физической безопасности типового избирательного участка. В первую группу были включены рекомендации, включающие в себя следующие организационные меры:

1. Определение письменного списка избирателей и ответственных лиц, которые имеют право доступа в помещения, в которых расположены избирательные участки.
2. Обеспечение безопасности и охраны помещений, в которых расположена избирательная комиссия и бюллетени для голосования.
3. Обеспечение взаимодействия избирательной комиссии с МВД России и Росгвардией России для обеспечения безопасности избирательного участка.
4. Определение совместно с сотрудниками правоохранительных органов мест их дежурств и проведение периодического осмотра помещений.

5. Проведение по документам, удостоверяющим личность, идентификации посетителей и сверка их со списками избирателей.

6. Перекрытие всех помещений, которые не имеют отношения к избирательному процессу.

7. Обеспечение наличия нескольких эвакуационных выходов.

8. Запрет автомобилям на парковку вблизи здания, где расположен избирательный участок.

Во вторую группу были включены рекомендации, включающие в себя следующие инженерно-технические средства:

1. Установка средств инженерных заграждений.

2. Оборудование входа в здание стационарным металлоискателем и обеспечение сотрудников МВД России и Росгвардии России ручными металлоискателями.

3. Обеспечение непрерывной видеосъемки помещений, в которых расположен избирательный участок.

4. Обеспечение избирательных участков первичными средствами пожаротушения (огнетушителями), а также исправной телефонной связью.

Предложенные в докладе рекомендации потенциально могут способствовать повышению физической безопасности избирательных участков.

Список литературы

1. ФЗ от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».

2. Методическое пособие по взаимодействию избирательных комиссий и ОВД по обеспечению прав граждан и правопорядка на выборах и референдумах. М.: ЦИК России, 2011.

3. Обеспечение безопасности при проведении выборов – одна из главных задач [Электронный ресурс]. – Режим доступа: https://www.cikrb.ru/index.php?ELEMENT_ID=82501. – Дата доступа: 07.05.2024.

4. Торокин, А. А. Инженерно-техническая защита информации / А. А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ БЕССЕРВЕРНЫХ ТЕХНОЛОГИЙ

Ю.В. Авсейкова

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

Безопасность данных в современном цифровом мире становится ключевым аспектом, особенно при использовании бессерверных технологий для передачи информации. Расширение спектра безсерверных подходов, таких как Peer-to-Peer, локальные сети, Bluetooth и Wi-Fi Direct, открывает новые возможности для обеспечения высокого уровня конфиденциальности и защиты данных в процессе передачи. Внедрение бессерверных решений в рамках организации не только способствует улучшению безопасности передачи информации, но и минимизирует уязвимости, часто связанные с централизованными серверами, обеспечивая при этом повышенную приватность пользователей. Преимущества бессерверных методов передачи данных включают в себя высокую скорость выполнения операций, гибкость настройки сетевых взаимодействий и независимость от инфраструктуры централизованных серверов, что сказывается на повышении уровня безопасности обмена информацией. Непрерывные исследования и разработки в области безсерверных технологий являются первостепенной важностью для совершенствования

механизмов обеспечения безопасности данных и снижения рисков при передаче конфиденциальной информации. На текущий момент существует несколько инновационных технологий для организации бессерверной передачи данных: WebRTC, IPFS, Dat Protocol, Secure Scuttlebutt. WebRTC – это технология, которая позволяет устанавливать P2P соединения между браузерами для передачи данных в реальном времени. Она используется, например, для передачи файлов на платформах веб-приложений без необходимости загрузки на сервер. IPFS – это протокол передачи файлов, который создает децентрализованную сеть для обмена и хранения данных. Он позволяет передавать файлы напрямую между устройствами, минуя централизованные серверы. Dat Protocol – это пиринговый протокол для обмена версионированными данными. Он предлагает децентрализованную систему передачи файлов, которая основана на концепции распределенных хеш-таблиц. Secure Scuttlebutt – это протокол для обмена данных между доверенными пирами, работающий без постоянного соединения с Интернетом. Он может использоваться для обмена файлами и сообщениями между участниками сети. Эти технологии и протоколы представляют новаторские методы передачи файлов без использования централизованных серверов, что обеспечивает большую приватность, безопасность и эффективность в обмене информацией между устройствами.

Список литературы

1. WebRTC [Электронный ресурс]. – Режим доступа: https://webrtc.org – Дата доступа: 05.05.2024

2. An open system to manage data without a central server [Электронный ресурс]. – Режим доступа: https://ipfs.tech/ – Дата доступа: 05.05.2024

3. Dat Protocol [Электронный ресурс]. – Режим доступа: https://www.datprotocol.com/. – Дата доступа: 05.05.2024

4. Secure Scuttlebutt: A decentralised social networking platform for the privacy-conscious [Электронный ресурс]. – Режим доступа: https://medium.com/@picrong/secure-scuttlebutt-a-decentralised-social-networking-platform-for-the-privacy-conscious-64eb421de13b. – Дата доступа: 05.05.2024

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СПЕКТРОГРАММ ДЛЯ ОТСЛЕЖИВАНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

В.М. Алефиренко, А.М. Асиненко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время ощущается острая необходимость создания новых специальных программно-аппаратных технических средств и комплексов защиты речевой информации на основе стандартных вычислительных устройств, с помощью которых может быть достигнута значительная экономия временных и материальных ресурсов, затрачиваемых на разработку традиционных средств специальной техники. Кроме того, может быть увеличен срок использования такого вида новой техники за счет обновления как программных, так и аппаратных компонентов. На сегодняшний день наблюдается отставание в методах цифровой обработки аудио сигналов, применительно к решению различных задач обеспечения безопасности речевой связи [1].

В современных системах обеспечения безопасности речевой связи основными требованиями к компьютерным технологиям цифровой обработки сигналов и изображений являются быстрота и эффективность выполнения различных процедур обработки речевого сигнала. Однако такие факторы как безопасность речевых файлов и верификация речевых сообщений учитываются в меньшей степени.

Для понимания процессов аудио преобразований, посредством цифровой обработки изображений динамических спектрограмм, желательно выбрать модель аналитического представления звукового сигнала, с которой в дальнейшем будет удобно работать. Данные, необходимые для расчета параметров (амплитуд и фаз) следов фонообъектов могут содержаться в динамических спектральных развертках речевого сигнала – амплитудно-фазовых, частотно-временных описаниях мгновенных спектров речи с заданным шагом анализа по времени и по частоте и, прежде всего, в изображениях узкополосных амплитудных сонограмм. Примером такого рода технологий может служить кратковременный Фурье анализ-синтез звуковых сигналов, часто используемый в цифровых системах речепреобразования [2].

В качестве примера рассмотрим два речевых сигнала и их спектрограммы, в одном из которых содержится сигнал со скрытым сообщением. При объединении двух звуковых файлов в один получается другая спектрограмма, на которой можно наблюдать довольно большие различия, что свидетельствует о наличии скрытого сообщения. Однако, если прослушать эти файлы, то можно не заметить разницу, отображенную на спектрограммах. Поэтому только использование специальных программных средств поможет определить наличие скрытого сообщения.

Список литературы

1. Цифровая обработка изображений динамических спектрограмм аудио сигналов в задачах безопасности речевой связи [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=496&lvl=04.03. – Дата доступа: 23.03.2024.

2. Haykin, S. Adaptive Filter Theory. – 4-th edition / S. Haykin. – Prentice Hall, 2002.

ВЫБОР АКУСТИЧЕСКИХ СЕЙФОВ ДЛЯ ЗАЩИТЫ МОБИЛЬНЫХ ТЕЛЕФОНОВ ОТ НЕСАНКЦИОНИРОВАННОЙ АКТИВАЦИИ

В.М. Алефиренко, А.Д. Денскевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В контексте современного технического прогресса, где обеспечение безопасности информации становится все более проблематичной в связи с использованием высокотехнологичных методов несанкционированного съема, акцент на безопасность информации стал особенно значимым. Особое внимание уделяется акустическим сейфам – специализированным устройствам, предназначенным для защиты мобильных телефонов от несанкционированной активации при ведении конфиденциальных переговоров. В условиях сохранения конфиденциальности переговоров эти технические решения становятся ключевым элементом в сфере обеспечения безопасности информации. Таким образом, проведение анализа технических характеристик различных моделей акустических сейфов приобретает важное значение для оптимизации и повышения эффективности их использования в различных ситуациях.

На сегодняшний день на рынке представлено множество моделей акустических сейфов, предназначенных для различных устройств, включая смартфоны и кнопочные телефоны. Однако, выбор оптимальной модели становится сложной задачей, требующей анализа различных технических характеристик, которые имеют разные количественные значения. Для оптимального выбора был использован комплексный метод определения уровня качества изделий с использованием единичных показателей [1]. В качестве единичных показателей для акустических сейфов использовались такие технические характеристики как эффективный спектр шумового сигнала, время

непрерывной работы, габариты прибора, диапазон рабочих температур, вес и габаритные отсеков под защищаемое устройство. Для сравнения были выбраны следующие модели: КОКОН-DS, ЛАРЕЦ-5А, SPYCASE II, Шкатулка BW, ЛАДЬЯ-LTZ, GSM SAFE 3, ЛАГ-104, Скат-5, УЛЬТРА, АРБ-ДГ КОЛЧАН и ряд других. Всего для сравнения было выбрано 32 модели. Расчет проводился с использованием средневзвешенного геометрического показателя качества [2]. Предварительно было проведено нормирование единичных показателей и соответствующих им коэффициентов значимости. Как показали результаты расчетов, наилучшие значения показателей качества были у группы моделей SPYCASE: II, M, S (0,83; 0,82; 0,82), на четвертом месте – АРБ-ДГ КОЛЧАН (0,77) и на пятом месте – ASU-20A (0,75).

Таким образом, определение качественных характеристик акустических сейфов, выраженных относительными численными значениями, позволило провести их сравнение и определить лучшие модели по выбранным техническим характеристикам.

Список литературы

1. Алефиренко, В. М. Выбор состава технических средств для систем обеспечения безопасности / В. М. Алефиренко // Доклады БГУИР. – 2017. – № 2 (104). – С. 39–44.

2. Алефиренко, В. М. Анализ технических характеристик переносных радиоэлектронных средств подавления БПЛА с помощью комплексного геометрического показателя качества / В. М. Алефиренко, А. Д. Денскевич, А. М. Асиненко // Технические средства защиты информации: тезисы докладов XXI Белорусско-российской науч.-техн. конф., Минск, 6 июня 2023 г. / БГУИР. – Минск, 2023. – С. 14.

КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ В POS-ТЕРМИНАЛАХ

Э.Д. Альбино Родригес, М.Н. Гиль, В.В. Лобунов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В наше время, когда электронные платежи становятся все более распространенными и незаменимыми для современного бизнеса, безопасность и надежность транзакций играют ключевую роль. Криптографические модули в PoS-терминалах становятся фундаментом для обеспечения этой безопасности, обеспечивая защиту конфиденциальности данных и целостности транзакций.

Криптографический модуль представляет собой набор алгоритмов и протоколов, используемых для защиты конфиденциальных данных при передаче информации между терминалом и платежной системой. Принцип работы криптографического модуля основан на использовании сильных криптографических алгоритмов для шифрования данных, таких как алгоритмы шифрования с открытым и закрытым ключом. При совершении платежа данные, такие как номер карты, сумма транзакции и другие важные сведения, защищаются путем шифрования перед их отправкой на сервер платежной системы. После получения данных сервер дешифрует их с помощью соответствующего ключа для обработки транзакции.

Если криптографический модуль становится подвержен атакам или воздействию злоумышленников, это может иметь серьезные последствия. Нарушение безопасности модуля может привести к утечке конфиденциальной информации о платежах и карты пользователя, что в свою очередь может привести к финансовым потерям и потере доверия со стороны клиентов и партнеров компании. Кроме того, такие атаки могут нанести ущерб репутации компании и вызвать юридические последствия, вплоть до штрафов и судебных исков.

В работе рассмотрены механизмы шифрования Triple DES, AES. Также продемонстрированы их работа в реальном времени на платежном терминале PAX A930RTX, уровни защиты от физического / программного воздействия злоумышленника.

Платежные терминалы используются и будут использоваться, так как они существенно упрощают взаимодействие клиента и продавца, ускоряют бизнес-процессы. Однако их функционирование требует мониторинга, соблюдения стандартов безопасности, поиска уязвимостей и их последующего устранения.

Список литературы

1. Стандарт безопасности данных, принятый в индустрии платежных карт PCI DSS [Электронный ресурс]. – Режим доступа: https://listings.pcisecuritystandards.org/ptsdocs/4-90260%20A930RTX_Securi- ty_Policy-1706898394.63736.pdf. – Дата доступа: 07.05.2024.

2. Механизмы обеспечения безопасности платежа [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles /281438/. – Дата доступа: 07.05.2024.

АЛГОРИТМ «АПРИОРИ» КАК СПОСОБ ПОИСКА АССОЦИАТИВНЫХ ПРАВИЛ

М.Е. Артюх

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

Алгоритм «Априори» – алгоритм для поиска ассоциативных правил в базах данных. Ассоциативные правила – часть метода ассоциативного анализа данных, который используется для выявления интересных и часто встречающихся взаимосвязей между переменными в больших наборах данных. Данный метод особенно полезен в области анализа покупательского поведения, корзины товаров, медицинских диагнозов и других областях, где важны взаимосвязи между элементами.

Получаемые с помощью алгоритма «Априори» данные состоят из консеквента и антецедента. Антецедент (предпосылка) – это условие или событие, которое предшествует другому событию. В ассоциативных правилах антецедент указывает условия, которые, если выполняются, могут привести к выполнению другого условия. Консеквент (следствие) – это событие, которое следует за выполнением антецедента. В контексте ассоциативных правил, консеквент представляет собой результатом или событие, которое вероятно произойдет, если выполнены условия, заданные антецедентом (предпосылкой).

Для получения ассоциативных правил с помощью алгоритма «Априори» необходимо учитывать такие понятия как поддержка, уверенность и лифт. Поддержка – частота появления определенного подмножества в базе данных. К примеру, для набора [ноутбук, телефон] поддержка равняется 2,0%, а это означает, что два данных товара присутствуют в двух процентах всех произведенных транзакций. Уверенность – мера того, насколько часто определенное правило ассоциации верно в данных. Простыми словами, уверенность говорит о том, насколько вероятно, что если клиент выбрал один набор, то он выберет и другой. Лифт – это вероятность появления двух элементов вместе в одном наборе, при этом учитывается появление каждого элемента независимо друг от друга.

Использование алгоритма «Априори» в кибербезопасности позволяет обнаруживать интересные паттерны и зависимости между различными событиями и активностями в больших наборах данных. Этот метод анализа данных может быть широко применен для выявления скрытых угроз, выявления необычных

или аномальных действий, а также для создания моделей угроз и анализа динамики кибератак.

Преимущества использования алгоритма «Априори» в кибербезопасности включают в себя возможность выявления сложных шаблонов атак, повышение эффективности детектирования угроз за счет полученных в результате анализа паттернов, а также простоту интерпретации результатов, что облегчает принятие решений в области кибербезопасности.

КОНЦЕПЦИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СИСТЕМ И СЕТЕЙ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

А.М. Ахапкина, Р.А. Божко, В.А. Федоренко

Учреждение образование «Белорусский государственный университет информатики и радиоэдектроники», Минск, Беларусь

В настоящее время развитие инфокоммуникационной сферы критически важных информационных систем военного назначения происходит во многих направлениях, в том числе и в области совершенствования информационного пространства, объединяющего информационные ресурсы (ИР) предметной области в единое информационное пространство (ЕИП). Согласно концепции развития ЕИП создаваемое ЕИП должно выполнять следующие задачи [1]:

– предоставление пользователям своевременного и безопасного доступа к любому ИР из любой точки ЕИП с учетом разграничения прав доступа;

– обеспечение устойчивости ИР к воздействию на них всевозможных неблагоприятных факторов;

– наличие возможности у пользователей запрашивать ИР как на чтение, так и на модификацию.

Эффективное выполнение данных задач характеризует степень достижения цели создания ЕИП. В тоже время эффективность функционирования ЕИП может быть достигнута благодаря повышению показателей своевременности за счет оптимального распределения ИР по узлам.

Для возможности исследовать процесс функционирования ЕИП необходимо построить модель [2], которая в последствии позволит рассчитать необходимые для задачи исследования показатели. Предположим, что имеется инфокоммуникационная сеть (ИКС) с произвольной топологией, имеющая информационную связность «каждый с каждым» (рис. 1). Имеются узлы, объединенные в информационное пространство посредством каналов связи ИКС. Узлы можно условно разделить на два вида: активные и пассивные. Активные узлы включают в свой состав:

– пользователей, которые могут осуществлять запросы на доступ к ИР ЕИП, причем в качестве пользователей ЕИП могут рассматриваться любые гетерогенные устройства [1];

– сервер информационных ресурсов (СИР);

– сервер метаданных (СМД);

– сервер управления маршрутизацией (СУМ).

Пассивные узлы не осуществляют запросы, выступают только в роли хранилищ ИР и включают в свой состав только СУМ и СИР.

Развитие инфокоммуникационной сферы критически важных информационных систем военного назначения находится на передовой стадии, где основное внимание уделяется совершенствованию информационного пространства и его объединению в единое информационное пространство (ЕИП). Эффективное функционирование ЕИП играет ключевую роль в обеспечении своевременного и безопасного доступа

к информационным ресурсам, их устойчивости к воздействию неблагоприятных факторов, а также обеспечении возможности модификации данных. В конечном итоге, разработка и совершенствование ЕИП играет ключевую роль в обеспечении информационной безопасности и успешного выполнения военных задач.

Список литературы

1. Кингман, Дж. Пуассоновские процессы / Дж. Кингман. – М.: МЦНМО, 2017. – 136 с.
2. Черноморов, Г. А. Теория принятия решений «Системы передачи» / Г. А. Черноморов. – 2020. – 448 с.

АНАЛИЗ СЛОЖНЫХ СИГНАЛОВ СВЧ ДИАПАЗОНА

И.В. Баженова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В работе исследованы возможности управления твердотельными источниками СВЧ-энергии, показаны возможности современных технических средств формировать сложные сигналы с практически любым численным значением базы [1]. Обычно при использовании простых (импульсов) сигналов для увеличения дальности действия РЛС необходимо увеличивать энергию сигнала. При ограниченной мощности передатчика это можно сделать только за счет увеличения длительности импульса, что приводит к уменьшению точности измерения и разрешающей способности по дальности, которые определяются длительностью отклика – его основного пика. При использовании сложных сигналов эта противоречивая взаимосвязь разрешима, т. е. можно увеличивать длительность сложного сигнала, его энергию, сохраняя неизменной ширину спектра. При этом максимальная длительность сигнала будет ограничиваться допустимой мощностью передатчика. Поэтому для повышения точности измерения и разрешающей способности по дальности можно увеличивать ширину спектра. Модуль комплексной огибающей позволяет судить о точности измерения полезных параметров сигнала. С точки зрения корреляционных свойств, для простого сигнала (прямого радиоимпульса), чем больше длительность импульса, тем больше размер области сильной корреляции по оси времени, и тем меньше ее размер по оси частот, и наоборот, т. е. для простых сигналов разрешающие способности по дальности и скорости зависят друг от друга обратно пропорционально.

В рамках поставленной задачи, на основе результатов проведенных экспериментов, выполнены численные расчеты корреляционных свойств полученных сложных сигналов, которые имеют тесную взаимосвязь с двухпараметрической функцией неопределенности.

Список литературы

1. Лущицкий, В. В. Анализ работы и расчет основных характеристик генератора на диодах Ганна с варакторной перестройкой частоты / В. В. Лущицкий, В. Я. Савельев, Ф. А. Ткаченко // Радиотехника и электроника. Республиканский межведомственный сборник– 1984. – Высшая школа. – Вып. 13. – С. 69–73.

СЛЕДЯЩИЙ ИЗМЕРИТЕЛЬ НАПРАВЛЕНИЯ

И.В. Баженова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Задачей следящего измерителя направления (СИН) является непрерывное совмещение опорного направления антенны измерителя с направлением прихода волны от источника сигнала к измерителю.

В настоящее время существуют два типа следящих измерителей направления: системы с одновременным и последовательным сравнением сигналов [1]. Программа SIN моделирует следящий измеритель направления и предназначена для изучения физических принципов, лежащих в основе построения и функционирования следящих измерителей направления, также для экспериментального исследования пеленгационных характеристик.

Моделируемое устройство состоит из следующих устройств: имитатора отраженного видеосигнала сигнала; устройства выделения сигнала ошибки; устройства сопровождения цели по азимуту; устройства сопровождения цели по углу места; формирователя опорных напряжений; устройства контроля управляющих напряжений. Амплитуда и фаза сигнала определяется с помощью контрольных приборов. Для исследования влияния помех на функционирование устройства используется генератор шума. Окно программы SIN состоит из нескольких областей. Некоторые области содержат элементы управления, позволяющие выполнять те или иные действия, например, управлять глубиной модуляции и фазой имитируемого амплитудно-импульсного модулируемого сигнала. В других областях отображаются контрольные приборы и переключатели, обеспечивающие вывод осциллограмм напряжений в контрольных точках модели.

Список литературы

1. Радиотехнические системы / Под ред. Ю.М. Казаринова. – М.: Высшая школа, 1990.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ

А.А. Батура, А.В. Будник

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Предлагаемая методика оценки эффективности функционирования электронной системы безопасности (далее – ЭСБ) включает следующие основные этапы: уточнение электрической структурной схемы ЭСБ; определение условия работоспособности ЭСБ с учетом задач, решаемых системой, и указаний технической документации о том, что рассматривается в качестве нормального функционирования системы; разработка структурной схемы надежности ЭСБ с учетом условий работоспособности системы, а также указаний и рекомендаций ГОСТ [2]; определение возможных технических состояний рассматриваемой ЭСБ; получение математического выражения для определения коэффициентов эффективности возможных состояний ЭСБ; расчет эффективности функционирования рассматриваемой системы безопасности с учетом ее возможных технических состояний и коэффициентов эффективности этих состояний с точки зрения обеспечения защиты объекта [1].

Будем считать, что согласно технической документации ЭСБ сохраняет работоспособное состояние в случаях, если хотя бы один из датчиков вырабатывает сигнал об угрозе объекту, устройство МППКУ правильно обрабатывает сигнал об угрозе, а устройство ИУ правильно формирует команду для ликвидации угрозы.

Полученное в результате расчетов [3] значение показателя эффективности функционирования рассматриваемой системы безопасности составило 0,9151. Расчет вероятности работоспособного состояния ЭСБ с учетом только устойчивых отказов дает значение 0,9472. Поэтому для получения более достоверных данных о защите объекта следует учитывать влияние временных отказов на функционирование ЭСБ.

Список литературы

1. Боровиков, С. М. Теоретические основы конструирования, технологии и надежности: учеб. для студ. инжен.-техн. специальностей вузов / С. М. Боровиков. – Минск: Дизайн ПРО, 1998. – 336 с.

2. Надежность в технике. Термины и определения: ГОСТ 27.002-2015. – Введен 1.03.2017. – М.: Стандартинформ, 2016. – 24 с.

3. Теоретические основы проектирования электронных систем безопасности. Лабораторный практикум: пособие / С. М. Боровиков [и др.]; под ред. С.М. Боровикова. – Минск: БГУИР, 2014. – 70 с.

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.П. Бахар

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Техническая защита информации – это комплекс мероприятий и технологий, направленных на обеспечение конфиденциальности, целостности и доступности информации. Она играет ключевую роль в современном информационном обществе, где угрозы безопасности данных постоянно возрастают.

Одним из основных элементов технической защиты информации является шифрование данных. Этот процесс преобразует информацию в нечитаемый формат с помощью специальных алгоритмов, обеспечивая ее защиту от несанкционированного доступа. Современные методы шифрования обеспечивают высокий уровень безопасности и используются в различных сферах, включая банковское дело, здравоохранение и государственные учреждения.

Брандмауэр также является важным компонентом технической защиты информации. Это устройство, которое контролирует поток данных между компьютерными сетями, блокируя нежелательный трафик и защищая сеть от внешних атак. Брандмауэры могут быть реализованы как программное или аппаратное обеспечение и являются неотъемлемой частью современных сетевых систем.

Для обнаружения и удаления вредоносных программ используется антивирусное программное обеспечение. Оно сканирует файлы и системы на наличие вирусов, троянов и других угроз, предотвращая их нанесение ущерба информации. Регулярные обновления баз данных антивирусов обеспечивают эффективную защиту от новых видов вредоносного ПО.

Есть так же средства обнаружения вторжений (Intrusion Detection Systems, IDS) и средства предотвращения вторжений (Intrusion Prevention Systems, IPS) используются для мониторинга и обнаружения несанкционированных попыток доступа или атак на информационные системы. IDS анализируют сетевой трафик и системные журналы

на предмет подозрительной активности, такой как необычные запросы или попытки взлома, и предупреждают администраторов о потенциальных угрозах. IPS, в свою очередь, имеют возможность автоматически реагировать на обнаруженные угрозы, блокируя или изолируя подозрительные устройства или трафик, что позволяет предотвратить возможные атаки до их реализации.

Техническая защита информации требует системного подхода и постоянного обновления мер безопасности в соответствии с изменяющимися угрозами. Эффективное применение технологий шифрования, брандмауэров и антивирусных программ позволяет обеспечить надежную защиту данных и сохранить их целостность и конфиденциальность.

Список литературы

1. Объяснение защиты информации [Электронный ресурс] – Режим доступа: https://www.it-explained.com/words/information-protection-explained-explained – Дата доступа: 03.05.2024.

2. Объяснение защиты информации [Электронный ресурс] – Режим доступа: https://www.prosec-networks.com/en/blog/technischer-datenschutz – Дата доступа: 02.05.2024.

СИСТЕМА ДЛЯ КОНТРОЛЯ ПОСЕЩАЕМОСТИ СТУДЕНТОВ

А.Ю. Богачёва, И.М. Салей

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Обеспечение информационной безопасности в современном обществе является одной из наиболее актуальных задач. С этой целью в настоящее время разрабатываются разнообразные программно-аппаратные системы, направленные на обеспечение безопасности информации, субъектов и объектов информационных отношений. Одним из самых перспективных направлений в таких системах является использование биометрических данных человека [1]. Распознавание лиц имеет практическое применение и в стенах университета. Например, для упрощения организации учебного процесса, в частности, для контроля посещаемости студентами учебных занятий.

Аутентификация по геометрии лица человека является одним из основных методов биометрии, наряду с распознаванием по радужной оболочке и сканированием отпечатка пальца. Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. В нашей работе для реализации распознавания человека на основе геометрии лица были использованы нейронные сети, которые являются одним из наиболее популярных методов. Суть обучения нейронных сетей сводится к настройке весов межнейронных связей в процессе решения оптимизационной задачи методом градиентного спуска. В процессе обучения нейронной сети происходит автоматическое извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними.

В результате была разработана программа на языке Python, с использованием библиотек Face Recognition и OpenCV. Для работы с программой необходимо заранее подготовить набор данных (фотографии лиц студентов). Уже обученная нейронная сеть, создаст 128-мерный вектор для каждого лица в наборе. Далее можно переходить непосредственно к распознаванию лиц на фото или видео. Для этого нужно лишь сделать фотографию присутствующих в аудитории студентов и отправить файл на обработку. Поступившее на вход поступает изображение конвертируется в нужный формат, а найденные на нем лица преобразуются в 128-мерный вектор. Далее программа

загрузит полученные ранее кодировки известных лиц и проведет поиск совпадений найденных на фото лиц с уже известными. В итоге, программа возвращает обработанное изображение с распознанными лицами и список студентов, присутствующих в аудитории.

Таким образом, программа позволяет распознавать лица на изображениях и видео, а также формировать список студентов, присутствующих на контролируемой территории. Биометрическая аутентификация на основе геометрии лица остается актуальной и эффективной технологией, которая имеет широкий спектр применения в обеспечении безопасности и оптимизации технологических аспектов человеческой деятельности. Дальнейшие исследования в этой области могут сосредоточиться на улучшении точности распознавания и расширении функциональности системы.

Список литературы

1. Байрбекова, Г. С. Разработка и исследование биометрических методов и средств защиты информации: дис….доктора философии: 004.7.056/ Г.С. Байрбекова. – А., 2017. – 12 с.

КОНСТРУКЦИИ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ СВЧ-ДИАПАЗОНА НА ОСНОВЕ УГЛЕРОДОСОДЕРЖАЩИХ ВОЛОКНИСТЫХ МАТЕРИАЛОВ И СВЯЗУЮЩИХ ВЕЩЕСТВ

О.В. Бойправ, Е.С. Белоусова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время для изготовления конструкций электромагнитных экранов СВЧ-диапазона широко используются углеродосодержащие волокнистые материалы. Это обусловлено высокой электропроводностью и гибкостью указанных материалов. Однако конструкции электромагнитных экранов СВЧ-диапазона на основе углеродосодержащих волокнистых материалов характеризуются нестабильностью значений коэффициентов отражения, передачи и поглощения электромагнитного излучения, обусловленной тем, что углеродосодержащие волокна слабо зафиксированы в объеме таких материалов и в результате механического воздействия (изгиба, растяжения и т. п.) могут менять свое взаимное расположение. В связи с этим авторами предложена технология изготовления конструкций электромагнитных экранов СВЧ-диапазона на основе указанных материалов, для которых не характерен обозначенный недостаток. Эта технология состоит в нанесении слоем толщиной 2,0±1,0 мм связующего вещества (силиконовый герметик, акриловый герметик, полиуретановая мастика) на обе поверхности фрагментов углеродосодержащих волокнистых материалов, размеры и форма которых определяются требованиями к размерам и форме изготавливаемых конструкций электромагнитных экранов СВЧ-диапазона. Значения коэффициента передачи электромагнитного излучения в диапазоне частот 0,7–17,0 ГГц конструкций электромагнитных экранов, изготовленных в соответствии с предложенной технологией, изменяются в пределах от –20,0 до –40,0 дБ, а значения коэффициента отражения электромагнитного излучения в указанном диапазоне частот – от –0,1 до –7,0 дБ. Следует отметить, что значения коэффициента отражения электромагнитного излучения в указанном диапазоне частот у конструкций электромагнитных экранов, изготовленных в соответствии с предложенной технологией, ниже на 1,0–5,0 дБ, чем у углеродосодержащих волокнистых материалов, на основе которых они изготовлены. Обозначенные конструкции представляются перспективными для использования в целях защиты оборудования информационных систем от воздействия электромагнитных помех СВЧ-диапазона.

ФОРМИРОВАНИЕ КАДРОВОГО ПОТЕНЦИАЛА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Т.В. Борботько

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Стратегическими интересами Республики Беларусь являются устойчивое экономическое развитие и высокая конкурентоспособность экономики, что должно способствовать достижению высокого уровня и качества жизни ее граждан. Конкуренция между государствами, за рынки сбыта, и различные виды ресурсов обуславливают противостояние стран, а для занятия лидирующих позиций при таком противостоянии и их удержания, государства вынуждены объединять усилия и формировать политические, экономические и другие блоки и объединения на выгодных для них условиях, что позволяет им упрочнить свои позиции.

В Республике Беларусь активное формирование сферы кибербезопасности началось с утверждения Концепции информационной безопасности [2], а в настоящее время формируется соответствующая инфраструктура, которая необходима для оперативного обнаружения и реагирования на киберинциденты. Сегодня обеспечить устойчивое экономическое развитие и высокую конкурентоспособность экономики страны без этого невозможно.

На кафедре защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР) ведется подготовка инженеров по специальности 6-05-0611-02 «Информационная безопасность» профилизации «Защита информации в телекоммуникациях».

С учетом потребностей реального сектора экономики в содержание дисциплин специальности внесены изменения, которые учитывают современные тенденции развития направления кибербезопасности в стране. Дисциплины специальности позволяют обеспечить получение студентами знаний и получения практических навыков в части создания информационных сетей, а также настройки оборудования, применения средств защиты информации, решения задач мониторинга информационных сетей, обнаружения кибератак и реагирования на киберинциденты. Совершенствуется и материально-техническая база университета, так, например, с компанией ООО «Код безопасности» подписано соглашение о сотрудничестве осенью 2023 года, а с января 2024 года по дисциплине «Обеспечение безопасности автоматизированных и информационных систем» реализуется цикл лабораторных работ, в рамках которых студенты получают практические навыки применения и настройки многофункциональных межсетевых экранов Континент 4.

Необходимо отметить, что в виду открытости информационного пространства Республики Беларусь, население страны живет в условиях различных социотехнических воздействий, заключающихся в навязывании недостоверной информации, дискредитации руководства страны и самого государства в целом, влияние на мнение населения и его отношения к объективной действительности. На кафедре защиты информации БГУИР для студентов, обучающихся по указанной выше специальности, проводятся лекционные и практические занятия по дисциплине «Социально-психологические аспекты информационной безопасности». В дальнейшем планируется расширить спектр и содержание дисциплин касающихся этого направления.

МОДЕЛИ ПРОГНОЗИРОВАНИЯ КЛАССА РАБОТОСПОСОБНОСТИ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ИХ ИНФОРМАТИВНЫХ ПАРАМЕТРОВ В ДИСКРЕТНЫЙ КОД

С.М. Боровиков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Практический интерес для отбора изделий электронной техники (ИЭТ), отвечающих требования надежности для заданной наработки, представляет индивидуальное прогнозирование с разделением (классификацией) готовых изделий на два класса с точки зрения работоспособности:

– класс работоспособных экземпляров, которые соответствуют условию работоспособности ИЭТ данного типа для заданной наработки;

– класс потенциально ненадежных экземпляров, которые с большой степенью вероятности из-за невыявленных при их изготовлении скрытых дефектов потеряют работоспособность раньше заданной наработки электронной аппаратуры, в составе которой они будут работать.

Основу моделей прогнозирования класса работоспособности ИЭТ составляет прогнозирующая функция, вычисляемая в начальный момент времени для каждого прогнозируемого экземпляра с использованием результатов измерения у экземпляра его информативных параметров [1]. По значению прогнозирующей функции принимают решение о классе экземпляра для заданной (будущей) наработки. Модель прогнозирования и прогнозирующую функцию в ее составе получают с помощью предварительных исследований выборки ИЭТ интересующего типа с проведением ускоренных испытаний, эквивалентных по продолжительности заданной наработке ИЭТ в обычных рабочих условиях. Используя полученную модель, индивидуальное прогнозирование класса работоспособности выполняют для однотипных экземпляров, не принимавших участия в предварительных исследованиях.

Необходимость выполнения математических расчетов по определению значения прогнозирующей функции для рассматриваемого экземпляра сдерживает внедрение и широкое использование индивидуального прогнозирования.

Автором предложено выполнять преобразование (по определенным правилам) полученных при измерении значений информативных параметров в двоичные или троичные кодовые сигналы. В этих случаях модель индивидуального прогнозирования, полученная с использованием результатов предварительных исследований, в конечном итоге может быть представлена логической таблицей, показывающей, какой комбинации двоичных или троичных кодовых сигналов соответствует тот или иной класс работоспособности ИЭТ для заданной наработки. Это существенно упрощает процедуру индивидуального прогнозирования. С результатами исследования эффективности предложенных моделей прогнозирования можно ознакомиться в [2].

Список литературы

1. Боровиков, С. М. Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники / С. М. Боровиков. – М.: Новое знание, 2013. – 343 с.

2. Боровиков, С. М. Статистическое имитационное моделирование в исследовании эффективности моделей прогнозирования надежности изделий по информативным параметрам / С. М. Боровиков // BIG DATA и анализ высокого уровня: сборник научных статей X Международной научно-практической конференции, Минск, 13 марта 2024 г.: в 2 ч. Ч. 2. – Минск, 2024. – С. 122–131.

ПРОГНОЗИРОВАНИЕ НАДЕЖНОСТИ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ ПО ПОСТЕПЕННЫМ ОТКАЗАМ МЕТОДОМ ИМИТАЦИОННЫХ ВОЗДЕЙСТВИЙ

С.М. Боровиков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Метод имитационных воздействий, используемый для изделий электронной техники (ИЭТ), позволяет по реакции (реагированию) электрического параметра конкретного экземпляра на имитационное воздействие получить прогнозное значение параметра и, следовательно, принять решение о надежности этого экземпляра по постепенным отказам для заданной длительной наработки [1].

Недостатком использования температуры (как классического имитационного воздействия) является низкая оперативность получения прогноза значения электрического параметра для заданной длительной наработки из-за необходимости нагрева или охлаждения прогнозируемого экземпляра (ИЭТ). Актуальным является вопрос о выборе других, более эффективных имитационных воздействий.

Для биполярных транзисторов было предложено использовать в качестве имитационного воздействия электрические нагрузки: ток коллектора или обратное электрическое напряжение, прикладываемое к коллектору транзистора [1]. Теоретической основой возможности использования указанных нагрузок в качестве имитационных воздействий для транзисторов является наличие тесной линейной корреляции между обратимыми изменениями рассматриваемого электрического функционального параметра, обусловленными сменой значений тока коллектора или прикладываемого к коллектору напряжения, с одной стороны, и необратимыми изменениями (деградацией) электрического параметра при длительной наработке транзисторов, с другой стороны. При этом следует различать рабочий ток коллектора или рабочее напряжение на коллекторном переходе транзистора и имитационное значение тока коллектора или прикладываемого к коллектору напряжения.

В работе [2] показано, как по данным проведенного обучающего эксперимента (предварительные исследования выборки транзисторов интересующего типа) получать имитационную модель в виде функции пересчета заданной наработки на значение имитационного тока коллектора. Измерение электрического параметра при имитационном токе коллектора у конкретного экземпляра, из числа не принимавших участия в обучающем эксперименте, дает прогнозное значение электрического параметра этого экземпляра для заданной длительной наработки, что позволяет принять решение о соответствии или несоответствии прогнозируемого экземпляра требованию надежности по постепенным отказам для этой наработки. Полученные результаты позволили уточнить, а затем внедрить в практику методику индивидуального прогнозирования надежности биполярных транзисторов по постепенным отказам для интересующих длительных наработок.

Список литературы

1. Боровиков, С. М. Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники / С. М. Боровиков. – М.: Новое знание, 2013. – 343 с.

2. Калита, Е. В. Прогнозирование надежности биполярных транзисторов по постепенным отказам методом имитационного моделирования / Е. В. Калита, С. М. Боровиков, А. И. Бересневич // Интернаука: научный журнал. – 2023. – № 8(278). – Ч. 3. – С. 19–22.

ПРАВОВЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ: ОБЗОР ЗАКОНОДАТЕЛЬСТВА И ПРАВОВЫХ НОРМ

Д.И. Бураков, Е.А. Лещенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Республика Беларусь регулирует аспекты криптографической защиты информации следующими законодательными актами:

– законом Республики Беларусь от 10 ноября 2008 г. «Об информации, информатизации и защите информации»;

– законом Республики Беларусь от 28 декабря 2009 г. «Об электронном документе и электронной цифровой подписи»;

– указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», которым утверждено Положение о технической и криптографической защите информации в Республике Беларусь;

– приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

Закон Республики Беларусь «Об информации, информатизации и защите информации» не содержит прямых положений о криптографической защите информации. В разделе «Обеспечение безопасности информации» содержатся нормы, которые затрагивают вопросы криптографической защиты.

Закон Республики Беларусь от 28 декабря 2009 г. «Об электронном документе и электронной цифровой подписи». Закон устанавливает, что электронная цифровая подпись должна обеспечивать установление авторства электронного документа и целостности его содержания. Для этого используются криптографические методы, позволяющие зашифровать данные и подписать их с использованием закрытого ключа.

Указом № 196 Положение определяет правовые и организационные основы технической и криптографической защиты информации в Республике Беларусь. Оно описывает особенности технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации; контроль за технической и криптографической защитой информацией. Оно не распространяется на информационные системы, обрабатывающие государственные секреты.

Приказом № 62 утверждены специальные правила о порядке шифрования и защиты информации в государственных информационных системах, информационных системах обработки информации ограниченного распространения и (или) предоставления информации, не отнесенной к государственной тайне, и критически важных информационных объектах.

На средства защиты информации, обращающиеся на территории Республики Беларусь, распространяется действие технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность», утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375.

Согласно Положению о лицензировании отдельных видов деятельности, утвержденного Указом Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видах деятельности», отношения в области лицензирования деятельности по криптографической защите информации регулируются законодательством о лицензировании. В главе 21 Положения подробно изложены особенности лицензирования деятельности по криптографической защите информации.

Список литературы

1. Закон Республики Беларусь от 10 ноября 2008г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/laws-rb/455-z.pdf. – Дата доступа: 07.05.2024.
2. Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3961&p0=H10900113. – Дата доступа: 07.05.2024.
3. Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=P31300196. – Дата доступа: 07.05.2024.
4. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=T61302561. – Дата доступа: 07.05.2024.
5. Постановление совета министров Республики Беларусь от 15 мая 2013 г. № 375 «Информационные технологии. Средства защиты информации. Информационная безопасность» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/resolutions-sm/2013%20-%20375.pdf. – Дата доступа: 07.05.2024.
6. Указ Президента Республики Беларусь от 1 сентября 2010 года № 450 «О лицензировании отдельных видах деятельности» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3961&p0=P31000450. – Дата доступа: 07.05.2024.

ФОРМИРОВАНИЕ НАНОРАЗМЕРНЫХ ПЛЕНОК Fe НА ПОВЕРХНОСТИ ПОРИСТОГО ОКСИДА АЛЮМИНИЯ ДЛЯ ЭЛЕМЕНТОВ ЭЛЕКТРОНИКИ

А.И. Воробьева, Е.А. Уткина

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Разработан метод получения наноразмерных пленок железа на поверхности пористого анодного оксида алюминия (ПАОА) с различными топологическими параметрами. ПАОА используется в качестве основы с рельефной пористой поверхностью, на которую методом ионно-лучевого распыления осаждаются тонкие пленки железа, толщиной до 100 нм. В результате на поверхности ПАОА из атомов железа образуется сетка наноразмерной толщины с наноразмерными геометрическими параметрами (порами), соответствующими параметрам ПАОА, нанопористая магнитная пленка. Метод и режимы синтеза нанопористых пленок Fe совместимы с технологией производства кремниевых приборов микро- и наноэлектроники. Методами СЭМ и ЭДС установлено, что морфология тонких пленок Fe (до 100 нм), осажденных на ПАОА с различными топологическими параметрами и соответственно особенностями рельефа поверхности, полностью повторяет рельеф ПАОА. Несмотря на развитую морфологию поверхности ПАОА, (выступы на границах ячеек) пленки осаждаются однородно на области ячеек ПАОА вокруг пор и частично в поры, и представляют собой ячеисто-пористую гексагонально упорядоченную наноструктуру. Методом рентгеноструктурного анализа установлено, что структурно-фазовые характеристики пористых пленок Fe, несмотря на развитую морфологию поверхности,

аналогичны структуре сплошных пленок и определяются режимом осаждения, типом подложки и толщиной слоя. Установлено, что магнитные параметры полученного композитного материала, значительно выше, чем для массивного α-Fe железа (bulk Fe), и для сплошных пленок железа сопоставимой толщины. Результаты магнитных измерений показали, что нанопористые пленки железа характеризуются перпендикулярной магнитной анизотропией с увеличением коэрцитивной силы $H_C\perp$ примерно в 1,6–2 раза при измерениях в перпендикулярной геометрии, по сравнению с данными, полученными в плоскости пленки. Областью применения полученных результатов может быть фундаментальная наука (физика наноразмерных систем, физика конденсированных сред, нанофотоника, нелинейная оптика). Прикладная составляющая связана с разработкой процессов синтеза новых наноструктурированных материалов для магнитных запоминающих устройств, нового поколения магниточувствительных транзисторов, энергоаккумулирующих систем, химических и биохимических сенсоров [1–3]. Формирование магнитных пленок осаждением на пористые темплаты, позволит значительно упростить производство таких материалов, и снизить его стоимость, по сравнению с традиционными литографическими методами.

Список литературы

1. Probing the energy barriers and magnetization reversal processes of nanoperforated membrane based percolated media / V. Neu, [et al.] // Nanotechnology. – 2013. – Vol. 24. – P. 145702.

2. Magnetic characteristics of CoPd and FePd antidot arrays on nanoperforated Al_2O_3 templates / A. Maximenko [et al.] // J. Magn. Magn. Mater. – 2016. – Vol. 400. – P. 200–205.

3. Influence of lattice defects on the ferromagnetic resonance behavior of 2D magnonic crystals / A. Manzin [et al.] // Sci. Rep. – 2016. – Vol. 6. – P. 22004.

РЕАЛИЗАЦИЯ БЕЗОПАСНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ПО ПРОТОКОЛУ ДВУХ АГЕНТСТВ НУРМИ-САЛОМАА-САНТИН

Е.О. Высоцкий, А.М. Кадан

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

Тема электронного голосования (ЭГ) стала популярной по нескольким причинам. Это, в первую очередь, удобство и доступность: ЭГ предлагает удобство голосования из любого места с доступом в интернет. Это уменьшает барьеры для участия в выборах, особенно для людей с ограниченной подвижностью или теми, кто находится далеко от центра голосования.

В докладе представлена реализация подхода, предполагающего использование технологий безопасного электронного голосования при проведении различных процедур, связанных с определением предпочтений различных групп участников. В качестве таких процедур могут рассматриваться: проведение анкетирования для определения предпочтений членов группы, голосование внутри коллектива по актуальным вопросам, прочие процедуры. При проведении этих процедур важными являются такие аспекты, как секретность (обеспечение анонимности голосования каждого участника); безопасность (надежность и защищенность от любых видов вмешательства); доступность (для всех, включая лиц с ограниченными возможностями); однозначность (исключена возможность двойного голосования или голосования от имени другого человека); прозрачность (для участника – возможность проверить, что голос его был правильно учтен, а для группы в целом –

получить доступ к аудиту и проверке системы); надежность (способность выдерживать большие объемы трафика); независимый аудит (включая проверку программного обеспечения, безопасности данных и соблюдения процедур); соответствие законодательству (полностью соответствовать действующему законодательству страны, на территории которой она используется) [1].

Целью доклада является обсуждение методов безопасного электронного голосования на основе криптографических протоколов и представление реализации пилотного проекта на их основе. Для реализации протокола безопасного голосования выбран протокол двух агентств Нурми-Саломаа-Сантин [2] с возможностью биометрической идентификации участника электронного голосования. На основе данного протокола разработано приложение в архитектуре клиент-сервер.

Серверная компонента включает два сервера, обеспечивающих реализацию алгоритма ЭГ. Клиентская часть обеспечивает веб интерфейс, через который пользователь может осуществлять регистрацию, аутентификацию с возможностью биометрической идентификации, а также принимать участие в голосовании. Первое серверное приложение: отвечает за регистрацию пользователей, аутентификацию и обработку запросов на сканирование и сохранение данных лица пользователя. Реализовано с использованием Flask и SQLite. Второе серверное приложение: обрабатывает запросы на генерацию и сохранение меток для пользователей, шифрование и сохранение голосов, а также предоставляет результаты голосования. Реализовано с использованием Flask и SQLite.

Список литературы.

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С / Б. Шнайер. – Wiley, 2016. – 1024 с.

2. Salomaa, A. Verifying and recasting secret ballots in computer networks. New Results and New Trends in Computer Science / A. Salomaa. – Berlin: Springer-Verlag, 1991. – P. 283–289.

ВОЗМОЖНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ ПО БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ, ОПИСАННЫЕ В БАНКЕ ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ

А.А. Гавришев

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Известно [1, 2], что при использовании беспроводных каналов связи (БКС) для передачи данных создаются условия для получения несанкционированного доступа (НСД) к БКС из-за пределов контролируемой зоны. В связи с этим представляется целесообразным определение угроз безопасности информации (УБИ), реализация которых способна нарушить безопасность передачи (БП) данных по БКС.

В России одним из наиболее важных ресурсов, содержащих относительно полный перечень и описание УБИ, является Банк данных угроз безопасности информации ФСТЭК России (БДУ) [3], необходимость использования которого закреплена в нормативных и методических документах ФСТЭК России. Однако его использование для определения УБИ при передаче данных по БКС описано в литературе недостаточно [2]. Воспользуемся данными из БДУ для определения перечня возможных УБИ, реализация которые потенциально способна нарушить БП данных по БКС. Проведенный анализ позволил выделить следующие УБИ, описанные в существующем разделе БДУ: угроза НСД к системе по беспроводным каналам (УБИ.083); угроза деавторизации санкционированного клиента беспроводной сети

(УБИ.011); угроза перехвата данных, передаваемых по вычислительной сети (УБИ.116); угроза подключения к беспроводной сети в обход процедуры аутентификации (УБИ.125); угроза подмены беспроводного клиента или точки доступа (УБИ.126); угроза получения сведений о владельце беспроводного устройства (УБИ.133). В настоящее время, в соответствии с [4], ФСТЭК России разработан новый раздел БДУ, работающий в тестовом режиме. Проведенный анализ позволил выделить следующие УБИ, описанные в новом разделе БДУ: угрозы утечки информации, передаваемой по физическим линиям связи (ФЛС): за счет использования недостатков архитектуры (УБИ.1.12.3), за счет захвата сетевого трафика (УБИ.1.12.7), за счет атаки типа «человек посередине» (УБИ.1.12.10); угрозы НСД к ФЛС за счет: использования недостатков архитектуры (УБИ.2.12.3), захвата сетевого трафика (УБИ.2.12.7), атаки типа «человек посередине» (УБИ.2.12.10), подбора аутентификационной информации (УБИ.2.12.17); угрозы несанкционированной модификации информации, передаваемой по ФЛС за счет: использования недостатков архитектуры (УБИ.3.12.3), атаки типа «человек посередине» (УБИ.3.12.10); угрозы несанкционированной подмены информации, передаваемой по ФЛС связи за счет: использования недостатков архитектуры (УБИ.4.12.3), атаки типа «человек посередине» (УБИ.4.12.10); угрозы вызова отказа в обслуживании ФЛС за счет: захвата сетевого трафика (УБИ.6.12.7), атаки типа «отказ в обслуживании» (УБИ.6.12.14); угрозы нарушения работоспособности ФЛС за счет: захвата сетевого трафика (УБИ.8.12.7).

Представленные в докладе результаты могут быть использованы специалистами по информационной безопасности в своей практической деятельности.

Список литературы

1. Сухарев, Е. М. Общесистемные вопросы защиты информации Кн. 1 / Е. М. Сухарев. – М.: Радиотехника, 2003. – 292 с.

2. Гавришев, А. А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций / А. А. Гавришев // Вестник НГУ. Серия: ИТ. – 2017. – № 1. – С. 5–14.

3. БДУ ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru. – Дата доступа: 07.05.2024.

4. Информационное сообщение ФСТЭК России от 04.05.2022 г. N 240/22/2432.

СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

Е.В. Гайкевич, М.Г. Рогов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Современные антивирусные программы используют множество сложных технологий для обнаружения и предотвращения вирусных угроз. К основным компонентам и методам, используемым в современных антивирусах, относят сигнатурное обнаружение, поведенческий анализ и эвристику, облачные технологии, защиту в реальном времени, санбоксинг и виртуализацию [1].

Программы анализируют поведение системы и приложений, автоматически блокируют или инициируют проверки при обнаружении отклонений, указывающих на вредоносную активность [2].

Наиболее традиционным методом обнаружения вирусов является сигнатурное обнаружение. Антивирус сравнивает файлы на компьютере пользователя с базой данных вирусных сигнатур – уникальных строк кода или шаблонов, ассоциированных

с известными вирусами. Если обнаруживается совпадение, файл считается зараженным и принимаются соответствующие меры.

Современные угрозы часто используют эксплойты для эксплуатации уязвимостей, требуя непрерывного обновления антивирусов. Искусственный интеллект и машинное обучение помогают разрабатывать новые методы обнаружения вирусов, предоставляя антивирусам возможность анализировать большие и разнообразные наборы данных, учиться на примерах прошлых атак и непрерывно адаптироваться к новым угрозам [3].

Эффективность антивирусных программ улучшается благодаря интеграции ИИ и машинного обучения, что делает их неотъемлемым элементом современной информационной безопасности.

Использование нейросетей в разработке вредоносного ПО позволит создавать целенаправленные атаки, оптимизировать распространение вирусов и даже разрабатывать новые типы атак. Эти возможности делают искусственный интеллект мощным инструментом в руках злоумышленников.

Искусственный интеллект может обучаться на гораздо больших и разнообразных наборах данных, чем это возможно при традиционных подходах. Это позволяет антивирусным программам обнаруживать сложные угрозы, основываясь на поведенческих шаблонах и аномалиях, которые трудно заметить обычным сканированием.

Использование машинного обучения при разработке антивирусных программ является целесообразным не только с точки зрения улучшения работы с имеющимися проблемами, но и для предсказания новых угроз на основе анализа поведения существующих.

Список литературы

1. Вредоносные программы [Электронный ресурс]. – Режим доступа: https://www.calameo.com/read/006720537f97cf50b7288. – Дата доступа: 23.04.2024.

2. Introduction to Antivirus – Tryhackme [Электронный ресурс]. – Режим доступа: https://nehrunayak.medium.com/introduction-to-antivirus-tryhackme-3bdbdc6d8ab8. – Дата доступа: 23.04.2024.

3. How cybercriminals try to bypass antivirus protection [Электронный ресурс]. – Режим доступа:https://www.kaspersky.com/resource-center/threats/combating-antivirus. . – Дата доступа: 23.04.2024.

ПАРАМЕТРЫ СИСТЕМЫ ПРОТИВОДЫМНОЙ ЗАЩИТЫ

В.Е. Галузо, А.И. Пинаев, М.С. Гурский

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Согласно [1] в зданиях высотой более 30 м при пожаре из коридоров системами противодымной защиты (СПДЗ) следует удалять дым с весовым расходом $G_{\text{Р}}$. После монтажа по методике [2] проводят испытания (проверку) СПДЗ на соответствие проектным значениям характеристик. Однако, проектирование СПДЗ согласно [1] выполняют при температуре 300 °С, а испытания при нормальной температуре.

В [2] предлагается формула расчета приведенного значения массового расхода воздуха $G_{\text{ПР}}$ (при нормальной температуре), удаляемого из коридоров при количестве этажей N от 10 до 35: $G_{\text{ПР}} = G_{\text{Р}} \cdot (1{,}7 - 0{,}0075 \cdot N - 0{,}00025 \cdot N^2)$.

Эта формула не имеет физического смысла. Это какая-то попытка уменьшить фактическое значение весового G и объемного L расходов. Согласно [1] в жилом доме

при стандартном размере дверного проема 0,9х2,0м весовой расход $G_P \approx 7200$ кг/ч, а объемный расход $L_{ДЫМА} = G_P/\rho_{ДЫМА} = 7200/0,6 = 12000 м^3/ч$. При таком значении $L_{ДЫМА}$ перепад давления на дверях путей эвакуации превышает норму. В [2] сказано, что в случае отсутствия проектных значений «объемный расход 10000 $м^3/ч$».

При температуре 300 °С в шахте СПДЗ имеет место естественная тяга P_{EC}. Эта тяга «помогает» вентилятору СПДЗ, увеличивая его производительность ($L_{ВЕНТ}$), и тем самым увеличивает объемный расход L в клапане СПДЗ. В то же время при проведении испытаний P_{EC} можно пренебречь, а значит будет меньше L. Предлагается следующая методика определения приведенных значений расходов $G_{ПР}$ и $L_{ПР}$ при проектировании СПДЗ.

Согласно [3] объемный расход вентилятора $L_{ВЕНТ}$ не зависит от температуры и удельного веса воздуха $\gamma_{ВОЗД}$ или дыма $\gamma_{ДЫМА}$. В тоже время $L_{ВЕНТ}$ зависит от падения давления в вентиляционной сети $P_{СЕТИ}$. Из этого следует, что $P_{СЕТИ}$ не зависит от температуры и при проектировании СПДЗ рассчитывается по воздуху согласно [4], а не по дыму. При этом расход $L_{ВОЗДУХА}$ удаляемого через клапан приравнивается $L_{ДЫМА}$. При удалении дыма в шахте дымоудаления высотой $H_{ШАХТЫ}$ будет P_{EC}, которая определяется по формуле [4]: $P_{EC} = (\gamma_{ВОЗД} - \gamma_{ДЫМА}) \cdot H_{ШАХТЫ}$. Далее рассчитываются потери давления в вентиляционной системе $P_{ВЕНТ}$ с учетом P_{EC} по формуле $P_{ВЕНТ} = P_{СЕТИ} - P_{EC}$.

Далее рассчитывается суммарный подсос воздуха $L_{КЛАП}$ через клапана СПДЗ с учетом [4] и определяется $L_{ВЕНТ} = L_{ДЫМА} + L_{КЛАП}$ и по характеристике $L_{ВЕНТ}$ ($P_{ВЕНТ}$) [3] выбирается вентилятор.

Далее следует уточнение. При проведении испытаний СПДЗ тягой P_{EC} пренебргаем. Давление $P_{ВЕНТ} = P_{СЕТИ}$. По графику аэродинамической характеристики вентилятора $L_{ВЕНТ}$ ($P_{ВЕНТ}$) [3] определяется $L_{ВЕНТН}$ для нормальной температуры. Далее определяется приведенный объемный расход воздуха в клапане $L_{ПР} = L_{ВЕНТН} - L_{КЛАП}$. Соответственно весовой расход $G_{ПР} = L_{ПР} \cdot \rho_{ВОЗД}$.

Список литературы

1. СН 2.02.07-2020 Противодымная защита зданий и сооружений при пожаре.
2. НПБ 23-2010* Противодымная защита зданий и сооружений. Методы испытаний.
3. ООО «ВЕЗА». Оборудование для противодымной вентиляции.
4. ТКП 45-4.02-273-2012. Противодымная защита зданий и сооружений при пожаре.

ЛЮМИНЕСЦЕНТНЫЕ ПОКРЫТИЯ НА СТЕКЛАХ И ТКАНЯХ ДЛЯ ВИЗУАЛИЗАЦИИ ПРИМЕНЕНИЯ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ ДЛЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Н.В. Гапоненко, Е.И. Лашковская, В.А. Зайцев, Н.В. Насонова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В докладе приведены результаты ап-конверсионной фотолюминесценции на покрытиях, сформированных золь-гель методом на стеклах и тканях, которые могут быть использованы для визуализации ИК излучения на окнах зданий в целях защиты от воздействия лазерного ИК излучения при попытках получения несанкционированного доступа к информации. При попадании лазерного излучения с длиной волны 980 нм, не видимого глазом, в покрытии возбуждается ап-конверсионная фотолюминесценция трехвалентных ионов эрбия с полосами на 410, 523, 546, 658, 800 и 830 нм,

соответствующих переходам $^2H_{9/2} \rightarrow {}^4I_{15/2}$, $^2H_{11/2} \rightarrow {}^4I_{15/2}$, $^4S_{3/2} \rightarrow {}^4I_{15/2}$, $^4F_{9/2} \rightarrow {}^4I_{15/2}$ и $^4I_{9/2} \rightarrow {}^4I_{15/2}$ трехвалентных ионов эрбия. Эффективность визуализации (интенсивность ап-конверсионной ФЛ), обеспечивающая обнаружение лазерного излучения с длиной волны 980 нм, возрастает при введении в состав покрытия ионов иттербия [1, 2]. Для лазерного излучения с длиной волны 1.53 мкм солегирование иттербием не является эффективным для визуализации. В докладе приведены результаты ап-конверсионной ФЛ покрытий из суспензии с порошком титаната бария, легированном эрбием и иттербием, и сформированных на стеклах и тканях.

Список литературы

1. Optical properties and upconversion luminescence of $BaTiO_3$ xerogel structures doped with erbium and ytterbium / E. I. Lashkovskaya [et al.] // Gels. – 2022. – Vol. 8. – P. 347.

2. Upconversion luminescence from sol-gel-derived erbium- and ytterbium-doped $BaTiO_3$ film structures and the target form / N. V. Gaponenko [et al.] // Photonics. – 2023. – Vol. 10. – P. 359.

ПОДХОДЫ К ПОВЫШЕНИЮ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ ТЕХНИЧЕСКИХ ВУЗОВ

М.С. Гурский

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В нынешнем году качества в нашей республике остро встает вопрос о качестве подготовки молодых специалистов. И здесь первостепенной задачей любого ВУЗа является подготовка высококвалифицированных профессионалов, способных к инновационной деятельности, самообразованию и саморазвитию. Между тем для отечественной системы образования существует определенная проблема, которая возникает еще в период обучения в средней школе: при относительно достаточном уровне теоретических знаний школьники с трудом применяют их на практике, в жизненных ситуациях. Поэтому так важно, опираясь на опыт советской школы, дополнить образование наших будущих абитуриентов приобретением практических навыков и умений. Думается, что именно в этой связи и создаются ныне инженерные классы, активизируется работа кружков технического творчества (ТТ), организуются конкурсы среди ребят, увлекающихся техникой. Стоит подумать о создании кружков ТТ при СКБ ВУЗов технической направленности, а также промышленных предприятий нашей республики. Вот и будет профориентационная работа в действии, направленная на подготовку своих абитуриентов, действительно заинтересованных в получении образования именно в том университете, где они занимаются в кружках технического творчества соответствующего направления и умеющих не только работать практически, но и проявлять самостоятельность в решении конкретных технических задач. Особенно это важно в настоящее время при увеличении приема студентов на подготовку по целевым направлениям предприятий.

Любого рода соревнования, конкурсы (технические, научно-технические, инженерные), олимпиады способствуют осознанному стремлению молодежи к освоению технических специальностей в будущем. Получая в юном возрасте путевку в науку и техническое творчество, можно быть уверенными, что такие наши абитуриенты станут в будущем учеными, конструкторами, рационализаторами на предприятиях.

К сожалению, в средней школе обращается очень мало внимания на самостоятельную работу учащихся, и будущие студенты в своем большинстве не имеют навыков поиска, сбора информации, анализа и обобщения полезной информации. Занимаясь же в кружках подобного рода, живя в век инновационных технологий, будущий абитуриент будет сориентирован на предметную самостоятельную работу, что, в свою очередь, в дальнейшем, скажется на его учебе в ВУЗе.

Между тем проблем на пути эффективного процесса обучения в техническом ВУЗе предостаточно из-за снизившегося уровня знаний выпускников школ, а также перехода на четырехлетнее обучение в вузах. Думается, что с точки зрения потребностей инновационного развития экономики страны, именно научно-техническое творчество школьников и учащихся будет способствовать формированию востребованного кадрового резерва инженеров, способных решать задачи высокотехнологических отраслей экономики Республики Беларусь.

ИЗМЕРЕНИЕ ВЫТАЛКИВАЮЩЕЙ СИЛЫ ВИБРАЦИОННЫХ ПРЕОБРАЗОВАТЕЛЕЙ

Г.В. Давыдов, В.А. Попов, А.В. Потапович

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Вибрационные преобразователи, используемые в системах активной защиты речевой информации и устанавливаемые на ограждающих конструкциях помещения, наиболее часто, представляют собой электромагнитные преобразователи с подвижной системой в виде пластины со штоком для установки на ограждающие конструкции. Наиболее важным техническим параметром, характеризующим эффективность работы вибрационных преобразователей в системе активной защиты речевой информации, является выталкивающая сила (сила воздействия вибрационного преобразователя на ограждающие конструкции защищаемого помещения).

Для измерения выталкивающей силы вибрационных преобразователей необходимо использовать датчик силы, установленный между штоком вибрационного преобразователя и массой, моделирующей элемент ограждающей конструкции и ограничивающей амплитуду колебаний штока вибрационных преобразователей. Для измерения максимальной выталкивающей силы, амплитуда колебаний штока должна быть равной нулю, тогда выталкивающая сила будет максимальной. На практике точность измерения максимальной выталкивающей силы зависит от отношения ограничивающей массы и массы вибрационного преобразователя. При соотношении масс равном 200 ошибка в измерении максимальной выталкивающей силы из-за конечного соотношения масс будет составлять 0,5 %.

Таким образом, для измерения выталкивающей силы вибрационных преобразователей массой не более 80г, ограничивающая масса должна быть в 200 раз больше, т.е. не менее 16 кг.

Важным конструктивным требованием к ограничивающей массе является требование такой формы, чтобы отсутствовали механические резонансные колебания в заданном диапазоне частот измерения выталкивающей силы.

Так как ограничивающая масса выполнена из стали, то скорость звука в данном материале составляет ориентировочно 5100 м/с. Для максимальной частоты измерений выталкивающей силы в 5700 Гц длина ограничивающей массы для случая полуволнового вибратора должна быть не более 0,447м.

В применяемой схеме измерений ограничивающая масса составляет 16 кг и выполнена в виде цилиндра диаметром 85 мм и длиной 400 мм.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ РЕАЛИЗАЦИИ БЕЗОПАСНОЙ ЭЛЕКТРОННОЙ ЗАЧЕТНОЙ КНИЖКИ УЧАЩИХСЯ

Д.И. Даревский, П.А. Буйвидович, Н.Д. Оникийчук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Блокчейн – новая технология, которая обеспечивает надежность и безопасность при хранении и передаче данных между пользователями [1]. В ходе повсеместной оцифровки различных документов, ей подвергнутся и зачетные книжки учащихся. Использование блокчейна для создания безопасной от взлома зачетной книжки является оптимальным решением.

Чтобы использовать блокчейн для зачетной книжки учащихся необходимо:

– организовать структуру блоков и непосредственно сам блокчейн;

– разработать веб-сайт с выполнением принципов UX/UI дизайна;

– подобрать сервер с подходящими характеристиками.

Блок представляет собой файл с JSON-объектом, который содержит: ФИО студента, номер группы, факультет и все оценки за все семестры. Блоки объединяются в цепочку, причем в каждый новый блок записывается хеш предыдущего, что в совокупности с децентрализацией блокчейна дает нам безопасное хранение данных. В функции записи блока реализован следующий алгоритм: запрашивается номер файла крайнего блока, вычисляется хэш крайнего блока, формируется новый файл блока, содержащий хэш предыдущего блока, новый файл блока записывается на диск.

Для пользования веб-сайтом учащимся и преподавателям выдается мнемоническая фраза, благодаря которой доступ к профилю есть только у владельца этой фразы. Далее у преподавателя есть возможность выбрать группу и конкретного учащегося, которому нужно выставить оценку. У учащегося в это время будут лишь отображаться его данные, в том числе и оценки.

Одним из наиболее подходящих вариантов для реализации блокчейна является использование open-source блокчейн платформы Waves Enterprise [2]. При развертывании платформы Waves Enterprise в локальном режиме будет получена сеть из трех нод (узел, от англ. node), где можно будет протестировать основные функции: отправка транзакций, прием данных из блокчейна, установка и вызов смарт-контрактов, передача конфиденциальных данных между нодами, тестирование мониторинга ноды при помощи InfluxDB и Grafana. Системные требования: операционные системы CentOS 6/7 (x64), Debian 8/9/10 (x64), Red Hat Enterprise Linux 6/7 (x86), Ubuntu 18.04 (x64) (для серверов), Ubuntu 18.04+ (x64), macOS Sierra и выше (для рабочих станций); программное обеспечение для автоматизации развертывания Docker Engine и Docker Compose; технические характеристики: 2+ vCPU, 4 ГБ RAM, 50 ГБ SSD.

Таким образом, был получен пошаговый план создания основного функционала электронной зачетной книжки учащегося и проведена его реализация.

Список литературы

1. Как использовать блокчейн для хранения информации // MEREHEAD [Электронный ресурс]. – Режим доступа: https://merehead.com/ru/blog/how-to-use-blockchain-to-store-data/. – Дата доступа: 12.02.2024

2. Как развернуть свою блокчейн-платформу на базе технологий Web3 Tech // Habr [Электронный ресурс]. – Режим доступа: https://clck.ru/3AVHc9. – Дата доступа: 06.05.2024.

ОБУЧАЮЩИЙ МОДУЛЬ «ИССЛЕДОВАНИЕ СТОЙКОСТИ КРИПТОСИСТЕМЫ RSA»

А.М. Деликатный

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

В современном информационном мире обеспечение безопасности данных является одним из приоритетов. Криптосистема RSA (RSA Cryptosystem) широко используется для защиты информации, особенно в сфере финансов, коммуникаций и электронной коммерции. Однако, несмотря на свою распространенность, она подвержена различным атакам, таким как атака Винера, атака с использованием общего модуля и других [1]. Понимание этих уязвимостей крайне важно для специалистов по информационной безопасности.

В этой работе был разработан веб-сайт на фреймворке React, который может быть использован для обучения молодых специалистов атакам на криптосистему RSA. Веб-сайт предлагает доступ к лабораторным работам, состоящим как из теоретического материала, так и из практических заданий. Задания позволяют студентам углубленно изучить и применить полученные знания о криптосистеме RSA. Каждая лабораторная работа представляет собой комплексное изучение определенного аспекта криптосистемы RSA и связанных с ней уязвимостей. В теоретическом материале освещаются основы криптографии, включая принципы работы алгоритма RSA, методы шифрования и дешифрования, а также ключевые аспекты безопасности. Практические задания предлагают студентам решать реальные криптографические задачи, включая атаки на RSA, такие как атака Винера и атака с использованием общего модуля.

Веб-сайт предоставляет студентам возможность активного участия в обучении, позволяя им применять полученные теоретические знания на практике. Они могут выполнять практические задания, проверять правильность своих решений и постоянно совершенствовать свои навыки в области криптографии и кибербезопасности.

Разработка обучающего модуля по атакам на криптосистему RSA является значимым шагом в обучении специалистов по информационной безопасности. Понимание уязвимостей криптосистемы RSA и методов их защиты является ключевым элементом в обеспечении безопасности данных в современном информационном мире. Предоставление студентам возможности изучать и практиковать атаки на RSA в безопасной среде способствует их подготовке к реальным ситуациям и повышает общий уровень компетенции в области кибербезопасности.

Дальнейшее развитие обучающего модуля позволит расширить его функциональность до включения новых криптосистем и методов защиты данных. Возможность изучать не только уязвимости RSA, но и других криптографических алгоритмов позволит студентам получить более глубокие знания в области криптографии и информационной безопасности. Такой подход позволит создать полноценный ресурс для подготовки специалистов, способных эффективно защищать данные и информационные системы от различных угроз в сфере кибербезопасности.

Список литературы

1. Ян, С. Й. Криптоанализ RSA / С. Й. Ян. – Ижевск: НИЦ «Регулярная и хаотическая динамика»: Ижевский институт компьютерных исследований, 2011. – 312 с.

НАЗНАЧЕНИЕ И ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА CROSS-ORIGIN RESOURCE SHARING

Ю.А. Демидова, И.М. Воробьев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Cross-origin, или междоменные запросы (Cross-Origin Resource Sharing, CORS) – это механизм безопасности веб-браузеров, который ограничивает взаимодействие между веб-страницами, запущенными в разных источниках (доменах), протоколах или портах.

Браузеры применяют политику одного источника (Same-Origin Policy, SOP), которая предотвращает скрипты на одной странице от доступа к ресурсам на другой странице, если эти страницы не имеют одинаковый источник (домен, протокол или порт). Например, скрипт, загруженный с одного домена, обычно не может получить доступ к данным на другом домене.

С помощью CORS можно настроить сервер таким образом, чтобы он разрешал запросы с других доменов. Это позволяет веб-страницам запрашивать и получать ресурсы с других источников, если сервер явно разрешил это через заголовки CORS.

При выполнении междоменных запросов браузер добавляет дополнительные HTTP-заголовки (например, «Origin») к запросам и выполняет предварительные запросы (preflight) для проверки разрешений сервера. Если сервер отвечает соответствующими заголовками CORS, браузер разрешает доступ к ресурсам на другом источнике.

Cross-origin запросы полезны для разработки распределенных систем, когда веб-приложения должны взаимодействовать с различными серверами или API, расположенными на разных доменах.

Для реализации механизма CORS необходимо, чтобы необходимые заголовки поддерживались браузерами как отправителя, так и получателя. К таким браузерам относятся Yandex Browser, Google Chrome, Mozilla Firefox и другие распространенные в наше время клиенты.

Механизм CORS будет рассмотрен на практике на примере добавления заголовков в конфигурации веб-сервера Nginx. Простота и надежность использования данного метода разрешения междоменных запросов позволяет ему быть востребованным при решении задач, связанных с настройкой работы серверов с разными доменными именами.

Список литературы

1. Cross-Origin Resource Sharing [Электронный ресурс]. – Режим доступа: https://developer. mozilla.org/ru/docs/Web/HTTP/CORS. – Дата доступа: 05.05.2024.

2. CORS и принцип одинакового источника [Электронный ресурс]. – URL: https://yandex.cloud/ru/docs/glossary/cors#sfery-primeneniya (дата обращения: 06.05.2024).

3. Информация о CORS [Электронный ресурс]. – Режим доступа: https://aws.amazon. com/ru/what-is/cross-origin-resource-sharing/. – Дата доступа: 05.05.2024.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОЦЕССА АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Довгун, В.А. Марцинкевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аттестация системы защиты информации (далее – СЗИ) – представляет собой комплекс мер, целью которых является проверка того, что информационные активы компании соответствуют требованиям законодательства. Это включает в себя Приказ №66 Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. [1].

Согласно Закону Республики Беларусь от 10. ноября 2008 г. № 455-З «Об информации, информатизации и защиты информации» [2] все данные, которые хранятся в государственных информационных системах, должны обрабатываться с использованием сертифицированной СЗИ. Это обеспечивает защиту информации от несанкционированного доступа, изменения, уничтожения или распространения.

Для получения сертифицированной СЗИ при ее создании необходимо использовать инструменты защиты информации, которые имеют сертификат соответствия. Этот сертификат выдается в Национальной системе подтверждения соответствия Республики Беларусь. Также можно использовать инструменты защиты информации, которые получили положительное заключение после проведения государственной экспертизы.

Только организация, имеющая лицензию Оперативно-аналитического центра при Президенте Республики Беларусь, может заниматься разработкой СЗИ.

Процедура аттестации СЗИ осуществляется в соответствии с Положением о порядке проведения аттестации СЗИ, утвержденным постановлением № 675 Совета Министров Республики Беларусь от 26 мая 2009 г. [3].

Список литературы

1. Приказ оперативно-аналитического центра при президенте Республики Беларусь от 20.02.2020 г. № 66 «О мерах по реализации Указа Президента Республики» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа: 07.05.2024.

2. Закон Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защиты информации» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/laws-rb/455-z.pdf. – Дата доступа: 07.05.2024.

3. Постановление Совета Министров Республики Беларусь от 26.05.2009 г. № 675 «О некоторых вопросах защиты информации» [Электронный ресурс]. – Режим доступа: https://portal.gov.by/i/portalgovby/download/post-675.pdf. – Дата доступа: 07.05.2024.

ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ОТЧЕТА ПО ОБОСНОВАНИЮ БЕЗОПАСНОСТИ АТОМНОЙ ЭЛЕКТРОСТАНЦИИ

С.В. Дробот, В.Н. Русакович, С.М. Сацук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Публикация МАГАТЭ [1] устанавливает десять принципов, которые используются для реализации основополагающей цели безопасности – защиты людей и окружающей среды от вредного воздействия ионизирующего излучения. Один из принципов приводит к установлению требования о необходимости проведения оценки безопасности ядерных установок и деятельности в области использования атомной энергии. Ключевую роль при проведении такой оценки играет отчет по обоснованию безопасности (ООБ) атомной электростанции (АЭС), в котором эксплуатирующая организация совместно с разработчиком проекта АЭС описывает систему технических и организационных мер, обеспечивающих безопасность АЭС, а также использованные принципы проектирования систем и элементов, важных для безопасности. Полнота и качество представленных в ООБ информации и обоснований позволяют регулирующему органу убедиться в том, что предлагаемые меры обеспечат необходимый уровень безопасности, и выдать соответствующий разрешительный документ на переход к очередному этапу жизненного цикла АЭС. В соответствии с публикацией МАГАТЭ [2] регулирующий орган должен издать нормативный правовой акт, который определяет состав и содержание ООБ АЭС.

Проведен анализ зарубежного и отечественного законодательства в области использования атомной энергии, в том числе в части, касающейся определения требований к составу и содержанию ООБ АЭС. Взамен публикации 2004 года из Серии норм безопасности МАГАТЭ № GS-G-4.1 «Format and Content of the Safety Analysis Report for Nuclear Power Plants» появилось руководство по безопасности [3]. Новый документ МАГАТЭ содержит рекомендации по структуре и содержанию ООБ, учитывающие опыт аварии на АЭС «Фукусима-дайити» и проведенных после этого на АЭС стресс-тестов, а также передовой опыт государств членов МАГАТЭ в подходах к обеспечению и оценке безопасности.

Федеральные нормы и правила в области использования атомной энергии Российской Федерации НП-006-16, введенные взамен нормативного документа ПНАЭ Г-01-036-95, определяют требования к содержанию ООБ блока АЭС с реактором типа ВВЭР, которые претерпели значительные изменения в сравнении с отмененным документом. Эти изменения связаны с появлением в составе АЭС новых систем безопасности, цифровых управляющих систем, новых технических средств, в том числе для управления запроектными авариями, значительным обновлением требований к обеспечению безопасности АЭС, например, в части кибербезопасности, культуры безопасности, которые произошли за последние 25-30 лет.

Анализ законодательства Республики Беларусь в области использования атомной энергии показал, что на протяжении последних лет оно претерпело значительные изменения: принят Закон Республики Беларусь от 10 октября 2022 г. № 208-З «О регулировании безопасности при использовании атомной энергии» взамен Закона Республики Беларусь от 30 июля 2008 г. № 426-З «Об использовании атомной энергии», Постановлением Министерства по чрезвычайным ситуациям Республики Беларусь от 13 апреля 2020 г. № 15 утверждены новые нормы и правила по обеспечению ядерной и радиационной безопасности «Общие положения обеспечения безопасности атомных электростанций».

Проведенный анализ указанных выше документов может быть использован при разработке нового нормативного документа Республики Беларусь, устанавливающего требования к содержанию ООБ энергоблока АЭС, с учетом современных международных требований.

Список литературы

1. Основополагающие принципы безопасности. Нормы МАГАТЭ по безопасности. Основы безопасности. № SF-1. – Вена, МАГАТЭ, 2007. – 24 с.

2. Государственная, правовая и регулирующая основа обеспечения безопасности. Нормы безопасности МАГАТЭ. Общие требования безопасности. № GSR Part 1 (Rev.1). – Вена, МАГАТЭ, 2016. – 50 с.

3. Формат и содержание отчета по обоснованию безопасности атомных электростанций. Нормы безопасности МАГАТЭ. Руководство по безопасности. № SSG-61. – Вена, МАГАТЭ, 2024. – 236 с.

ЗАЩИТА СПЕЦИАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ В МЕДИЦИНСКОМ ЦЕНТРЕ

С.А. Зайкова

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Защита персональных данных пациентов в обязательном порядке должна учитывать специфику и чувствительность медицинских конфиденциальных данных. Система управления и эксплуатация аппаратно-программных средств с защитой данных пациентов, особенно в частных медицинских центрах, до сих пор недостаточно развита. Разработка информационно-справочных приложений, способных обеспечить защиту специальных персональных данных пациентов, является актуальной и важной задачей. Часть этих задач может быть решена на основе новых интеллектуальных технологий обработки неструктурированных данных [1]. В работе предложено новое программное средство обработки и защиты специальных данных пациентов медицинского центра в г.Гродно. Были учтены следующие важные бизнес требования к МИС: Конфиденциальность данных пациентов: приложение должно обеспечивать высокий уровень конфиденциальности для персональных данных пациентов, включая идентификационные данные, медицинскую историю, результаты лабораторных тестов и прочую чувствительную информацию. Соответствие законодательству и регуляторным требованиям: приложение должно соответствовать применимым законам и нормативным актам, таким как GDPR, HIPAA и другим регуляторным требованиям, касающимся защиты и обработки персональных данных пациентов в Республике Беларусь, включая следующие. Надежная аутентификация и авторизация пользователей. Интеграция с другими медицинскими системами и приложениями, такими как электронные медицинские записи (EMR), чтобы обеспечить централизованный доступ к информации о пациентах [2]. Резервное копирование и восстановление данных. Безопасность при передаче данных: шифрование и защищенные протоколы передачи данных между клиентом и сервером. Система уведомлений пациента о важных событиях, включая изменение статуса пациента, результаты лабораторных исследований или предстоящие встречи со специалистом медицинского центра. Разработанное для одного из медицинских центров г. Гродно приложение по результатам тестирования, готово предоставить надежное, удобное и безопасное средство для управления медицинской информацией. Решена задача обеспечения защищенного доступа к персональным медицинским данным граждан

в цифровой форме, таких как: дата приема, вакцинация, анализы, аллергические реакции, назначенные лекарства, предшествующие медицинские манипуляции и операции, результаты радиографии, специальные отметки врачей

Список литературы

1. Зайкова, С.А. Система обработки неструктурированных данных на основе интеллектуального алгоритма / С. А. Зайкова // Управление информационными ресурсами: материалы XIX Междунар. науч.-практ. конф., Минск, 22 марта 2023 г. – Минск: Академия управления при Президенте Республики Беларусь, 2023. – С. 332–333.

2. Зайкова, С.А. Система аутентификации на основе интеллектуальной модели безопасности RBA / С. А. Зайкова // Технические средства защиты информации: тезисы докладов XXI Белорусско-российской науч.-техн. конф., Минск, 6 июня 2023 г. / ред. кол.: Т. В. Борботько. – Минск: БГУИР, 2023. – С. 35–36.

ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКИ ИЗМЕНЯЮЩИХСЯ КЛЮЧЕЙ ДЛЯ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Блочные алгоритмы шифрования данных с симметричным ключом появились достаточно давно и нашли заслуженно широкое распространение при применении их в качестве базовых алгоритмов, используемых в аппаратных и программных системах шифрования [1]. Стойкость шифрования данных такими алгоритмами обеспечивается в первую очередь длиной ключа, поэтому радикальным методом увеличения криптостойкости системы шифрования является использование системы с динамически изменяющимися в процессе шифрования ключами. Предлагаемый авторами способ позволяет изменять ключ в процессе передачи данных по компьютерным сетям, обеспечивая шифрование разных блоков одного сообщения разными ключами.

Сущность способа заключается в периодической смене ключа при передаче данных по компьютерным сетям с шифрованием последующих блоков с использованием измененного ключа. Для смены ключа используется специальный некорректный («битый») пакет, нарушающий тем или иным способом целостность передаваемых по сети пакетов, состоящих из зашифрованных блоков данных, но не нарушающий целостность сетевых данных. Наличие «битого» пакета синхронизирует переход к новому ключу, заранее определенному для двух сторон. «Битый» пакет должен быть абсолютно допустимым для компьютерной сети, не требующим специальной реакции со стороны сетевого оборудования или операционной системы. Для двух сторон, участвующих в процессе передачи зашифрованных данных, создается секретная таблица ключей. Каждый ключ в таблице имеет свой идентификационный номер, определяющий местоположение ключа в таблице. Очень желательно, чтобы в таблице содержалось множество идентификационных номеров псевдонимов для каждого конкретного ключа, и множество идентификационных номеров, соответствующих «пустым ключам», которые не предполагают смену ключей при шифровании и маскируют сам факт смены ключа при криптоанализе.

Идентификационный номер нового ключа может быть передан в любом заранее определенном месте сетевого пакета, например, его очень удобно совместить с передачей контрольных данных сетевого пакета. Этот подход потребует решения

обратной задачи вычисления исходного сообщения для известного контрольного кода. В сетях стандарта Ethernet в качестве алгоритма вычисления контрольной суммы используется тридцатидвухразрядный циклический избыточный код CRC32. Этот код позволяет легко сгенерировать псевдослучайный пакет исходного сообщения исходя из требуемого значения, используемого как идентификационный номер ключа. Для наполнения генерируемого пакета можно использовать не только математические псевдослучайные генераторы, но и физические генераторы случайных последовательностей, что является существенным для повышения криптостойкости.

Предложенный способ позволяет затруднить криптоанализ зашифрованных сообщений, так как в случае его проведения потребуется поиск множества ключей на которых шифровалось передаваемое сообщение.

Список литературы

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. – 2-е изд. / Б. Шнайер. – Киев: Диалектика, 2017.

КОНВЕЙЕРНАЯ РЕАЛИЗАЦИЯ ХЭШ-ФУНКЦИИ SHA-512 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Криптографическая хэш-функция SHA-512 предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины и используется в рамках криптографических алгоритмов и протоколов в различных приложениях, связанных с защитой информации. В ряде таких приложениях для обеспечения реального времени требуется высокопроизводительная аппаратная реализация алгоритма SHA-512. В докладе рассматривается конвейерная реализация хэш-функции SHA-512 на базе FPGA, позволяющая повысить производительность.

При конвейерной реализации алгоритма SHA-512 на базе FPGA важным вопросом является выбор архитектуры, оптимизированной с точки зрения таких параметров аппаратной реализации, как пропускная способность и пропускная способность/ресурсы кристалла. На алгоритмическом уровне для реализации алгоритма SHA-512 предлагается использовать подход, рассмотренный в работе [1]. Основной целью этой работы была разработка универсального модуля мега-раунда, позволяющего строить множество альтернативных конвейерных архитектур, обеспечивающих различные реализации алгоритма SHA-512 в FPGA фирмы Xilinx с точки зрения частоты и используемых ресурсов ПЛИС. Такие архитектуры начинаются от итеративного варианта, использующего один модуль мега-раунда, циклически реализующего все итерации алгоритма SHA-512, до полностью конвейерной архитектуры с 40 модулями мега-раундов. Анализ оптимизированного варианта мега-раунда, предлагаемого в работе [1], показывает, что окончательный критический путь состоит из двух блоков сумматоров с сохранением переноса CSA и двух нелинейных функций. Проведенные исследования показали, что проект процессора, использующий полностью конвейерную реализацию алгоритма SHA-512, предлагаемую в работе [1], система проектирования Vivado, не может реализовать на тактовой частоте 250 МГц.

В докладе предлагается модифицированный вариант мега-раунда, позволяющий уменьшить критический путь до одного 3-входового сумматора и одной нелинейной функции. Простое размещение регистров на выходе мега-раунда не приводит к уменьшению критического пути. Для уменьшения критического пути до одного

3-входового сумматора и одной нелинейной функции необходимо перенести ряд сумматоров CSA вместе с соответствующими нелинейными функциями из этапа пред-вычислений в пост-вычислительный этап. Кроме того, мега-раунд для удобства реализации разбивается на два модуля соответственно для каждого из этапов. В каждом из этих модулей критический путь состоит из одного 3-входового сумматора и одной нелинейной функции. Весь конвейер реализации алгоритма SHA-512 с учетом входного буфера для вектора инициализации алгоритма формирует хэш-значение за 85 тактов.

Характеристики реализации по отчету средств синтеза пакета Vivado 2021.2 для кристалла FPGA Virtex UltraScale+ xcu250-figd2104-2L-e: 96963 триггеров секций, 82197 просмотровая таблица (LUT), тактовая частота – 250 МГц.

Список литературы

1. Athanasiou G.S., Michail H.E., Theodoridis G., Goutis C.E. Optimising the SHA-512 cryptographic hash function on FPGAs // IET Comput. Digit. Tech., 2014, Vol. 8, Iss. 2, pp. 70-82 [Электронный ресурс]. – Режим доступа: https://ietresearch. onlinelibrary.wiley.com/doi/epdf/10.1049/iet-cdt.2013.0010. – Дата доступа: 02.05.2024.

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В СФЕРЕ КРИПТОГРАФИИ

Я.Д. Кваченюк, А.С. Николайчик, М.Г. Рогов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Нейросети, как следует из названия, являются сетями нейронов, где каждый нейрон – это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше.

1. Шифрование и дешифрование с использованием нейронных сетей.

Существует три основных способа шифрования данных, использующихся в большинстве случаев: хеширование, симметричное и асимметричное шифрование.

В симметричных криптосистемах в парах взаимосвязанных криптографических преобразований применяется один и тот же ключ. Для ассиметричного шифрования используются два различных криптографических ключа, образующих так называемую ключевую пару. Алгоритмы хеширования преобразуют данные произвольного размера в массив фиксированного размера – хеш-сумму [1].

Одним из примеров алгоритмов шифрования на основе нейронных сетей является нейронная сеть Хопфилда [2].

Преимуществом алгоритмов шифрования на основе нейронных сетей является их способность создавать сложные и надежные шифры.

2. Анализ криптографических алгоритмов.

Нейронные сети могут применяться для анализа криптографических алгоритмов с целью выявления уязвимостей и разработки новых методов атаки или защиты. Это включает обучение сетей на больших объемах криптографических данных для выявления слабых мест в существующих алгоритмах.

Существует три способа взлома нейросетевого протокола обмена ключом: с помощью генетической атаки, геометрической атаки и мажоритарной атаки.

Поскольку для шифровальных систем на основе нейросетевых технологий параметром, обеспечивающим безопасность передачи информации, является синаптическая глубина L нейронных сетей, то увеличение ее значения является необходимым условием для снижения вероятности успешной атаки. Так для геометрической и мажоритарной атак увеличение значения синаптической глубины является достаточным для предотвращения атаки [3].

Использование нейросетей в криптографии представляет собой мощный инструмент для защиты данных и борьбы с киберугрозами. Комбинация нейросетей с традиционными методами криптографии может повысить эффективность защиты данных и обеспечить безопасность в цифровом мире.

Список литературы

1. Угроза появления квантового компьютера для современной криптографии и шифрования [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/788590/ – Дата доступа: 18.04.2024.

2. Нейронные сети в криптографии: новые возможности и безопасность [Электронный ресурс]. – Режим доступа: https://nauchniestati.ru/spravka/primenenie-nejronnyh-setej-v-kriptografii/?ysclid=lv3q20m7c4684799624 – Дата доступа: 18.04.2024.

3. Студенческая наука - будущее государства : материалы II международной студенческой научно-практической конференции, УО «Полесский государственный университет», г. Пинск, 25 марта 2008 г. : в 2-х ч. Ч. 2 / Национальный банк Республики Беларусь [и др.]; редкол.: К.К. Шебеко [и др.]. – Пинск: ПолесГУ, 2008. – С. 91.

ПРИМЕНЕНИЕ ТЕСТА «СТОПКА КНИГ» ДЛЯ ОЦЕНКИ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Н.Г. Киевец

Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь

В докладе рассматривается оценка качества работы генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) на основе методики двухуровневого тестирования [1].

В докладе обсуждаются результаты двухуровневого тестирования ГСЧ пяти ЭПК на базе микроконтроллера K5004 BE2 с применением теста «стопка книг» [2]. Для проведения исследования от каждой ГСЧ получено по 500 случайных последовательностей (СП) длиной 2048 бит. На первом уровне тестирования к каждой из СП применен тест «стопка книг», в котором СП разбивалась на непересекающиеся блоки длиной два бита. На втором уровне тестирования выполнена проверка равномерности распределения вероятностей превышения полученных для каждой из СП тестовых статистик.

Применение теста «стопка книг» позволило в дополнение к тестам NIST проверить соответствие вырабатываемых генераторами СП равномерно распределенным случайным последовательностям и сделать выводы о качестве работы ГСЧ ЭПК.

Список литературы

1. Киевец, Н. Г. Применение духуровневого тестирования для оценки качества работы генераторов случайных чисел / Н. Г. Киевец // Проблемы инфокоммуникаций. – 2017. – № 1 (5). – С. 19–23.

2. Рябко, Б. Я. «Стопка книг» как новый статистический тест для случайных чисел / Б. Я. Рябко, А. И. Пестунов // Проблемы передачи информации. – 2004. – Т. 40, вып. 1. – С. 73–78.

МОДУЛЬ ЮНГА ПЛЕНОЧНЫХ СТРУКТУР НА ОСНОВЕ АНОДНОГО ОКСИДА АЛЮМИНИЯ

В.С. Козлов, А.Д. Цаладонов, С.А. Биран, А.В. Короткевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Устройства на основе микроэлектромеханических систем находят широкое применение в приборах для передачи и защиты информации. Благодаря своим механическим и прочностным характеристика анодный оксид алюминия является подходящим материалом для изготовления активных и чувствительных элементов в исполнительных устройствах. Для проектирования устройств на основе анодного оксида алюминия с заданной чувствительностью необходимо заранее знать его механические свойства, в частности модуль Юнга, которые в значительной степени определяются условиями формирования оксида.

Исследование модуля Юнга проводили на пленках свободного анодного оксида алюминия длиной 50 мм и шириной 4 мм. Толщина пленок варьировалась в процессе анодирования. Для исследования было выделено 3 группы образцов: пленки, полученные на подложках из алюминия марки А0Н толщиной 0,9 мм путем одностороннего анодирования; пленки, полученные на подложках из алюминиевой фольги толщиной 90 мкм путем одностороннего анодирования; пленки, полученные на подложках из алюминиевой фольги толщиной 90 мкм путем двухстороннего анодирования. Локальное анодирование проводили на подложках размером 60×48 мм через фоторезистивную маску, после формирования которой, на поверхности оставались открыты участки для анодирования с одной стороны или двух сторон соответственно. Анодирование проводили в гальваностатическом режиме в растворе на основе щавелевой кислоты при постоянной температуре. Время анодирования варьировали для получения пленок разной толщины. После этого лишний алюминий удаляли с помощью селективного травителя.

Далее измеряли прогиб образцов при приложении к ним механической нагрузки. По полученной величине прогиба рассчитывали модуль Юнга. Среднее значение модуля Юнга для пленок алюминия, полученных односторонним анодированием на подложках из алюминия А0Н толщиной 110 мкм составило 54 ГПа; для пленок, полученных односторонним анодирование фольги толщиной 135 мкм составило 42,5 ГПа; для пленок, полученных двухсторонним анодирование фольги толщиной 135 мкм составило 51 ГПа.

ОБЗОР ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ТРЕБОВАНИЙ В ОБЛАСТИ АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.В. Колосовский, А.Н. Марков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В наше время особое значение имеет организация безопасности информационных систем, особенно в государственных системах и системах, обрабатывающих конфиденциальную информацию. Аттестация этих систем проводится Оперативно-аналитическим центром при Президенте Республики Беларусь согласно приказам [1]. В приказах регламентируется законодательные нормы и требования к безопасности систем.

Законодательные и нормативные требования в области аттестации информационных систем отличаются в зависимости от класса информационной

системы. Так информационные системы выделяют в зависимости от типа обрабатываемой информации, того, является ли система государственной, имеет ли доступ к открытым каналам данных.

Общий перечень требований включает в себя аудит безопасности, требования по обеспечению защиты данных, требования по обеспечению идентификации и аутентификации, требования по защите системы защиты информации информационной системы, обеспечение криптографической защиты информации, дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре и иные требования.

Требования отличаются в зависимости от типов систем. Так, для некоторых типов систем «обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года» входит в список обязательных требований, а для классов 4-ин, 4-спец, 4-юл, 4-дсп и 3-юл является рекомендуемой частью аудита безопасности.

В ходе аудита составляется акт, в котором каждому вопросу выставляется отметка о выполнении, номер, дата, наименование документа в котором реализованы требования. Обязательным для всех классов систем является этап с составлением требований по обеспечению защиты данных, в рамках которых проводится регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием, и обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности [2].

Список литературы

1. Приказы оперативно-аналитического центра при Президенте Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/law/orders-of-the-oac. – Дата доступа: 07.05.2024.

2. Приказы оперативно-аналитического центра при Президенте Республики Беларусь о технической и криптографической защите персональных данных [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2021-195.pdf. – Дата доступа: 07.05.2024.

ПРОБЛЕМЫ И РЕШЕНИЯ В КОНТЕКСТЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.К. Крамаренко, А.Д. Кулик

Учреждение образования «Брестский государственный технический университет», Брест, Беларусь

ИТ сектор является одним из приоритетных и активно развивающихся как в пределах республики Беларусь, так и за ее пределами. В соответствии с важностью и востребованностью данной области, ставится вопрос о необходимости тщательного подбора и подготовки специалистов в ИТ области, а также защиты информации. Рассматривая эту тему на примере инженеров по информационной безопасности, стоит отметить основные проблемы, связанные с подготовкой специалистов.

1. Недостаток квалифицированных кадров. Быстрое развитие ИТ приводит к дефициту опытных и высококвалифицированных специалистов в области информационной безопасности. Существует значительный разрыв между спросом на таких специалистов и доступностью подготовленных кадров.

2. Обновление учебных программ. Быстрый темп развития технологий требует постоянного обновления учебных программ и материалов, которые используются для подготовки специалистов. Некоторые образовательные учреждения и организации не всегда успевают соответствовать последним требованиям.

3. Необходимость практического опыта. Информационная безопасность – это область, где практический опыт играет важную роль. Однако многие программы обучения не обеспечивают достаточно практических тренировок и опыта работы с реальными системами и уязвимостями. Это может создавать проблемы при вхождении выпускников в профессиональную среду.

4. Быстрое изменение угроз и технологий. Это может привести к устареванию их компетенций и недостаточной готовности к новым угрозам [1].

В целях преодоления данных проблем необходимо соответственно активно развивать и совершенствовать образовательные программы, предоставлять студентам больше практического опыта и обеспечивать доступ к актуальным знаниям и ресурсам. Кроме того, важно содействовать сотрудничеству между образовательными учреждениями, предприятиями и профессиональными организациями для обмена опытом и создания партнерских программ. Инженер по информационной безопасности должен обладать знаниями о различных правовых нормах и регулятивных требованиях. Эти нормы предполагают следующие.

1. Законодательство о защите персональных данных. Инженер по информационной безопасности должен быть ознакомлен с законодательством, регулирующим обработку и защиту персональных данных.

2. Законодательство о кибербезопасности. Инженер по информационной безопасности должен быть знаком с законодательством, касающимся кибербезопасности и защиты информационных систем.

3. Законодательство о киберпреступлениях. Это может включать законы о компьютерных мошенничествах, хакерстве, краже личных данных и других киберпреступлениях.

4. Законодательство о защите интеллектуальной собственности. Инженер по информационной безопасности должен быть ознакомлен с законодательством о защите интеллектуальной собственности, таким как авторские права, патенты, товарные знаки и другие права интеллектуальной собственности. Беларусь участвует в двусторонних международных договорах по вопросам интеллектуальной собственности [2].

Требования к знанию правовых норм могут также различаться в зависимости от конкретной страны или региона, а потому в конкретных случаях требуют уточнения и заверения. Поэтому инженер по информационной безопасности должен следить за обновлениями и изменениями в законодательстве, связанном с информационной безопасностью в своей конкретной области работы.

Список литературы

1. Черноокий, И. В. Тенденции внедрения ИТ в образовательный процесс высшей школы в Республике Беларусь / И. В. Черноокий // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции, Могилев, 1–30 июня 2022 г.; под ред. Н. В . Маковской. – Могилев : МГУ имени А. А. Кулешова, 2022. – С. 111–114.

2. Интеллектуальная собственность [Электронный ресурс] – Режим доступа: https://president.gov.by/ru/belarus/science/intellectual-property. – Дата доступа: 06.05.2024.

НОВЫЙ ПОДХОД К ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ: ИСПОЛЬЗОВАНИЕ ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ ДЛЯ ИЗОБРАЖЕНИЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНВАРИАНТНОСТИ РАЗМЕРОВ И ОРИЕНТАЦИИ

А.К. Крамаренко, А.В. Матиевская

Учреждение образования «Брестский государственный технический университет», Брест, Беларусь

В данном докладе представлен новый подход к технической защите информации, основанный на использовании локальных бинарных шаблонов (LBP) для обработки изображений с целью обеспечения инвариантности их размеров и ориентации. Защита информации является критическим аспектом в современном цифровом мире, где конфиденциальность и целостность данных играют важную роль [1]. Одной из основных проблем в области технической защиты информации является разработка методов, способных обеспечить надежность и инвариантность в условиях изменчивости размеров и ориентации изображений. В данном исследовании мы сосредоточились на обработке изображений с использованием локальных бинарных шаблонов, которые позволяют создавать инвариантные признаки для описания изображений независимо от их размеров и ориентации. Локальные бинарные шаблоны (LBP) являются текстурными признаками, впервые предложенными в 1994 г. Они вычисляются в окрестности каждого пикселя и описывают зависимость между значениями яркости в этой окрестности [2]. В данном исследовании мы предлагаем применить вычисление LBP к пикселям бинарного представления изображений с целью создания инвариантных признаков.

Процедура обработки изображений включает последовательность преобразований, таких как бинаризация изображения, фильтрация, поворот изображения до горизонтальной ориентации, вырезание описывающего прямоугольника и масштабирование в шаблон фиксированного размера. После этого применяется вычисление локальных бинарных шаблонов к пикселям бинарного представления изображения. Полученные LBP значения строят гистограмму, которая представляет собой новый инвариантный признак нормализованного представления изображения. Эксперименты, проведенные в рамках данного исследования, показали, что вычисление корреляции Пирсона между инвариантными признаками, основанными на локальных бинарных шаблонах, позволяет различать изображения различных объектов и обеспечивает надежную защиту информации [3].

Таким образом, представленный подход к технической защите информации на основе локальных бинарных шаблонов открывает новые перспективы для создания инвариантных признаков изображений, которые могут быть использованы в различных областях, связанных с защитой информации. Это может включать обнаружение поддельных изображений, аутентификацию и идентификацию объектов на изображениях, а также защиту цифровых данных. Однако следует отметить, что данное исследование представляет только начальный этап в разработке нового подхода к технической защите информации. Дальнейшие исследования и эксперименты требуются для более полного понимания эффективности и применимости этого подхода в различных сценариях.

В заключение, использование локальных бинарных шаблонов для обработки изображений представляет собой новый и перспективный подход к технической защите информации. Этот подход может быть применим в различных областях, связанных с защитой данных, и имеет потенциал для улучшения надежности и инвариантности признаков изображений.

Список литературы

1. Черноокий, И. В. Тенденции внедрения ИТ в образовательный процесс высшей школы в Республике Беларусь / И. В. Черноокий // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции, Могилев, 1–30 июня 2022 г.; под ред. Н. В. Маковской. – Могилев: МГУ имени А. А. Кулешова, 2022. – С. 111–114.

2. Панов, И. О. Особенности применения локальных бинарных шаблонов в задачах компьютерного зрения / И. О. Панов, А. А. Калинин // Вестник Московского государственного технического университета имени Н. Э. Баумана. Серия: Приборостроение. – 2015. – № 4. – С. 92–106.

3. Шишкина, Е. Анализ и сравнительная оценка методов распознавания текстурных изображений / Е. Шишкина // Известия Самарского научного центра Российской академии наук. – 2016. – № 18(2-2). – С. 583–588.

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТАХ

В.А. Крищенович

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Стремительное развитие технологий и интенсивное использование их в сфере здравоохранения привело к цифровизации медицинских систем. Оцифрованная карта пациентов, содержащая полную историю болезни, называется электронная медицинская карта (ЭМК). ЭМК позволяет непрерывно и качественно оказывать медицинскую помощь пациентам, сокращая вероятность потери данных. В связи с тем, что ЭМК содержит большое количество персональных данных, оцифровка личных медицинских карт сопряжена с рисками для безопасности и конфиденциальности [1].

Исследование HOPAA показало, что в период с 2009 по 2022 год поступило 5 150 обращений о случаях утечки данных из медицинских учреждений. Эти утечки, включавшие более 500 файлов, привели к обнародованию 382 262 109 медицинских записей. А по данным статистики HIPAA Journal в 2023 году поступило 725 сообщений об утечке данных, и в результате этих утечек было раскрыто более 133 млн. записей [2]. Для устранения этих рисков необходима целая техническая и правовая инфраструктура. Например, комбинация национального стандарта HIPAA и международного стандарта ISO 13606-4:2019. Информация о пациентах в ЭМК должна быть защищена, чтобы она не угрожала здоровью пациента и его частной жизни [3].

Внедрение биометрических систем в ЭМК позволяет решить ряд проблем, обеспечивая механизм уникальной идентификации личности и дополнительный уровень безопасности. Распознавание лица, голоса помогает предотвратить несанкционированный доступ к медицинским данным и улучшить процесс идентификации пациентов. А внедрение биометрических технологий в управление цифровыми данными позволяет медицинским учреждениям укрепить свои протоколы безопасности и защитить данные пациентов от злоумышленников. Также упрощается контроль доступа к ЭМК и другой конфиденциальной информации, обеспечивая просмотр и изменение данных пациента только авторизованным персоналом.

Ряд преимуществ такие как: обеспечение высокого уровня безопасности, ввиду сложности подделки физиологических параметров, высокая точность и удобство использования делают биометрическую аутентификацию новым стандартом защиты конфиденциальной информации о пациентах. Согласно исследованиям Exactitude

Consultancy, мировой рынок биометрии в здравоохранении к 2029 году достигнет 10,20 млрд. долл. и на втором месте распределения данного бюджета – безопасность медицинских записей [4]. Таким образом, разработка ЭМК с внедрением биометрической аутентификации, является перспективным направлением.

Список литературы

1. Карцан, И. Н. Биометрические данные: новые возможности и риски / И. Н. Карцан // Современные инновации, системы и технологии. – 2023. – Т. 3, № 3. – С. 0201–0211.

2. The HIPAA Journal [Electronic resource]. – Access mode: https:// https://www.hipaajournal.com/healthcare-data-breach-statistics – Date of access: 02.05.2024.

3. Chen, H. Computer-Aided Secure Access and Management of Wireless Medical Devices using Internet of Things and Biometric Technology / H. Chen // Computer-Aided Design Applications. – 2024. – Vol. 21(S9). – P. 82–103.

4. Exactitude Consultancy [Electronic resource]. – Access mode: https://exactitudeconsultancy.com/report-store – Date of access: 03.05.2024.

СМЯГЧЕНИЕ ФОНОННОГО СПЕКТРА В СВЕРХПРОВОДЯЩИХ ПЛЕНКАХ НАНОРАЗМЕРНОЙ ТОЛЩИНЫ

В.Н. Кушнир, С.Л. Прищепа

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Устройства низкотемпературной сверхпроводниковой спинтроники содержат элементы с пленками сверхпроводника наноразмерных толщин. Основные проблемы их использования связаны с низкими значениями критической температуры, T_c, и с ее большими вариациями при изменении толщины сверхпроводящей пленки, d, в диапазоне малых d. Для обыкновенных сверхпроводников из одноэлементных металлов (наиболее предпочтительным является Nb) обе проблемы могут быть решены стимуляцией сверхпроводимости путем покрытия пленки графеном [1]. Суть метода состоит в изменении фононного спектра пленки сверхпроводника в силу ее взаимодействия с пленкой графена. В отличие от ранее рассмотренных методов воздействия на фононный спектр путем какой-либо модификации поверхности сверхпроводника [2], метод графенового покрытия можно отнести к регулярным, коль скоро фононный спектр покрытия может быть определен и задан. Расчет эффекта покрытия включает в общем случае вычисление вариации структурной функции Элиашберга, однако, в рассматриваемом случае он сводится к вычислению фононной спектральной плотности, поскольку частотная зависимость электрон-фононного взаимодействия является почти константой в рабочей области частот. Эффект оказывается обнаружимым и контролируемым в силу следующих факторов. Во-первых, акустическая ветвь колебаний пленки графена с поляризацией в ортогональном поверхности пленок направлении почти полностью перекрывается со спектральной характеристикой металла (Nb). Во-вторых, неупорядоченный поверхностный слой металла, насыщенный окислами, оказывается фильтром высоких частот. В-третьих, тот же слой приводит к слабой связи между графеном и пленкой. В результате оценки эффекта оказывается, что плотность числа фононных состояний увеличивается на низких частотах (увеличивается статистический вес низкочастотной области фононного спектра) – это и есть «смягчение» фононного спектра, приводящее к возрастанию критической температуры.

Список литературы

1. Superconducting critical temperature and softening of the phonon spectrum in ultrathin Nb and NbN/graphene hybrids / S. L. Prischepa [et al.] // Supercond. Sci. Technol. – 2021. – Vol. 34. – P. 115021 (15).

2. Prischepa, S. L. Phonon softening in nanostructured phonon–mediated superconductors (review) / S. L. Prischepa, V. N. Kushnir // J. Phys.: Cond. Matt. – 2023. – Vol. 35. – P. 313003 (54).

КРЕМНИЕВЫЕ ЛАВИННЫЕ СВЕТОДИОДЫ С ВНУТРЕННЕЙ МОДУЛЯЦИЕЙ ОПТИЧЕСКОГО СИГНАЛА ДЛЯ ИНТЕГРАЛЬНОЙ ФОТОНИКИ

С.К. Лазарук[1], А.Ю. Клюцкий[1], А.В. Долбик[1], А.А. Лешок[1],
Н.С. Ковальчук[2], В.А. Лабунов[1]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*
[2] *ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ», Минск, Беларусь*

Использование оптических сигналов для передачи информации имеет ряд преимуществ по сравнению с электрическими аналогами с точки зрения защиты передаваемой информации, скорости ее обработки и энергетических затрат. Источниками оптического сигнала в интегральной фотонике являются светодиоды и лазеры, большая часть которых имеют ограничение по быстродействию, не позволяющее им работать в гигагерцовом диапазоне частот без внешнего модулятора.

Кремниевые лавинные светодиоды в отличие от вышеотмеченных источников оптического сигнала являются быстродействующими устройствами, что позволяет использовать их в гигагерцовом диапазоне частот [1–3]. В этом случае работает внутренняя модуляция выходного оптического сигнала за счет управления электрическим смещением входного сигнала светодиода. В частности, измерения показали, что уменьшение барьерной емкости светодиодов до значений фемтофарадного диапазона при уменьшении рабочей площади светодиодов (единицы мкм^2) обеспечивает надежное управление выходным оптическим сигналом на частотах до 50,0 ГГц. Достигнутые значения частотных параметров не являются предельными. Расчеты показывают, что за счет дальнейшего уменьшения рабочей площади лавинных светодиодов можно достичь частот 100,0 ГГц и более. При этом важно отметить, что внутренняя модуляция выходного оптического сигнала является значимым преимуществом разработанных оптоэлектронных устройств, обеспечивающим возможность их масштабирования и объединения с логическими схемными блоками. Еще одним важным преимуществом разработанных светодиодов является их совместимость с кремниевой технологией КМПОП ИС, что позволяет создавать на их основе устройства интегральной фотоники.

Работа выполнена при финансовой поддержке БРФФИ (проект № Т23МЭ-018).

Список литературы

1. Visible electroluminescence from Al-porous silicon reverse bias diodes formed on the base of degenerate *N*-type silicon / S. Lazarouk [et al.] // MRS Online Proceedings Library. – 1994. – Vol. 358. – P. 659–664.

2. Эффективность лавинных светодиодов на основе пористого кремния / С. К. Лазарук [и др.] // Физика и техника полупроводников. – 2005. – Т. 39. С. 149–152.

3. Silicon photonic structures based on avalanche LED with interconnections through optical interposer / S. Lazarouk [et al.] // International Journal of Nanoscience. – 2019. – Vol. 18. – P. 1940091.

ЗАЩИТНЫЕ ПОКРЫТИЯ НА ОСНОВЕ АЛЮМИНИЕВЫХ СЕТОК, ВСТРОЕННЫХ В АНОДНЫЙ ОКСИД АЛЮМИНИЯ

С.К. Лазарук[1], Д.А. Сасинович[1], А.В. Долбик[1], В.В. Дудич[1], Л.П. Томашевич[1], С.А. Ефименко[2], А.А. Козлов[3], В.А. Лабунов[1],

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2] *ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ», Минск, Беларусь*

[3] *Министерство промышленности Республики Беларусь, Минск, Беларусь*

Защита от электромагнитного излучения СВЧ диапазона является актуальной задачей для обеспечения надежного функционирования ряда электронных устройств. Металлические экраны способны обеспечивать защиту от электромагнитных волн. Однако, в ряде случаев возникает необходимость экранирования волн одного диапазона, например, СВЧ и пропускания электромагнитных волн другого диапазона, например, видимого и инфракрасного. Данную задачу можно решить за счет использования металлических сеток с периодом решетки менее 1,0 мм. Металлические сетки из алюминия формировали на стеклянных подложках при помощи следующих технологических операций: напыление алюминиевых пленок толщиной 1,0–2,0 мкм, формирование маски при помощи фотолитографии, электрохимическое анодирование алюминия, незакрытого маской [1]. Сквозное прокисление алюминия обеспечивает формирование областей анодного оксида алюминия, прозрачного для видимого и инфракрасного света. При этом излучение СВЧ диапазона надежно экранируется алюминиевой сеткой. Измерения показали, что сформированные образцы пропускают 85,0–90,0 % в видимом и инфракрасном диапазонах, в то время как для излучения СВЧ-диапазона затухание сигнала составляет 20,0–40,0 дБ. Чтобы уменьшить отражение видимого и ИК света от алюминиевой поверхности использовались антиотражающие покрытия оксидов вентильных металлов, уменьшающие коэффициент зеркального отражения до 1,0–2,0 % [2]. Для уменьшения отражения СВЧ диапазона на определенной длине волны использовались сетчатые структуры с определенным периодом решетки, соответствующем необходимом резонансному поглощению. В частности, период решетки 15 см обеспечивал снижение коэффициента отражения на частоте 2,0 ГГц более чем на 50 % по сравнению со сплошными экранами. Таким образом, разработана конструкция защитных экранов на основе алюминиевых сеток, встроенных в анодный оксид алюминия. Данная разработка позволяет обеспечить защиту от электромагнитного излучения СВЧ диапазона в электронных устройствах, обрабатывающих сигналы видимого и инфракрасного диапазонов. Кроме этого, предлагаемая разработка обеспечивает эффективное уменьшение отраженных сигналов видимого и инфракрасного диапазонов, а также СВЧ диапазона определенной длины волны.

Работа выполнена при финансовой поддержке БРФФИ (проект № Т24В-009).

Список литературы

1. Lazarouk, S. K. High field porous anodization of aluminium films with a photolithographic mask / S. K. Lazarouk // Physics, Chemistry and Application of Nanostructures. World Scientific Press. Singapore. – 2013. – P. 355–358.

2. Anodic nanoporous titania for electro-optical devices / S. Lazarouk [et al.] // Japanese Journal of Applied Physics. – 2007. – Vol. 46. – P. 4390–4394.

ПРИМЕНЕНИЕ SDR-ПРИЕМОПЕРЕДАТЧИКОВ ДЛЯ ОЦЕНКИ ПОБОЧНЫХ МАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК ОТ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В.А. Либорас, М.А. Буневич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время для обработки конфиденциальной коммерческой информации используются средства электронной вычислительной техники (ЭВМ). Эти устройства генерируют побочные электромагнитные излучения и наводки (ПЭМИН), которые могут быть зарегистрированы и измерены с помощью приемников с программно-определяемой архитектурой (SDR-приемников). Таким образом, проведение анализа подходящих SDR-приемников для регистрации ПЭМИ средств ЭВМ является актуальной задачей в области радиочастотной безопасности.

Технология SDR (Software Defined Radio) представляет собой инструмент для управления радиочастотными параметрами оборудования, такими как диапазон частот и тип модуляции. SDR обладает рядом ключевых особенностей, включая визуализацию спектра принимаемого сигнала в реальном времени, использование разнообразных программно-настраиваемых фильтров, а также возможность измерения уровня сигнала. Однако, главное преимущество SDR заключается в его универсальности.

Существуют три основных типа SDR-приемопередатчиков [1].

1. Устройства, где цифровая обработка сигнала происходит на внешнем вычислительном устройстве, таком как ПК или микроконтроллер. Эти устройства преобразуют входной сигнал и передают его на вычислительное устройство. Приемники данного типа предпочтительны, если важна гибкость и возможность использовать мощные вычислительные ресурсы для обработки данных, что полезно для сложных задач анализа ПЭМИН.

2. SDR-приемопередатчики с интегрированным АЦП. Они передают сигнал на вычислительное устройство в цифровом формате и имеют архитектуру супергетеродинного приема с полосой пропускания до 20 МГц. Такие приемники полезны, если необходима высокая скорость обработки и передачи данных. Передача сигнала в цифровом виде может упростить анализ ПЭМИН.

3. DDC (direct down conversion) SDR-приемопередатчики. Они отличаются от других SDR-приемопередатчиков отсутствием аналогового генератора для подстройки на частоту приема. Оцифровка сигнала с антенны выполняется АЦП с высокой частотой дискретизации. Данные устройства наиболее подходят для анализа ПЭМИН, требующих высокой точности и широкого диапазона частот.

В современном мире, где коммерческая информация становится все более ценной, обеспечение радиочастотной безопасности приобретает особую важность. Одним из перспективных направлений в этой области является использование SDR-приемников для обнаружения и анализа побочного электромагнитного излучения от средств ЭВМ. Выбор конкретного типа SDR-приемника зависит от специфических требований задачи.

Список литературы

1. Буневич, М. А. Применение SDR-приемопередатчиков в системах для поиска закладных радиоустройств / М. А. Буневич, А. И. Майоров, И. А. Врублевский // Цифровая трансформация. – 2022. – Т. 28, № 4. – С. 62–71.

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

К.Д. Линцевич

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

С увеличением объема цифровых данных и повышением уровня угроз безопасности информации возрастает необходимость в специалистах, обладающих глубокими знаниями и навыками в области защиты информации. Однако подготовка таких специалистов сталкивается с рядом вызовов, которые требуют внимания и разработки эффективных стратегий.

Один из основных вызовов в подготовке специалистов в области защиты информации состоит в быстром развитии технологий и появлении новых видов угроз. Это требует постоянного обновления учебных программ и внедрения современных методов обучения, что иногда затрудняется ограниченными ресурсами и консервативностью академических институтов.

Другим вызовом является нехватка опыта у преподавателей, особенно в сфере новейших технологий и методов защиты информации. Это приводит к необходимости привлечения курсов квалифицированных практикующих специалистов из индустрии для обучения студентов.

Для решения этих вызовов необходимо активное сотрудничество между учебными заведениями, индустрией и правительством. Создание партнерских отношений между университетами и компаниями поможет обеспечить актуальность учебных программ и подготовить студентов к реальным вызовам в области защиты информации.

Важно также сосредоточить внимание на развитии практических навыков студентов. Проведение практик и стажировок в компаниях по защите информации поможет студентам применить свои знания на практике и подготовить их к успешной карьере в этой области.

Использование инновационных методов обучения, таких как онлайн-курсы и виртуальные лаборатории, может значительно расширить доступ к образованию в области защиты информации и обеспечить более гибкий график обучения для студентов.

ПОДГОТОВКА БАКАЛАВРОВ ПО СПЕЦИАЛЬНОСТИ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

В.М. Логин

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

Образовательным стандартом высшего образования бакалавриата по специальности 6-05-0611-01 «Информационные системы и технологии» предусмотрена подготовка по квалификации инженер-программист, обладающего практическими навыками в области информационной безопасности [1]. Будущим специалистам в данной области предлагается в ходе учебного процесса и курса специальных дисциплин освоить методику анализа и разработки информационных систем, а также программирование сетевых приложений, обеспечивающих комплексную защиту как отдельных устройств и компонентов, так и локальной компьютерной сети (далее – КС) предприятия в целом.

Выпускник бакалавриата будет обладать следующими базовыми профессиональными компетенциями:

– разрабатывать модели КС, программы сетевого взаимодействия, использовать аппаратные и программные компоненты КС при решении задач по обеспечению защиты информации технические средств, входящих в состав локальной КС, а также уметь работать с сетевыми протоколами разных уровней;

– разрабатывать программные комплексы и системы для решения профессиональных задач на основе базовых технологий сетевого программирования, типовых решений, инструментальных и языковых средств создания приложений клиент-серверной архитектуры с поддержкой многоступенчатой системы защиты информационных ресурсов и данных.

Учебным планом по специальности предусматривается изучение дисциплины «Основы информационной безопасности» [2], в которой наибольшее внимание уделяется рассмотрению следующих тенденций в области защиты информации:

– защита от несанкционированного доступа информационных ресурсов компьютеров, работающих как автономно, так и в составе КС. В первую очередь эта проблема определяется для серверов и пользователей сети Интернет. Эта функция может быть реализована многочисленными программными, программно-аппаратными и аппаратными средствами;

– защита различных информационных систем от компьютерных вирусов, имеющих возможность не только разрушить необходимую информацию, но даже повредить технические компоненты системы;

– защита секретной, конфиденциальной и личной информации от чтения посторонними лицами и целенаправленного ее искажения. Эта функция может обеспечиваться как средствами защиты от несанкционированного доступа, так и с помощью криптографических средств защиты информации.

Выпускники специальности могут работать на предприятиях и в организациях, производящих программное обеспечение, занимающихся деятельностью в области информационной безопасности, осуществляющих инженерно-программное проектирование, консультационные и другие сопутствующие услуги.

Список литературы

1. ОСВО 6-05-0611-01-2023. Информационные системы и технологии. – Минск: Министерство образования Респ. Беларусь.

2. Информационные системы и технологии [Электронный ресурс]. – Режим доступа : https://abitur.bsuir.by/m/12_113227_1_55178.pdf. – Дата доступа: 07.05.2024.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ТЕЛЕФОННЫХ ЛИНИЙ ОТ ПЕРЕХВАТА ПЕРЕДАВАЕМОЙ ПО НИМ ИНФОРМАЦИИ

В.М. Логин

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

В современных условиях многофункциональные интеллектуальные системы безопасности и технические средства защиты информации, построенные на IP- и IT-технологиях, становятся наиболее востребованными, вытесняя традиционные системы. Такие высокотехнологичные решения, как «Умный дом», «Безопасный город», «Безопасный транспорт», принцип «все в одном», предназначены для самых взыскательных заказчиков и объектов жизненно важной инфраструктуры. Подобные инновационные системы используют уникальные технологии видеоаналитики, включая захват и распознавание лиц и номерных знаков автомобильных средств, мониторинг транспортных потоков, специализированные

решения для контроля за кассовыми терминалами и банкоматами. Значительная их часть использует беспроводные каналы связи, в том числе спутниковые и каналы мобильной связи.

В качестве технических средств защиты информации в настоящее время широко применяются маскираторы телефонных переговоров [1], предназначенные для защиты телефонных линий от перехвата идущей по ним информации. Маскиратор телефонной линии подает в линию мощный шумовой сигнал, который делает неэффективным подключение к линии средства съема информации на всем ее протяжении. Маскираторы, имеющиеся в настоящее время на рынке технических средств безопасности информации, обладают высокой эффективностью, но имеют недостаток – высокую стоимость.

Технические решения компании Motorola, такие как телефоны серий Iridium и Satellite, которые могут служить как спутниковым, так и мобильным сотовым телефоном со встроенным маскиратором, позволяют решать широкий спектр подобных задач. В крупном городе за счет использования сменных картриджей, разработанных для основных стандартов сотовой связи, телефонный аппарат Motorola можно использовать как сотовый. За пределами сотового покрытия антенна телефона соединяется со спутниковой группировкой, гарантируя глобальное покрытие и устойчивый сигнал. Основой таких многофункциональных телефонов является микроконтроллер.

Для получения начальных практических навыков работы с микроконтроллерами семейства MC68HC11 фирмы Motorola в учебных целях можно использовать курс лабораторных работ [2], предназначенный помочь студентам развить навыки программирования микроконтроллеров, необходимые для успешного усвоения теоретических сведений по способам и методам технических средств защиты информации, связанных с аппаратными и цифровыми устройствами. Курс лабораторных работ предполагается проводить с использованием симулятора-отладчика Micro-IDE фирмы-производителя BiPOM Electronics. Перед выполнением лабораторных работ студентам предлагается ознакомится с описанием микроконтроллеров семейства MC68HC11 и программы-отладчика Micro-IDE.

Список литературы

1. Простейшие технические средства защиты информации [Электронный ресурс]. – Режим доступа: http://aktrb.by/product/prosteyshie-tehnicheskie-sredstva-zashhityi-informatsii. – Дата доступа: 07.05.2024.

2. Логин, В. М. Интеллектуальные электронные системы безопасности: Лабораторный практикум. В 2 ч. Ч. 2 : Программирование микроконтроллеров: пособие / В. М. Логин, О. Ч. Ролич. – Минск : БГУИР, 2020. – 72 с.

ИССЛЕДОВАНИЕ НЕЗАДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В.В. Маликов

Совместное открытое акционерное общество «Коммунарка», Минск, Беларусь

В целях выявления возможных незадекларированных возможностей установленного прикладного программного обеспечения и уязвимостей в информационно-управляющей системе производственно-хозяйственной деятельности было проведено исследование уровня информационной безопасности с использованием решений «Kaspersky Symphony XDR».

В результате исследования было выявлено 128 случаев, детектированных компонентами «Kaspersky Symphony XDR» как аномальные (отличные от типовых / разрешенных правил функционирования).

В ходе детального изучения аномальных случаев функционирования были получены результаты:

– по причине генерации значительного числа подозрительных запросов к внешним ресурсам сети интернет – удалены 2 прикладных программных продукта, распространяемых в категориях «GNU» / «Freeware»;

– установлены и устранены попытки эксплуатации уязвимости операционной системы Windows;

– дополнительно установлена защита от нелегитимных задач/установки новых сервисов в планировщиках хостов и обращений к вредоносным ресурсам в сети интернет.

По результатам проведенного исследования принято решение о минимизации использования программных продуктов, распространяемых в категориях «GNU»/«Freeware».

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

Д.Л. Мартинкевич, Н.В. Насонова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Эксплуатация информационных систем (ИС), предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, регулируется приказом Оперативно-аналитического центра при Президенте РБ (ОАЦ) [1], который определяет порядок технической и криптографической защиты информации в таких ИС.

В соответствии с законодательством Республики Беларусь ограничение распространения информации в режиме коммерческой тайны (техническая информация, ноу-хау, бизнес-информация) является добровольным выбором владельцев компании. Но наличие в организации персональных данных, юридической, врачебной тайны или служебной информация ограниченного распространения накладывает на предприятие обязательства по ее защите, в первую очередь от несанкционированного доступа.

На основе типового класса ИС и подключения к открытым каналам передачи данных определяются требования к составу системы защиты информации (СЗИ) ИС. В комплекс СЗИ большинства коммерческих организаций для обеспечения защиты информации входят средства фильтрации и управления информационными потоками, средства обнаружения и предотвращения вторжений, мониторинга за функционированием ИС, средства централизованного управления учетными записями, потоковый антивирус, средства виртуализации, ПО антивирусной защиты, средства криптографической защиты информации, имеющие сертификат ОАЦ. Передача защищаемой информации осуществляется по протоколам стека протоколов TCP/IP и средств линейного шифрования на основе протоколов OpenVPN и TLS. Производится конфигурирование средств для обеспечения установленных требований по безопасности.

Заключительным этапом создания системы защиты является разработка политики информационной безопасности и локальных нормативно-правовых актов, ее поддерживающих, а также реализация организационных мер по защите информации, таких как особый режим допуска в помещения со средствами обработки информации распространение которой ограничено.

Список литературы

1. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 20 февраля 2020 г. № 66 [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа: 07.05.2024.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ НА ОСНОВЕ ОБОРУДОВАНИЯ HUAWEI

А.К. Матюшенко, П.А. Снигирь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Среди техник MITRE ATT&CK, использующих уязвимости канального уровня, известна такая техника, как Adversary in the Middle Attack (AiTM) с идентификатором T1557 [1]. Используя данную технику, нарушитель может осуществлять прослушивание сети, манипуляции с передаваемыми данными или реализовывать другие кибератаки. В соответствии с субтехникой 1557.002 [2] нарушитель, используя протокол канального уровня ARP (Address Resolution Protocol), может осуществлять кибератаку типа ARP-spoofing (ARP Cache Poisoning), то есть отравлять кэш протокола, чтобы позиционировать себя между двумя или более сетевыми устройствами.

Основным методом предотвращения ARP-spoofing в сетях является настройка функции ARP Anti-spoofing на коммутаторах. Минимальные настройки безопасности включают в себя строгое распознавание ARP, фиксированный ARP для предотвращения изменения записей поддельными ARP-пакетами и настройку отбрасывания ARP-пакетов.

Для анализа уязвимостей ARP-протокола была создана локальная сеть в виртуальной лаборатории PNETLab, которая предоставляет возможность моделирования локальных сетей на базе устройств различных производителей в режиме реального времени. Элементами созданной модели локальной сети являются:

– маршрутизатор Huawei серии NE40E;

– коммутатор Huawei серии CE6800;

– компьютер нарушителя с ОС Linux;

– компьютер пользователя с ОС Linux.

Для обеспечения безопасности от кибератак на канальном уровне предлагается настроить коммутатор, используя следующие команды [3]:

1. Настройка строгого распознавания ARP (команда arp learning strict).

2. Настройка фиксированного ARP (команда arp anti-attack entry-check fixed-mac enable).

3. Настройка безвозмездного отбрасывания ARP-пакетов (команда arp anti-attack gratuitous-arp drop).

В дальнейшем в смоделированной локальной сети в виртуальной лаборатории PNETLab планируется реализовать кибератаки на канальном уровне с целью тестирования правильности работы функции ARP Anti-Spoofing коммутатора Huawei серии CE6800.

Список литературы

1. Adversary-in-the-Middle [Электронный ресурс]. Режим доступа: https://attack.mitre.org/techniques/T1557/. – Дата доступа: 06.05.2024.

2. Adversary-in-the-Middle: ARP Cache Poisoning [Электронный ресурс]. Режим доступа: https://attack.mitre.org/techniques/T1557/002/. – Дата доступа: 06.05.2024.

3. Настройка безопасности ARP [Электронный ресурс]. Режим доступа: https://support.huawei.com/enterprise/ru/doc/EDOC1100112933/2fd242a8/configuring-arp-security-arp-anti-spoofing. – Дата доступа: 06.05.2024.

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

А.Д. Метельский, П.Б. Гусаков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Подготовка специалистов в области защиты информации является важной задачей, требующей комплексного подхода. Обучение должно включать в себя как теоретическую подготовку, так и практическое применение полученных знаний. Только так можно обеспечить эффективную защиту информации в современном мире.

В современном мире информация стала одним из самых ценных ресурсов. Защита информации от несанкционированного доступа, изменения, уничтожения или распространения стала критически важной задачей. Подготовка специалистов в области защиты информации играет ключевую роль в обеспечении информационной безопасности.

Подготовка специалистов в области защиты информации включает в себя обучение теоретическим основам информационной безопасности, изучение методов и технологий защиты информации, а также практическое применение полученных знаний. Теоретические основы включают в себя изучение принципов информационной безопасности, законодательных и нормативных актов, регулирующих область защиты информации, а также основ криптографии и систем защиты информации.

Специалисты в области защиты информации должны быть знакомы с различными методами и технологиями защиты информации, включая физическую защиту, программные и аппаратные средства защиты, методы обнаружения и предотвращения вторжений, а также методы резервного копирования и восстановления данных. Практическое применение знаний в области защиты информации включает в себя участие в проектах по обеспечению информационной безопасности, проведение аудитов безопасности, анализ угроз и рисков, разработку планов по обеспечению безопасности и реагированию на инциденты.

С развитием киберугроз, таких как вредоносные программы, фишинг, DDoS-атаки, кража данных и другие, специалисты в области защиты информации должны быть готовы к новым вызовам и постоянно обновлять свои знания и навыки. Кроме того, существует значительное количество законодательных и нормативных актов, которые регулируют область защиты информации. Важно ознакомиться с такими документами, чтобы понимать требования и стандарты, которым должны соответствовать специалисты в области информационной безопасности.

Список литературы

1. National Institute of Standards and Technology (NIST) [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/. – Дата доступа: 07.05.2024.

2. Information Systems Security Association (ISSA) [Электронный ресурс]. – Режим доступа: https://www.issa.org/. – Дата доступа: 07.05.2024.

ЗАЩИТА ПРОСТРАНСТВЕННЫХ ДАННЫХ ПОЛИГОНАЛЬНЫХ ОБЪЕКТОВ

А.И. Митюхин, З.Н. Мурашкина

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В работе рассматривается алгоритм передачи и обработки пространственных данных изображений с космических, авиационных средств наблюдения с целью защиты их от перехвата. Изображения могут отображать объекты инфраструктурного вида (промышленные сооружения, дороги, сети коммуникаций и пр.) Предполагается, что цифровые данные получены после процесса сегментации изображений. В центре внимания, например, могут находится геометрические, текстурные характеристики наблюдаемых объектов: длина, площадь, граница, вогнутости, форма и др. Изображения полигональных объектов описываются атрибутивными данными [1]. Особенность представления данных в атрибутивном виде позволяла эффективно использовать методы энтропийного и спектрального кодирования [2]. Для сокращения времени передачи считанной информации с максимально возможной скоростью, уменьшения времени на обнаружение интересующих радиоизлучений в исследовании применялся код Хаффмена и кодирование на основе дискретных функций Уолша. Уменьшение времени, требуемое на обнаружение, прием, анализ и декодирование перехватываемого сигнала имеет важное значение для надежной защиты информации в канале. Третий этап защиты основывался на применении помехоустойчивого кода Голда, обеспечивающего уменьшение мощности электромагнитного излучения сигнала. Проведены экспериментальные исследования рассмотренного алгоритма в канале с шумом с равномерно распределенной мощностью в полосе частот помехоустойчивого кода. Для этого использовался пакета имитационного математического моделирования Simulink. Эксперименты на однослойных полигонах показали возможность применения рассмотренного метода защиты пространственных данных. Дальнейшее продолжение исследований связано с оценкой надежности защиты данных многослойных полигонов.

Список литературы

1. Mitsiukhin, A. Compressing the geospatial data of testing grounds / A. Mitsiukhin / WSEAS Transactions on Environment and Development. – 2023. – Vol. 19. – P. 1386–1391.

2. Митюхин, А. И. Защита информации на основе спектрально-пространственного кодирования / А.И. Митюхин / Кодирование и цифровая обработка сигналов в инфокоммуникациях: матералы междунар. науч.-практ. конф., Республика Беларусь, Минск, 19 апреля 2021 г. – Минск: БГУИР, 2021. – С. 40–43.

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ФИЗИЧЕСКОГО ПРОЦЕССА ПЕРЕНОСА НОСИТЕЛЕЙ ЗАРЯДА В ГРАФЕНЕ, ВХОДЯЩЕМ В СОСТАВ ГЕТЕРОСТРУКТУРНОГО ПОЛУПРОВОДНИКОВОГО ПРИБОРА

В.Н. Мищенко, П.А. Матусевич, А.Д. Митрофанов, И. С. Сурвило

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Приведены результаты моделирования особенностей физического процесса переноса носителей заряда в графене, входящем в состав гетероструктурного полупроводникового прибора. Создание новых полупроводниковых приборов требует исследования свойств новых материалов, среди которых большое внимание привлекает

графен, представляющий двухмерный слой из атомов углерода. Исследование транспортных процессов переноса носителей заряда в графене связано с основными механизмами их рассеяния в гетероструктурных приборах. Для этих целей были использованы программные комплексы “Quantum Espresso” и “EPW”. С их помощью было выполнено моделирование основных параметров и характеристик транспортных процессов – дрейфовой скорости переноса носителей заряда и их подвижности. Моделирование из первых принципов выполнялись в рамках теории DFT (теории функционала электронной плотности), используя обменно-корреляционный функционал вида PBE (Perdew-Burke-Ernzerhof) и обобщенное градиентное приближение вида GGA. Рассматривался вариант небольших по величине энергий электрического поля и выполнения линеаризации транспортного уравнения Больцмана (BTE) для получения тензоров проводимости и подвижности. При итерационном решении BTE получены зависимости средней скорости и подвижности носителей заряда от величины температуры и ряда других параметров. Результаты исследования особенностей физического процесса переноса носителей заряда в графене могут служить основой для создания новых гетероструктурных приборов, Графеновые гетероструктурные приборы с улучшенными выходными характеристиками позволят создать новые функциональные устройства, которые найдут широкое применение в системах передачи и обработки сигналов СВЧ и КВЧ диапазонов.

МОДЕЛИРОВАНИЕ ИЗ ПЕРВЫХ ПРИНЦИПОВ ТРАНСПОРТНЫХ СВОЙСТВ НОСИТЕЛЕЙ ЗАРЯДА В ГРАФЕНЕ, МОДИФИЦИРОВАННОМ АТОМАМИ ВОДОРОДА

В.Н. Мищенко, П.А. Матусевич, А.Д. Митрофанов, И.С. Сурвило

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Приведены результаты моделирования из первых принципов транспортных свойств носителей заряда в графене модифицированном атомами водорода. Разработка новых полупроводниковых приборов требует исследования свойств новых материалов и графен является одним из таких материалов, которые привлекают интерес исследователей. Графен с добавление атомов ряда других химических элементов, в том числе и водорода, позволяет создавать его химические модификации, обладающими новыми свойствами и характеристиками. Было выполнено моделирование из первых принципов параметров и характеристик гидрированного графена типа C_2H_2, который в литературе получил название графан. При моделировании были использованы программные комплексы Quantum Espresso и EPW, используя параметризацию PBE (Perdew-Burke-Ernzerhof) и обобщенное градиентное приближение вида GGA. Для расчета зависимостей скорости и подвижности носителей заряда от величины энергии был использован программный комплекс EPW. Для установления зависимостей величин скорости и подвижности носителей заряда от величины параметров моделирования их значения выбирались из специальных диапазонов. Так размер сеток вида $N \times N \times 1$ для при процедурах интерполяции определялся значением параметра N, величина которого изменялась в пределах от 120 до 300. Величина коэффициента сглаживания по Гауссу принималась равной 0,001 эВ. Количество функций Ванье (Wannier) при операциях интерполирования принималось равным величине 12. Путем итерационного решения транспортного уравнения Больцмана определены зависимости скорости и подвижности носителей заряда от величины температуры и ряда других параметров. Полученные зависимости и параметры гидрированного графена могут служить основой для создания новых гетероструктурных приборов, содержащих слои

модифицированного графена и других полупроводниковых материалов. Совершенствование технологии формирования гетероструктурных приборов с использованием графена и его модификаций позволит получить новые устройства и структуры, которые найдут широкое применение в системах передачи и обработки сигналов диапазонов сантиметровых и миллиметровых волн.

ДВУХСЛОЙНЫЕ УГЛЕСОДЕРЖАЩИЕ ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ПОЛИУРЕТАНОВОЙ МАСТИКИ И ПОЛИВИНИЛАЦЕТАТНОЙ ДИСПЕРСИИ

В.С. Мокеров, Е.С. Белоусова, О.В. Бойправ

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В работе [1] были представлены результаты исследования углесодержащих поглотителей на основе полиуретановой мастики, поверхность которых представляет собой совокупность полусферических геометрических неоднородностей. По результатам этого исследования экспериментально установлено, что увеличение до 25 мм диаметра полусферических геометрических неоднородностей на поверхности поглотителя электромагнитного излучения приводит к увеличению на 3–9 дБ значений коэффициентов отражения и передачи электромагнитного излучения (ЭМИ) в диапазоне частот 2–17 ГГц.

В работе [2] представлены результаты исследования углесодержащих поглотителей ЭМИ на основе поливинилацетатной дисперсии, поверхность которых представляет собой совокупность полусферических геометрических неоднородностей. По результатам этого исследования установлено, что поглотители ЭМИ, изготовленные на основе водного раствора поливинилацетатной дисперсии, характеризуются более низкими значениями коэффициента поглощения ЭМИ от 0,75–0,99, а также меньшей в 1,5–2,0 раза массой 5,0 кг/м^2 по сравнению с поглотителями, изготовленными на основе водного раствора гипса (7,5 кг/м^2) и полимерной мастики (9,5 кг/м^2).

В данной работе представлены результаты исследований характеристик отражения и передачи ЭМИ образцов многослойных поглотителей, которые комбинировались из углесодержащих поглотителей на основе поливинилацетатной дисперсии (слой А) или полиуретановой мастики (слой Б), поверхности которых представляли собой совокупность полусферических геометрических неоднородностей. Для первого образца поглотителя использовались слои в следующей комбинации А+Б, а для образца 2 – А+А. В результате проведенных измерений было установлено, что рабочий диапазон частот исследованных поглотителей – 5,5–16 ГГц. У обоих образцов поглотителей значения коэффициента отражения ЭМИ в рабочем диапазоне частот изменяется в пределах –7… –18 дБ, а значения коэффициент передачи – в пределах –21…–29 дБ в рабочем диапазоне частот. В ходе проведения измерений было установлено, что частотные характеристики обоих образцов коррелируют между собой.

Таким образом, исследованные образцы поглотителей ЭМИ характеризуются одинаковой эффективностью ослабления ЭМИ. Однако образец 1 (10,0 кг/м^2) по сравнению с образцом 2 (14,5 кг/м^2) имеет меньшую массу за счет того, что оба его слоя изготовлены на основе поливинилацетатной дисперсии, в то же время образец 2 по сравнению с образцом 1 имеет повышенную механическую прочность и эластичность за счет того, что один из его слоев изготовлена на основе полиуретановой мастики.

Список литературы

1. Белоусова, Е. С. Углесодержащие поглотители электромагнитного излучения с полусферическими геометрическими неоднородностями / Е. С. Белоусова, О. В. Бойправ, С. Э. Саванович // Электромагнитные волны и системы. – 2024. – Т. 29, № 2. – С. 22−29.

2. Углесодержащие поглотители электромагнитного излучения СВЧ-диапазона с рельефной поверхностью / О. В. Бойправ [и др.] // Известия Национальной академии наук Беларуси. Серия физико-технических наук. – Т. 69, № 1. – 2024. – С. 17–27.

ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ МОДИФИЦИРОВАННЫХ УГЛЕЙ

В.С. Мокеров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Использование модифицированного активированного угля при создании поглотителей электромагнитного изучения (ПЭИ) позволяет улучшить их коэффициенты отражения и передачи в различных диапазонах частот, увеличить механическую прочность. Выделяют следующие способы модификации углей, такие как пропитывание водными растворами, химическая модификация, изменение формы и структуры. В зависимости от размера фракций угля его гидрофильность может увеличивается на 25 %. Поэтому использование пропитки угля водными растворами на основе сульфатов и хлоридов является эффективным методом его модификации.

В данной работе представлены результаты сравнения частотных характеристик коэффициентов отражения и передачи ПЭИ на основе углей, модифицированных пропиткой водными растворами на основе хлоридов и сульфатов. Выбор метода пропитки активированного угля различными растворами обосновывается доступностью и экономичностью используемых материалов (до 100 бел. руб.), также данный способ модификации способствует уменьшению значений коэффициента отражения (до –4,5 дБ) и передачи (до –9 дБ) в диапазоне частот 10–12 ГГц.

По разработанной методике [1] были изготовлены образцы ПЭИ, в составе которых использовался активированные уголь, пропитанный следующими растворами: $MgSO_4$, $(NH_4)_2SO_4$, K_2SO_4, $CaCl_2$, NaCl, $MgCl_2$. В качестве связующего материала в ПЭИ использовалась полиуретановая мастика и отвердитель в соотношении 3:1.

На основе проведенных измерений было установлено, что наименьшими значениями коэффициентов отражения и передачи обладают следующие образцы:

1 ПЭИ на основе полиуретановой мастики с добавлением активированного угля, модифицированного путем пропитки в растворе $MgCl_2$ с коэффициентом отражения –8,3 дБ и коэффициентов передачи –25 дБ в диапазоне частот 8–15 ГГц.

2 ПЭИ на основе полиуретановой мастики с добавлением активированного угля, модифицированного путем пропитки в растворе K_2SO_4 с коэффициентом отражения –10 дБ и коэффициентов передачи –11,6 дБ в диапазоне частот 6,5–13 ГГц.

3 ПЭИ на основе полиуретановой мастики с добавлением активированного угля, модифицированного путем пропитки в растворе NaCl с коэффициентом отражения –11,2 дБ и коэффициентов передачи –14,2 дБ в диапазоне частот 13–17 ГГц.

Таким образом, полученные ПЭИ на основе модифицированных углей могут быть использованы для создания новых материалов с улучшенными свойствами поглощения электромагнитного излучения, что имеет большое значение для различных областей применения, включая электронику, радиотехнику и телекоммуникации.

Список литературы

1. Белоусова, Е. С. Методика модификации порошкообразного активированного угля для совершенствования поглотителей электромагнитного излучения / Е. С. Белоусова, В. С. Мокеров, О. В. Бойправ // Современные средства связи: материалы XXVIII Междунар. науч.-техн. конф., Минск, 26–27 октября 2023 года; редкол.: А. О. Зеневич [и др.]. – Минск: Белорусская государственная академия связи, 2023. – С. 81–83.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В ПРИЛОЖЕНИИ TELEGRAM

С.В. Недбайлик, П.Б. Гусаков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Основное отличие криптосистемы Telegram от стандартных криптосистем заключается в применении ряда уникальных методов шифрования данных.

1. Сквозное шифрование – шифрование, которое подразумевает генерацию ключей на устройствах клиентов в системе «клиент-клиент», ключи генерируются на устройствах клиентов.

2. Шифр RSA – алгоритм шифрования данных в ассиметричных криптосистемах. Суть заключается в генерировании случайных открытых ключей и последующая генерация закрытых ключей, на основе открытых (вычисления закрытого ключа производится при помощи функции mod).

3. Алгоритм SHA-256 – алгоритм обращения (шифрования) данных в крипто текст при помощи хэш-функции. Использует слово длиной 32 бит, 256 – размер хэш-сообщения.

4. Алгоритм AES-256 – симметричный алгоритм блочного шифрования.

5. Алгоритм Диффи-Хеллмана – алгоритм шифрования, позволяющий получить секретный ключ, используя незащищенный от прослушивания канал связи.

Шифрование происходит по следующей схеме:

1.Создание закрытого ключа посредством алгоритма DH.

2.Разбиение пакета на случайно 64 бит число меняющееся каждые 30 минут, случайного 64 бит числа, используемого для однозначной идентификации сообщения в сеансе, текста сообщения, добавление (12–1024 бит) «пустых» битов информации с целью повышения криптостойкости.

3.Далее ключ и текст шифруются алгоритмом SHA-256, ключ переписывается и сохраняется в виде хэш-функции.

4.Ключ переформируется на основе SHA – 256 на основе секретного значения.

5.Формирование ключей и создание шифрование сообщение AES-256 алгоритмом.

6.Разбиение сообщения на (64 бит) хеша SHA-1 и используется для идентификации ключа. 128 бит хеша SHA-256. Зашифрованного сообщения.

Особенность заключается в применении как симметричного, так и ассиметричного шифрования информации. Так же важной составляющей является применение сквозного шифрования данных, при котором ключи, как открытые, так и закрытые генерируются и хранятся на устройствах клиентов, что делает невозможным их перехват (за исключением случаев, в которых устройство клиента является скомпрометированных, но в таком случае нарушитель столкнется с проблемой, так как ключ хранится в виде хэша).

Список литературы

1. Шо там по MTProto в Telegram-то? [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/590667/. – Дата доступа: 07.05.2024.
2. Практическая криптография / под. ред. Н. Фергюсона, Б. Шнайера. – М.: Издательский дом «Вильямс», 2004. – 420 с.

ИСПОЛЬЗОВАНИЕ ПОЛЕЙ ЗАГОЛОВКА IP-ПАКЕТА ДЛЯ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

А.Н. Николайчук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Сетевая модель TCP/IP описывает процесс передачи информации между двумя устройствами сети. Согласно этой модели, символьное сообщение отправителя преобразуется к бинарной последовательности, отправляется, а также дополняется некоторой служебной информацией, которая необходима, например, для того, чтобы обратно преобразовать бинарную последовательность получателя к исходному символьному сообщению.

В зависимости от типа данных (видео, картинка), служебная информация будет формироваться по-своему, в соответствии с некоторыми правилами, которые принято называть протоколами. Но использовать разные способы передачи данных для разных типов было бы неэффективно, поэтому операцию преобразования сообщения разбили на несколько уровней (прикладной, транспортный, сетевой, канальный), чтобы вне зависимости от типа входных данных сформированная бинарная последовательность имела одинаковую структуру. Название стека (набора) протоколов TCP/IP, на котором базируется Интернет происходит из двух важнейших протоколов семейства – Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны первыми.

Протокол IP объединяет сегменты (данные транспортного уровня) в единую сеть, обеспечивая доставку пакетов (данные сетевого уровня) между любыми узлами сети через произвольное число промежуточных. IP не гарантирует надежной доставки пакета до адресата. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня. Возможно также возникновение ситуации, когда размер пакета превысит возможности узла системы связи. Для таких случаев протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки (фрагментация). В известных методах сетевой стеганографии используются следующие поля заголовка пакета протокола IP: Type of Service, Identification, Flags, Fragment Offset, Options, Padding [1–3]. Использование именно этих полей для задач стеганографии обусловлено тем, что они, при некоторых условиях, позволяют разместить дополнительную информацию в пакете, так как существуют ситуации, при которых данные поля не используются. Однако такие методы характеризуются низкой пропускной способностью [4].

Список литературы

1. Zander, S. A Servey of convert channels and countermeasures in computer network protocol / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials – 2007. – Vol. 9. – № 3. – P. 44–57.
2. Handel, T. Hiding data in the OSI network model / T. Handel, M. Sandford // Proceedings of the First International Workshop on Information Hiding. – 1996. – P. 23–38.

3. Jankowski, B. PadSteg: Introducing inter-Protocol Steganography / B. Jankowski, W. Mazurczyk, K. Szczypiorski // Telecommunication Sys-tems. – 2011. – Vol. 52. – No. 2. – P. 1101–1111.

4. Применения сетевой стеганографии для скрытия данных, передаваемых по каналам связи / О.Ю. Пескова, Ю. Г. Халабурда // Известия ЮФУ. Технические науки. – 2012.

КОНЦЕПЦИЯ ПОСТРОЕНИЯ МОДУЛЯ ЗАЩИТЫ WEB-ПРИЛОЖЕНИЯ НА ОСНОВЕ ИМИТАЦИИ И АНАЛИЗА СЕТЕВЫХ АТАК

Д.Н. Одинец, В.Л. Кулеш, Е.А. Алуев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время все большее число организаций обращают внимание на повышение надежности и безопасности своих web-приложений. Особенно это актуально для банковских компаний, имидж, а соответственно, и успешность работы которых, в первую очередь зависят от надежности и безопасности их web-приложений. Учитывая изложенное выше, разработка программного модуля защиты web-приложения на основе имитации и анализа сетевых атак сегодня является очень актуальной задачей.

Использование автоматизированного поиска уязвимостей web-ресурсов при помощи учета специфики исследуемых программ позволит предотвращать возможные атаки злоумышленников путем выявления, анализа и устранения уязвимостей web-приложения заблаговременно.

Предложена концепция обнаружения и защиты web-приложения от сетевых атак злоумышленников, на основе которой разработан кроссплатформенный программный модуль. Данный модуль работает на основе имитации сетевых атак и их анализе. Основное отличие созданного модуля от основных известных вариантов сетевых атак – поиск уязвимостей web-приложения в автоматизированном режиме.

Разрабатываемый программный модуль защиты web-приложения позволил выявлять следующие основные варианты уязвимости web-приложения:

– обнаружение, анализ и блокирование SQL-инъекций;

– обнаружение, анализ и блокирование возможности осуществления некорректной авторизации и управления сеансами;

– обнаружение, анализ и блокирование возможности межсайтового выполнения сценариев;

– обнаружение, анализ и блокирование возможности отказа в обслуживании.

Основу концепции составляют следующие алгоритмы:

– алгоритм сбора информации о целевом web-приложении;

– алгоритм сканирования приложения;

– алгоритм анализа результатов;

Такой подход дает возможность создать гибкую структуру программного модуля, что позволяет в дальнейшем модифицировать продукт путем добавления новые блоков и изменения старых без существенных вмешательств в общею схему работы всей взаимосвязанной системы.

В результате исследований получены записи логов для документирования фактов атак в виде списка и сохранения этой информации в файл. Каждая запись в этом списке является кортежем, содержащий тип атаки и временную метку атаки. Визуально это выглядит как [('DDoS', '2024-04-23 15:30:45'), ('SQL Injection', '2024-04-23 15:32:18'), ('Phishing', '2024-04-23 15:35:02')].

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Р.Д. Осипов, А.С. Герасимов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В этой работе будут рассмотрены приложения и средства защиты информации.

1. SIEM-системы оперативно обнаруживает внешние и внутренние атаки, оценивает уровень защиты информационной системы, формировать отчеты и другую аналитику. К таким системам относятся:

– MaxPatrol SIEM;

– RuSIEM.

2. Средства защиты информации от несанкционированного доступа нужны для защиты сети и данных от посторонних. Данные средства контролируют работу процессов и программ, управляют информационными потоками между устройствами, сканируют внешние и внутренние носители. К таким средствам относятся:

– Dallas Lock;

– электронный замок «Соболь».

3. Средства антивирусной защиты информации предназначены для поиска вредоносных программ и восстановления поврежденных файлов. К таким средствам относятся:

– «Доктор Веб»;

– ESET NOD32.

4. Средства межсетевого экранирования предназначены для защиты от проникновения в корпоративную сеть. К таким средствам относятся:

– TrustAccess;

– «Континет».

5. Средства обнаружения и предотвращения вторжений используются для выполнения анализа данных в корпоративных сетях в целях установления факта несанкционированного доступа. К таким средства относятся:

– VipNet IDS;

– «Рубикон».

Средства криптографической защиты информации защищают саму информацию, не давая ее прочесть нарушителям. К таким средствам относятся:

– КриптоПро CSP;

– КриптоАРМ.

Список литературы

1. СЗИ (Средства защиты информации): виды, для чего нужны, как выбрать [Электронный ресурс]. – Режим доступа: itglobal.com. – Дата доступа: 07.05.2024.

ИНТЕГРАЦИЯ СИСТЕМЫ ПОЛИГРАФИИ В МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ IOS: ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ

Н.В. Песняк

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

В современном цифровом мире мобильные приложения становятся неотъемлемой частью повседневной жизни пользователей, однако вместе с их распространением возникают и новые вызовы в обеспечении безопасности [1].

В данной научной работе обсуждаются технические аспекты разработки мобильного приложения для iOS, интегрированного с полиграфической системой, с целью автоматизации и усовершенствования процесса детектирования лжи.

Мы рассматриваем использование современных технологий, таких как микроконтроллер ESP32, для передачи данных с полиграфа на мобильное устройство по протоколу Bluetooth Low Energy, обеспечивая при этом экономию энергии и надежную связь.

В работе описывается использование различных датчиков, таких как датчик пульса, датчик сердечного ритма и модуль гальванических измерений, для сбора физиологических данных, необходимых для анализа вероятности лжи.

Особое внимание уделяется аспектам безопасности данной интегрированной системы. Обсуждаются меры по защите данных, передаваемых между мобильным приложением и полиграфом, а также методы обеспечения конфиденциальности и целостности полученных результатов.

Исследование показывает, что интеграция полиграфической системы с мобильными приложениями открывает новые перспективы для применения в различных областях, включая обеспечение безопасности и доверия к передаваемой информации [1].

Дальнейшие исследования будут направлены на улучшение алгоритмов анализа данных и расширение функциональности системы с целью повышения ее эффективности и надежности. Это исследование представляет собой важный шаг в направлении обеспечения безопасности и защиты информации в мобильных приложениях, а также в повышении доверия к передаваемым данным.

Список литературы

1. Фрай, О. Ложь. Три способа выявления. Как читать мысли лжеца, как обмануть детектор лжи / О. Фрай. – СПб.: Прайм-ЕВРОЗНАК, 2006. – 284 с.

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

И.А. Петриченко, Е.А. Лещенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Распределенные информационные системы (РИС) характеризуются передачей данных между территориально разнесенными компонентами, что повышает риск несанкционированного доступа и утечки конфиденциальной информации. В связи с этим обеспечение информационной безопасности в РИС является ключевой задачей.

Существует 3 основных средства криптографической защиты информации: программные, аппаратные и программно-аппаратные. Их цель состоит в том, чтобы:

– уберечь информацию во время ее изменения, использования и отправки;

– обеспечить целостность и подлинность данных при хранении, обработке и распространении;

– создавать информацию, которая будет применяться для аутентификации и идентификации субъектов, людей и устройств;

– выработать данные, используемые для сохранности аутентифицирующих средств при их хранении, создании, изменении и передаче.

Есть четыре основных метода криптографической защиты информации:

– симметричное шифрование: Использование общего ключа для шифрования и расшифрования данных. Примеры: AES, DES, Blowfish;

– асимметричное шифрование: Использование открытого и закрытого ключей. Примеры: RSA, Эллиптические кривые;

– хэширование: Применение криптографических хэш-функций для обеспечения целостности данных. Примеры: SHA-2, MD5;

– электронная цифровая подпись: Использование закрытого ключа для создания подписи, проверка с помощью открытого ключа. Примеры: DSA, ГОСТ Р 34.10.

Применение криптографических методов и средств является важным элементом обеспечения информационной безопасности в распределенных информационных системах. Их использование позволяет защитить конфиденциальность, целостность и доступность данных, циркулирующих в РИС.

Список литературы

1. Криптографическая защита информации: цели, методы, технологии [Электронный ресурс]. – Режим доступа: https://gb.ru/blog/kriptograficheskaya-zaschita-informatsii/. – Дата доступа: 07.05.2024.

ОСОБЕННОСТИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ СИСТЕМЫ ВЫСШЕГО ОБРАЗОВАНИЯ

А.Д. Петров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

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.

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 г. «О совершенствовании государственного регулирования в области защиты информации» 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 г. № 449 подробно описано в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

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.

УЯЗВИМОСТИ ИДЕНТИФИКАТОРА RFID-МЕТОК

С.Н. Петров[1], К.С. Булавин[2], А.О. Ворожцов[2]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2] *Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

Широкая область применения RFID-систем (систем радиочастотной идентификации) определяет необходимость защиты таких систем, и в особенности, RFID-меток (уникальных идентификаторах), как наиболее уязвимых элементов систем. Разработка механизмов защиты от атак на идентификатор метки способствует безопасному использованию систем на базе RFID в СКУД, здравоохранении, медицине и логистике

Устройство RFID-систем можно разделить на различные уровни, распределенные стандартами и физическими характеристиками меток. Каждый уровень имеет свои уязвимые места, в связи с чем существует большое количество атак на каждый из существующий уровней. Недостаточный уровень защищенности меток на физическом уровне, к примеру, позволяет нарушителю заменить в магазине метку желаемого товара меткой более дешевого товара. Открытость радиоканала, используемого как передачи данных, делает возможным перехват необходимых данных клонирования подлинной метки. На другом уровне нарушитель может использовать пространство метки, выделенное для данных для записи вредоносного кода с целью его дальнейшего распространения.

Эффективная защита RFID-меток достигается добавлением методов противодействия атакам для каждого из уровней коммуникации. Механизм взаимной аунтефикации карты и терминала может предотвратить изменение битов доступа к секторам памяти и перезаписи данных. Данное средство защиты позволяет закрыть возможность считывания данных с карты, выдав устройство за легитимный терминал, в том числе это реализуемо экранированием при помощи материалов, исключающих прохождение какого-либо сигнала. Наличие перезаписываемой памяти позволяет хранить в ней временные метки соединения, за счет которых возможна реализация как взаимной аутентификации, так и использование их для шифрования, как противодействие восстановлению ключа шифрования с последующей расшифровкой. Важной контрмерой является постоянная проверка метки на наличие вредоносного кода во время каждого цикла считывания информации.

СЛОЖНОСТИ ЭКСПЛУАТАЦИИ SIEM-СИСТЕМ ПРИ ОБРАБОТКЕ БОЛЬШОГО ОБЪЕМА СОБЫТИЙ БЕЗОПАСНОСТИ

С.Н. Петров, Г.С. Смотрук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В современной информационной среде, на фоне возрастающей сложности киберугроз, системы управления событиями и информационной безопасности (SIEM) выступают в роли ключевого инструмента обеспечения целостности и защиты информационных активов организаций. Несмотря на их важность, SIEM системы

сталкиваются с комплексом системных вызовов, которые требуют непрерывного внимания и усовершенствования.

Одной из основных проблем, является необходимость эффективной обработки и анализа огромного объема событий. В современных организациях, где сотни и тысячи устройств и приложений генерируют большое количество данных о событиях безопасности, SIEM системы должны оперативно обрабатывать эти данные для обнаружения и реагирования на угрозы в реальном времени. Однако, высокая скорость поступления информации, в сочетании с ограниченными ресурсами вычислительной мощности и хранилища данных, создает серьезные препятствия для SIEM. Это может привести к ситуации, когда система не успевает обработать все поступающие события в реальном времени, что в свою очередь может привести к упущению важных угроз или задержке их обнаружения.

Еще одной серьезной проблемой является неэффективная интеграция и корреляция данных из различных источников безопасности. Поскольку информация о безопасности формируется из множества источников, включая журналы событий операционных систем, логи сетевых устройств, журналы приложений, системы обнаружения и предотвращения вторжений и многих других, SIEM системы должны успешно интегрировать данные из всех этих источников и анализировать их в единой системе для выявления угроз и реагирования на них. Недостаточная интеграция и корреляция данных приводит к ложным срабатываниям, что в свою очередь, к избыточной нагрузке на персонал по их обработке и, в конечном итоге, к игнорированию реальных угроз.

Решение данных проблем требует комплексного подхода, включающего в себя применение передовых технологий анализа данных, таких как машинное обучение и искусственный интеллект, оптимизацию инфраструктуры и ресурсов. Для эффективного функционирования SIEM необходимо постоянное совершенствование алгоритмов анализа данных, улучшение интеграции с различными источниками информации и повышение гибкости системы. Только таким образом можно обеспечить эффективное функционирование SIEM систем и надежную защиту информационных активов организаций в условиях постоянно меняющихся угроз.

GOOGLE DORKING КАК МЕТОД АНАЛИЗА ЗАЩИЩЕННОСТИ ВЕБ-РЕСУРСОВ

А.П. Поблагуев, А.И. Ильющенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

1. Постановка проблемы: в современном мире киберугрозы становятся все более актуальными, вследствие чего, защита веб-ресурсов от кибератак становится приоритетной задачей для компаний и организаций.

2. Цель исследования: проанализировать эффективность использования Google Dorking в области проверки и обнаружения уязвимостей на веб-ресурсах.

3. Задачи исследования:

– изучение основных принципов и методов Google Dorking;

– анализ возможностей Google Dorking для обнаружения уязвимостей веб-ресурсов;

– проведение практических экспериментов с использованием Google Dorking для проверки безопасности различных веб-сайтов, с помощью Google Hacking Database, а также других ресурсов, содержащих перечни Google Dork запросов;

– автоматизация отправки Google Dork запросов, а также вывод этой информации в более удобном и структурированном виде, с помощью уже созданных утилит;

– сравнение результатов анализа с другими методами проверки безопасности.

4. Методы реализации: так как отправка Google Dork запросов не является незаконной, мы можем без каких-либо ограничений оправлять запросы и анализировать полученную информацию, для этого будет использовать следующие утилиты: DorkScout, Webdork.

5. Общее заключение: Результаты исследования позволят оценить эффективность Google Dorking в качестве инструмента анализа защищенности веб-ресурсов и найти лучшие методы защиты в области кибербезопасности. В дальнейшем это может способствовать повышению уровня защиты данных и предотвращению кибератак [1–6].

Список литературы

1. Практическое руководство [Электронный ресурс]. – Режим доступа: https://www.freecodecamp.org/news/google-dorking-for-pentesters-a-practical-tutorial/. – Дата доступа: 07.05.2024.

2. Как найти что-либо через Google Dorking [Электронный ресурс]. – Режим доступа: https://cyberlab1.medium.com/how-to-find-anything-through-google-dorking-d288132ddd00. – Дата доступа: 07.05.2024.

3. Использование Google Doking [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/postuf/articles/510766/. – Дата доступа: 07.05.2024.

4. Google Dorking [Электронный ресурс]. – Режим доступа: https://www.imperva.com/learn/application-security/google-dorking-hacking/. – Дата доступа: 07.05.2024.

5. DorkScout [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/dorkscout-automate-google-dork-scan-against-the-entiere-internet-or-specific-targets/. – Дата доступа: 07.05.2024.

6. Webdork [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/webdork-python-tool-to-automate-dorking/. – Дата доступа: 07.05.2024.

АКТУАЛЬНЫЕ АСПЕКТЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

К.Б. Поляков, И.Г. Скиба

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Постепенное упорядочение имеющегося нормативного массива в сфере защиты личной информации завершилось принятием Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон № 99-З). Преамбула Закона № 99-З гласит: «Настоящий Закон направлен на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных» [1].

Глава 1 Закона 99-З содержит толкование основных терминов (понятие персональных данных, их видов, оператора персональных данных, обработка и т. д.), которые используются в данной сфере законодательства, предмет Закона № 99-З и сферу действия [1]. Глава 2 Закона № 99-З направлена на регламентацию механизма обработки персональных данных. В рассматриваемой главе урегулированы вопросы согласия субъекта на обработку персональных данных, распоряжения персональными

данными несовершеннолетних и недееспособных, права наследников после смерти субъекта персональных данных и другие [1].

Главой 3 Закона №99-З регламентированы права и обязанности субъекта персональных данных и оператора [1]. Среди них право на отзыв согласия об обработке персональных данных, право на получение информации, касающейся обработки персональных данных, и изменение персональных данных и т.д.

Глава 4 устанавливает уполномоченный орган по защите прав субъектов персональных данных, а также ответственность за нарушение законодательства о защите персональных данных. Национальный центр защиты персональных данных Республики Беларусь (далее-Центр) является уполномоченным органом по защите прав субъектов персональных данных [1]. Как отмечено на официальном сайте Центра персональных данных учредителем является Оперативно-аналитический центр при Президенте Республики Беларусь. Центр действует независимо на основе Конституции Республики Беларусь, Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», Положения о Национальном центре защиты персональных данных, утвержденного Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных», а также приказов Оперативно-аналитического центра при Президенте Республики Беларусь.

Так, например, Центр оказывает образовательные услуги на основе приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 «Об обучении по вопросам защиты персональных данных». Также в пример можно привести новеллу законодательства о защите персональных данных: с 01.01.2024 в Республике Беларусь стал функционировать Реестр операторов персональных данных (далее-Реестр). В приказе Оперативно-аналитического центра при Президенте Беларуси № 94 от 1 июня 2022 года «О государственном информационном ресурсе «Реестр операторов персональных данных» регламентированы критерии ресурсов и системах, сведения о которых должны быть включены в Реестр.

Список литературы

1. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З ; в ред. Закона Респ. Беларусь от 01.06.2022 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

РОЛЬ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ: ТЕХНОЛОГИИ И РЕАЛИЗАЦИИ

И.В. Пронин, М.В. Романюк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Многофакторная аутентификация (MFA) – это концепция защиты, требующая как минимум двух способов аутентификации данных учетной записи, чтобы установить истинность личности и разрешить доступ в систему. Для проверки идентификационных данных многофакторная аутентификация объединяет несколько или более факторов, которые не связаны между собой напрямую.

Цель многофакторной аутентификации – путем формирования многоуровневой защиты осложнить злоумышленнику получение несанкционированного доступа в систему: сеть, устройства, базы данных.

Для возможности использования сценариев многофакторной аутентификации требуется поддержка следующих технологий:

– физические устройства, которые владелец носит при себе;

– приложения, которые создают временный одноразовый PIN-код;

– SMS-сообщения или обратные звонки на телефон;

– биометрия.

Все это говорит о том, что решения по многофакторной аутентификации требуют дополнительных ресурсов на их установку и обслуживание. Иногда затраты могут быть единовременными, а в некоторых случаях компании-поставщики взимают с пользователей ежегодную плату. Эти аспекты необходимо учитывать.

Стоит отметить, что многофакторная аутентификация не решает проблем той же парольной защиты в корне – она лишь усложняет задачу злоумышленника за счет ввода еще одного фактора. Ключевой изъян – отсутствие прямой связи с личностью пользователя – остается на месте. Поскольку возможность выдать себя за другого человека сохраняется, взломщики ищут обходные пути.

В целом, если нет специальных требований к системе защиты, а риски, связанные с компрометацией учетной записи, не слишком велики, то многофакторная аутентификация вполне надежна и в любом случае превосходит большинство однофакторных вариантов – особенно в том случае, если сотрудники или клиенты обучены базовым мерам безопасности.

Список литературы

1. Системы и методы аутентификации пользователей [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods. – Дата доступа: 07.05.2024.

2. Многофакторная аутентификация [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/events/blog/3421/?ysclid= lv0v5vykj0754775070. – Дата доступа: 07.05.2024.

АКТУАЛЬНОСТЬ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ПОВЕДЕНЧЕСКИМ ХАРАКТЕРИСТИКАМ

Т.А. Пулко[1], А.А. Лах[2], С.С. Румас[2]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2] *Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

В современном цифровом мире обеспечение безопасности данных и идентификации пользователей имеет первостепенное значение. Традиционные методы аутентификации, такие как пароли и токены, часто уязвимы для взлома и фишинга. Биометрическая аутентификация по поведенческим характеристикам предлагает надежное и удобное решение для преодоления этих проблем.

Поведенческая биометрика анализирует уникальные паттерны поведения пользователей, такие как динамика набора текста, движения мыши, использование сенсорного экрана, схема навигации и прочее, позволяя осуществлять аутентификацию пользователей автоматически на основе их поведения. Эти характеристики сложно подделать или взломать, при этом они остаются постоянными во времени, что делает их надежными идентификаторами, снижающими риск несанкционированного доступа и мошенничества. К изменяющимся паттернам поведения пользователей поведенческая биометрика может адаптироваться, обеспечивая непрерывную безопасность. Следует

отметить, что поведенческие характеристики не передаются через электронную почту или текстовые сообщения, что делает их неуязвимыми для популярных в настоящее время атак фишинга. Многие отрасли, такие как здравоохранение и финансы, требуют строгих мер безопасности, и биометрическая аутентификация по поведенческим характеристикам помогает организациям соответствовать этим требованиям. Помимо актуальности, биометрическая аутентификация по поведенческим характеристикам предлагает ряд преимуществ, связанных с аутентификацией без вмешательства пользователя, минимальными затратами на внедрение таких систем и их точностью, которая может достигать более 99 %. По мере совершенствования технологий поведенческая биометрика будет играть все более важную роль в создании безопасной и бесшовной цифровой среды.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ЯДЕРНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Кибербезопасность АЭС означает защиту технологического процесса от несанкционированного доступа и обеспечивается за счет эффективного управления системам АСУ ТП, решающими задачи надежного регулирования основного технологического процесса. При этом информация о ходе технологического процесса в АСУ ТП не представляется «в чистом виде», а поступает через систему защиты, которая для устранения искажений и сохранения конфиденциальности требует внедрения в технические средства АСУ ТП соответствующих программных или технических механизмов [1].

Особенностью структуры и алгоритмов работы технических средств защиты информации является согласование с принятой на АЭС структурой глубокоэшелонированной защиты, в которой каждый уровень защиты имеет свою подсистему информационной безопасности и обеспечивает определенную эффективность защиты барьеров от характерных для данного уровня воздействий и определенного типа атаки. Поэтому у АЭС, как и у любого крупного промышленного объекта автоматизации, можно выделить пять контуров кибербезопасности со своими техническими средствами.

В первом находятся все датчики, подключенные к программно-логическим контроллерам (ПЛК). Второй контур (шлюзовой) осуществляет сбор информации с ПЛК и ее передачу в сеть системы верхнего блочного уровня (СВБУ). В третьем контуре находится СВБУ, с которой взаимодействует оператор, управляющий технологическим оборудованием АЭС. В четвертом контуре с данными СВБУ работают технологи, отвечающие за конкретную подсистему АЭС. Пятый контур – контур внешнего доступа, сопряженный с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления.

АСУ ТП атомной электростанции находится в изолированной сети и отключена от внешних сетей, поэтому нелегитимное подключение к АЭС полностью контролируется системой безопасности АЭС, работающая на строго заданных алгоритмах.

Правильней говорить о «недекларированных возможностях» (НДВ) к вмешательству в рабочий процесс отдельных уровней защиты. НДВ могут быть везде. В процессоре, в контроллере, в сервере, в маршрутизаторе, коммутаторе и планшете. НДВ могут быть

в более высокоуровневом ПО, в операционных системах, прошивках оборудования, в ПО непосредственного управления техническими средствами.

В заключение можно отметить, что особенность задачи состоит в том, что технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля НДВ на каждом из уровней соответствующего технологического процесса. Отказы и повреждения технических и программных средств должны приводить к появлению сигналов на щитах управления (БПУ, РПУ и др.) и вызывать действия, направленные на обеспечение безопасности АЭС.

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Все указанные факторы в совокупности влияют на общую защищенность системы АСУ ТП и применяемые технические средства должны обеспечивать такое состояние подсистем и комплексов АСУ ТП АЭС, при котором риски нарушения технологического процесса из-за кибератак на АСУ ТП АЭС минимизированы

Список литературы

1. Путилин, В. Н. Задача обеспечения информационной безопасности атомных электростанций / В. Н. Путилин // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. – С. 82–83.

РАЗРАБОТКА ЗАЩИТНЫХ КОНСТРУКЦИЙ ДЛЯ ПОДАВЛЕНИЯ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИ

Г.А. Пухир[1], В.С. Колбун[1], И.А.К. Камил[2]
[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь*
[2]*Анбарский университет, Эр-Рамади, Ирак*

Для создания защитных конструкций, подавляющих утечку информации по каналам ПЭМИ, применяются экранирующие и радиопоглощающие материалы. Электромагнитное моделирование позволяет определить электрофизические свойства, толщину и форму элементов экранов и радиопоглотителей для достижения наибольшей эффективности [1]. На основе разработанных композиционных материалов [2, 3] предложены четырехслойные конструкции экранов и радиопоглотителей и определены параметры слоев для создания радиопоглотителей с коэффициентом отражения менее –10 дБ в диапазоне частот исследований 8–12 ГГц.

Установлено комплексное влияние электрофизических параметров и толщины отдельных слоев радиопоглотителя на характеристику коэффициента отражения и его частотную зависимость. Минимальная величина коэффициента отражения, полоса рабочих частот с коэффициентом отражения менее –10 дБ определяются комбинацией электрофизических и структурных параметров слоев, рассчитанных для данного частотного диапазона. Получена наименьшая величина коэффициента отражения для исследуемой области частот $К_{отр\ мин}$ = –37 дБ (на частоте 11,6 ГГц). Показано, что для четырехслойной конструкции радиопоглотителя общей толщиной 7,6 мм и величинах диэлектрической проницаемости радиопоглощающих слоев $\varepsilon'_1 = 3$; $\varepsilon'_2 = 9$; $\varepsilon'_3 = 30$, коэффициент отражения составляет менее –10 дБ в диапазоне частот 10,6–12,0 ГГц. Для расширения рабочей полосы частот толщина четырехслойной конструкции радиопоглотителя увеличивается до 14 мм, при этом коэффициент отражения составляет менее –10 дБ во всем диапазоне частот 8–12 ГГц. Общая эффективность экранирования конструкции составляет более 40 дБ во всем исследуемом диапазоне частот.

Список литературы

1. Насонова, Н. В. Закономерности формирования многослойных радиопоглощающих материалов / Н. В. Насонова, Т. А. Пулко, Г. А. Пухир // 14-ая Межд. научно-технической конференция: «Новые материалы и технологии: Порошковая металлургия, композиционные материалы, защитные покрытия, сварка»: материалы докладов, Минск, 9–11 сентября 2020 г. – Минск: Беларуская навука, 2020. – С. 357–363.

2. Использование жаростойкого сплава в качестве поглотителя ЭМИ микроволнового диапазона / А.Ф.Ильющенко [и др.] // Респ. межведомственный сборник научных трудов «Порошковая металлургия». – 2019. – Т. 42. – С. 27–35.

3. Электрофизические характеристики полимерных композиционных материалов для разработки радиопоглотителя СВЧ-диапазона / Г.А. Пухир [и др.] // Материалы 7-го Международного симпозиума «Пористые проницаемые материалы: технологии и изделия на их основе», Минск, 19–20 октября 2023 г. – Минск: Беларуская навука, 2023.– С. 252–261.

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ РЕШЕНИЙ: ТИПОВЫЕ ПОДХОДЫ КРУПНЫХ ВЕНДЕРОВ

В.А. Розина, Е.В. Бегляк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Вопросы безопасности являются основными препятствиями для широкого принятия облачных технологий. В данном докладе будут рассмотрены типовые подходы к безопасности облачных решений, а также механизмы обеспечения безопасности облачных инфраструктур и сервисов.

Защита памяти. Аппаратными средствами защиты являются: секционированный кэш (PC) и кэш с блокировкой по частям (PLC). В первом случае кэш динамически разбивается на защищенные области, которые могут быть специально сконфигурированы для конкретного приложения. Второй вариант предлагает изолировать только те строки кэша, которые содержат критические данные. Еще одним подходом является криптография. Одной из наиболее распространенных является Intel Advanced Encryption Standard (AES-NI), принципом действия которого заключается в аппаратной реализации некоторых подэтапов алгоритма AES.

Защита гипервизора. Защиты гипервизора от внедрения вредоносного кода включает в себя создание нескольких виртуальных машин клиента и их хранение в центральном хранилище. Также вендоры предлагают и базовые способы защиты, такие как системы мониторинга подозрительной активности:

– AWS CloudTrail;

– Azure Security Center;

– IBM Cloud Security Advisor.

Аутентификация и идентификация личности пользователей. Одна из проблем при использовании традиционных методов идентификации в облачной среде возникает, когда предприятие использует нескольких поставщиков облачных услуг. Это приводит к тому, что синхронизация данных о личности становится негибкой. Одним из подходов для решения данной проблемы является использование единой системы управления идентификацией и доступом (IAM). Некоторые крупные вендоры предлагают собственные решения IAM:

– Identity and Access Management от Amazon Web Services (AWS);

– IBM Cloud Identity and Access Management от IBM Cloud;

– Google Cloud Identity and Access Management от Google Cloud Platform (GCP).

Изоляция памяти. Изоляция памяти включает в себя использование техник, таких как Address Space Layout Randomization (ASLR) и CPU NX/XD, для предотвращения атак, основанных на переполнении буфера.

Изоляция устройств, сети. Изоляция устройств заключается в использовании механизмов виртуализации, таких как DMA-Remapping, позволяющих предотвратить несанкционированный доступ к физической памяти хостовой системы со стороны периферийных устройств с поддержкой DMA. Изоляция сети заключается в использовании виртуализированных сетевых контроллеров (vNIC) и межсетевых экранов, обеспечивающих контроль доступа и фильтрацию трафика между виртуальными машинами и внешней сетью,

Список литературы

1. Cloud Computing: Security Issues and Security Standards / S. Khan [et al.]. – 2024.

2. Coppolino, L. Cloud security: Emerging threats and current solutions / L. Coppolino, S. D'Antonio, G. Mazzeo // Computers & Electrical Engineering. – 2016/

АВТОМАТИЗАЦИЯ ИНСТРУМЕНТА NMAP ДЛЯ СКАНИРОВАНИЯ КОРПОРАТИВНОЙ СЕТИ С МЕЖСЕТЕВЫМ ЭКРАНОМ PFSENSE

Н.А. Рощупкин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

pfSense – это бесплатный межсетевой экран с открытым исходным кодом, основанный на операционной системе FreeBSD [1]. Он включает в себя пакеты с открытым исходным кодом для расширенных возможностей. Выбор межсетевого экрана pfSense обусловлен тем, что он является одним из самых популярных и свободно распространяемых межсетевых экранов. Это дает возможность детально изучать его исходный код, а также использовать его для построения обучающих стендов без необходимости приобретения лицензии.

Цель работы данной работы заключается в демонстрации применения инструмента Nmap для сканирования и тестирования безопасности корпоративной сети, а также в разработке автоматизированного скрипта для контроля сетевого периметра с использованием Nmap.

В результате достижения поставленной цели также был разработан образовательный стенд с возможностью активного мониторинга и моделирования атак на инфраструктуру корпоративной сети. Образовательный стенд состоит из зон DMZ и LAN. Эти зоны разделены межсетевым экраном pfSense, включающим в себя плагин Suricata [2], способный обнаруживать все попытки несанкционированного сканирования периметра (T1595 MITRE ATT&CK) [3] и отправлять журналы в систему SIEM, построенную на базе Opensearch Stack (Opensearch, Opensearch Dashboards, Logstash) [4]. Стенд развернут на базе платформы виртуализации VirtualBox. В зоне DMZ находится веб-сервер, работающий на основе дистрибутива Debian 4.19.181-1. В зоне LAN расположен хост с операционной системой Windows 10. Обе виртуальные машины демонстрируют базовые уязвимости, такие как Script Privilege Esalation, Remote File Inclusion, EthernalBlue, Weak Password, SQL Injection и другие, с целью дальнейшего использования стенда в образовательных целях.

Таким образом, внедрение разработанного образовательного стенда в учебный процесс на кафедре защиты информации будет способствовать развитию следующих навыков у учащихся:

1 Конфигурация межсетевого экрана pfSense с выделение демилитаризованной зоны.

2 Работа с системами мониторинга и журналирования событий информационной системы.

3 Тестирования и определение уязвимостей информационной системы с помощью автоматизированного инструмента Nmap на базе межсетевого экрана pfSense.

4 Устранение выявленных уязвимостей в информационной системе.

Список литературы

1. Межсетевой экран pfsense [Электронный ресурс]. – Режим доступа: https://www.pfsense.org/. – Дата доступа: 07.05.2024.

2. Система обнаружения и предотвращения вторжений Suricata [Электронный ресурс]. – Режим доступа: https://suricata.io/. – Дата доступа: 07.05.2024.

3. Техника активного сканирования матрица MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/techniques/T1595/. – Дата доступа: 07.05.2024.

4. Визулизатор логов Opensearch [Электронный ресурс]. – Режим доступа: https://opensearch.org/. – Дата доступа: 07.05.2024.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ ДЛЯ РАСТРОВЫХ ДОКУМЕНТОВ-КОНТЕЙНЕРОВ

М.Г. Савельева

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Современная цифровая эпоха внесла значительные изменения в процесс обработки и использования данных. Преднамеренное или непреднамеренное преобразование электронных текстовых документов может легко изменить их первоначальный вид. Одним из ключевых аспектов различных изменений и преобразований, вносимых в контейнерные текстовые документы, является растрирование текста. Однако это может быть использовано для добавления тайной информации к содержимому. Существующие математические модели не учитывают такую важную особенность, такие как растрирование электронных текстовых документов-контейнеров, что является основанием для разработки более детализированной математической модели стеганографической системы. В качестве основы для модификации с учетом растрирования векторных символов использована общая структура и ее компоненты [1]. Модель строится на основе следующих положениях. Произвольное тайное сообщение M можно скрыть в контейнере C при использовании ключей K, где $M \in \boldsymbol{M}$, $C \in \boldsymbol{C}$; $K \in \boldsymbol{K}$. Результатом такого преобразования будет стегоконтейнер S, $S \in \boldsymbol{S}$ [2]. Основным отличием математической модели стеганографической системы для растровых документов-контейнеров от известных моделей является разбиение ключей на ключи для генерации сообщения и ключи для методов внедрения сообщения и выбор массива пикселей для преобразования. Это позволит в полной мере использовать растрирование векторных символов для увеличения пропускной способности методов внедрения тайной информации. Это также увеличит стойкость к некоторым видам атак, в том числе и визуальных.

Список литературы

1. Шутько, Н. П. Моделирование стеганографической системы в задачах по охране авторских прав / Н. П. Шутько, Н. И. Листопад, П. П. Урбанович // Восьмая Междунар. научно-техн. конф. «Информационные технологии в промышленности» (ITI`2015): тезисы докладов. – Минск, ОИПИ НАН Беларуси, – 2015. – С. 30–31.

2. Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Part II Computer Science. – Wydawnictwo KUL, 2016. – P. 181–202.

УСТОЙЧИВОСТЬ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ К МЕТОДАМ СТЕГОАНАЛИЗА

М.Г. Савельева, И.А. Песецкий, Н.А. Песецкий

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Основной целью стеганоанализа является моделирование стеганографических систем и их исследование для получения качественных и количественных оценок надежности использования стеганопреобразования, а также построение методов выявления скрываемой в контейнере информации, ее модификации или разрушения [1].

Для анализа были выбраны следующие методы скрытия сообщения в растровых файлах: DCT и DWT. Дискретное косинусное преобразование (DCT) – это математическое преобразование, которое преобразует последовательность чисел в набор косинусоидальных компонент. Дискретное вейвлет-преобразование (DWT) – это метод анализа сигналов, который позволяет разложить сигнал на составляющие различных масштабов и частот. В стеганографии DWT часто используется для внедрения секретной информации в изображения. Этот метод позволяет скрыть данные в изображении таким образом, чтобы изменения были минимальны и незаметны для человеческого глаза. Для анализа были выбраны методы «Хи–квадрат» ($\chi 2$) атак и атака на основе корреляционного анализа (Correlation Analysis Attack), которые позволят узнать вероятность того, что в растровом изображении есть скрытое сообщение [2].

После проведенного исследования можно сделать вывод, что для рассмотренных методов атака $\chi 2$ неспособна полностью обнаружить сообщение и его реальный размер, однако предполагаемый размер сообщения возрастает вместе с реальным. То есть чем больше внедренное сообщение, тем больше вероятность его обнаружения с помощью данной атаки. Тем не менее, несмотря на рост объема данных, способность $\chi 2$ атаки к обнаружению скрытых сообщений остается менее эффективной по сравнению с CAA-атаками. В случае малого и большого объема скрытой информации способность корреляционных атак обнаруживать скрытые сообщения ограничена. Однако при достаточном объеме внедренной информации, который можно назвать «оптимальным», эффективность атаки достигает максимума. Это свидетельствует о сбалансированной комбинации между статистическими аномалиями и объемом информации, что делает обнаружение сообщения сложным. При слишком малом и слишком большом объеме внедренной информации эффективность данной атаки снижается.

Исследование подтверждает, что метод DWT обладает более высокой устойчивостью и незаметностью при скрытии сообщений в растровых изображениях по сравнению с DCT. При этом атака на основе корреляционного анализа является наиболее эффективным методом для обнаружения скрытых сообщений в таких изображениях.

Список литературы

1. Исследование устойчивости стеганографии в изображениях / Е. Г. Жиляков [и др.] // Экономика. Информатика. – 2014. – Т. 29, № 1-1 (172). – С. 168–174.

2. Разинков, Е. В. Стойкость стеганографических систем / Е. В. Разинков, Р. Х. Латыпов / Ученые записки Казан. гос. ун-та. – 2009. –Т. 151, № 2.

СОЗДАНИЕ УЧЕБНЫХ ВИДЕОМАТЕРИАЛОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

И.М. Салей, А.Ю. Богачёва

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

С появлением ряда образовательных инициатив, требующих создания современного образовательного материала, включая видеолекции и практикумы, создание видеоконтента с использованием нейронных сетей стало активно развиваться. Сейчас многие страны внедряют государственные программы по цифровизации образования и созданию современного учебного контента. Примерами таких программ могут служить «Цифровая школа» в России, «Образование 2030» в Канаде, «Единство цифрового образования» в США, «Digital India» в Индии, «e-Estonia» в Эстонии и «Smart Education 4.0» в Южной Корее. В Беларуси, также принята государственная программа «Цифровое развитие Беларуси» на период с 2021 по 2025 гг. В рамках этой программы разрабатывается проект «Электронное образование» [1].

Работа направлена на создание образовательного контента с использованием нейронных сетей. Были исследованы различные методы генерации текста и видео, с целью создания доступных и понятных видеолекций для использования в университетах.

Создание видеолекций без использования нейронных сетей может вызвать ряд проблем, включая отсутствие опыта, необходимость подготовки материалов и проблемы с коммуникацией. Для решения этих проблем были использованы системы на основе нейронных сетей, такие как Content Authenticity Initiative (CAI) от Adobe, MOOCshop от Stanford University, IBM Watson Studio, VideoKen и Vyond (ранее GoAnimate).

Для генерации текста был выбран чат-бот ChatGPT [2], который способен анализировать запросы пользователей и генерировать тексты на различные темы. Для создания «говорящих аватаров» использовался сервис D-ID [3], который позволяет создавать аватаров, способных озвучивать текст выбранным голосом. Процесс создания видеолекции состоял из трех этапов: генерация текста с помощью ChatGPT, озвучивание текста аватаром с помощью D-ID и объединение озвученного текста с готовой презентацией.

Разработанный метод может быть использован в образовательных учреждениях для создания видеоконтента, однако он не может полностью заменить прямое взаимодействие с преподавателем. Рекомендуется использовать его в сочетании с другими формами обучения.

Список литературы

1. Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс]. – Режим доступа: https://www.mpt.gov.by/ru/gosudarstvennayaprogramma-cifrovoe-razvitie-belarusi-na-2021-2025-gody. – Дата доступа: 29.04.2024.

2. Introducing ChatGPT [Электронный ресурс]. – Режим доступа: https://openai.com/blog/chatgpt. – Дата доступа: 29.04.2024.

3. Digital People, Text-to-Video [Электронный ресурс]. – Режим доступа: https://d-id.com. – Дата доступа: 29.04.2024.

МНОГОФУНКЦИОНАЛЬНАЯ СРЕДА ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ СПРАВОЧНИКОМ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ БЕЛОРУССКОЙ АЭС

С.М. Сацук, С.В. Дробот, В.Н. Русакович

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Информационный справочник показателей безопасной эксплуатации Белорусской АЭС и многофункциональная среда (МФС) для управления им созданы в целях поддержки принятия решений на основе дифференцированного подхода при организации надзора за обеспечением ядерной и радиационной безопасности Белорусской АЭС. Работа выполнена в рамках Государственной программы «Наукоемкие технологии и техника» на 2021–2025 гг.

Основное назначение МФС – управление информационным справочником показателей безопасной эксплуатации Белорусской АЭС и обеспечения пользователя информационного справочника интерфейсом и инструментарием для манипулирования данными и их визуализации.

Цель создания МФС – предоставление инструмента сотрудникам Госатомнадзора для управления информационным справочником при организации надзора за обеспечением ядерной и радиационной безопасности АЭС с использованием дифференцированного подхода [1].

МФС обеспечивает автоматизацию следующих процессов: ввода данных и документов; обработки информации; графического представления информации; вывода данных в файл с последующим выводом на печать средствами офисных приложений.

МФС представляет собой Web-приложение, состоящее из серверной и клиентской части реализованное на скриптовом языке JavaScript с использованием программной платформы Node.js для создания серверной части приложения.

Подсистема управления программными сущностями, которая реализует основные функции по управлению информационным справочником состоит из пяти компонентов:

– компонент 1 «Энергоблок 1»;
– компонент 2 «Энергоблок 2»;
– компонент 3 «Анализ»;
– компонент 4 «Документы»;
– компонент 5 «Конструктор отчетов».

Общий алгоритм работы МФС запускается после ввода в адресной строке браузера URL-адреса и номера порта сервера приложения. Открывается страница авторизации приложения и после ввода логина и пароля происходит авторизация в приложении и открывается главная страница. Работа с каждым из указанных компонентов осуществляется в соответствии с разработанным для него алгоритмом. Завершение работы с приложением осуществляется после нажатия на кнопку «Выход» на главной странице.

Список литературы

1. Стратегия Департамента по ядерной и радиационной безопасности Министерства по чрезвычайным ситуациям Республики Беларусь в области обеспечения ядерной и радиационной безопасности на 2021–2025 годы. [Электронный ресурс]. – Режим доступа: https://gosatomnadzor.mchs.gov.by/o-gosatomnadzore/reguliruyushchaya-strategiya-gosatomnadzora/. – Дата доступа: 03.05.2024.

ИСПОЛЬЗОВАНИЕ КАМЕРТОНА ОПЕРАТОРОМ РАДИОТЕХНИЧЕСКОЙ РАЗВЕДКИ

А.И. Серый

Учреждение образования «Брестский государственный университет имени А. С. Пушкина», Брест, Беларусь

Одной из важнейших характеристик сигнала, принимаемого средствами радиотехнической разведки (РТР), является период следования импульсов (ПСИ). Если отдельный импульс электромагнитного излучения, преобразуемый соответствующей аппаратурой в звуковой сигнал, воспринимается на слух, как правило, как щелчок, то группа импульсов достаточной длительности с достаточно стабильным периодом следования уже воспринимается на слух как вполне музыкальный звук, соответствующий определенной ноте (если оператор обладает так называемым абсолютным музыкальным слухом, который позволяет быстро и с хорошей точностью определить ноту воспринимаемого на слух звука). Этот факт находит простое теоретическое объяснение: частота звука, выраженная в герцах, находится путем деления единицы на выраженное в секундах значение ПСИ (хотя нередко указанный период принято для удобства выражать в микросекундах). После преобразования ПСИ в частоту остается по справочным данным определить, к какому тону равномерно-темперированного строя наиболее близок слышимый звук. При достаточно заметном разбросе значений периода следования импульсов соответствующее звуковое сопровождение, выдаваемое аппаратурой, напоминает, скорее, шум, нежели звук определенного тона. Если помимо основного значения ПСИ через определенное количество импульсов регулярно повторяется иное значение паузы между ними, то тогда воспринимаемый звук может быть слышен на фоне более низкого (соответствующего частоте следования упомянутого иного значения паузы).

Опыт работы на подобных установках (с соответствующим программным обеспечением) показал, что возможны ситуации, когда конкретное значение ПСИ не выводилось на экран либо отличалось от того, которое должно соответствовать слышимому тону, вдвое. Вопрос о том, насколько важной может оказаться такая ситуация в мирное и военное время, остается открытым, но поскольку поиск операторов РТР с абсолютным слухом может оказаться непростой задачей, можно дополнительно оснащать соответствующую аппаратуру электронным камертоном (не классическим вилочным, так как он для достижения обсуждаемой цели – точного определения ПСИ – не годится). Такие камертоны, способные мгновенно определять ноту воспринимаемого звука, в настоящее время широко используются на практике музыкантами, но для РТР такой камертон можно модифицировать, чтобы он вместо выдачи сведений о ноте сразу выдавал ПСИ. Такой камертон может предоставить дополнительный способ определения ПСИ в тех случаях, если другие используемые способы, не сработают должным образом.

Публикация дополняет работы автора [1] по вопросам использования акустических и электромагнитных сигналов, в том числе в технических средствах и методах защиты информации.

Литература

1. Серый, А. И. Об изучении акустических и электромагнитных волн в дисциплинах физического профиля / А. И. Серый // Современные научные проблемы и вопросы преподавания теоретической и математической физики, физики конденсированных сред и астрономии: сб. материалов VIII Республ. научн.-практ. конф., Брест, 21 октября 2021 г. – Брест : БрГУ, 2021. – С. 55.

ПРЯМЫЕ И ОБРАТНЫЕ ФИЗИЧЕСКИЕ ЭФФЕКТЫ В ТЕХНИЧЕСКИХ СРЕДСТВАХ И МЕТОДАХ ЗАЩИТЫ ИНФОРМАЦИИ

А.И. Серый

Учреждение образования «Брестский государственный университет имени А. С. Пушкина», Брест, Беларусь

Учебные программы дисциплины «Технические средства и методы защиты информации» [1], изучаемой студентами некоторых физико-математических и технических специальностей (в частности, «Компьютерная физика») широко опираются на сведения из различных разделов физики. В разной степени это касается, прежде всего, устройств приема, передачи, хранения и обработки информации, поскольку при анализе оптимальной работы таких устройств могут играть важную роль сведения из различных разделов физики. Поскольку информационные сигналы могут иметь электромагнитную или акустическую природу, то изучение устройств прямого или обратного преобразования таких сигналов уже автоматически связано с механикой и электродинамикой. Проблемы, относящиеся к перегреву и необходимости охлаждения, связаны с термодинамикой.

В связи с этим представляет интерес сведения о физических эффектах, играющих необходимую или негативную роль при работе различных устройств указанных типов. Физические эффекты могут быть прямыми и обратными (хотя не для всякого эффекта можно выделить ярко выраженный обратный). В качестве примеров можно назвать прямой и обратный пьезоэлектрический, пьезомагнитный и магнитострикцию, тепловое расширение и нагрев при деформации. Вопрос о широком применении ряда эффектов (например, термомеханический и механокалорический для сверхтекучего гелия) в устройствах указанных типов остается открытым.

Каждый физический эффект в рамках дисциплины «Технические средства и методы защиты информации» можно охарактеризовать по следующим пунктам. 1. Наличие обратного эффекта. 2. Раздел физики. 3. Теоретическое объяснение эффекта (прямого и обратного, если последний существует). 4. Исторически первые и современные примеры использования обоих эффектов в технических средствах и методах защиты информации. 5. Исторически первые и современные примеры борьбы с данными эффектами в случаях, когда их роль в технических средствах и методах защиты информации носит негативный характер.

Публикация дополняет другие публикации автора [2, 3] по вопросам методики преподавания дисциплины «Технические средства и методы защиты информации».

Список литературы

1. Технические средства и методы защиты информации / А. П. Зайцев [и др.]. – М.: Горячая линия–Телеком, 2012. – 616 с.

2. Серый, А. И. К вопросу о методике преподавания темы «Технические каналы утечки информации» / А. И. Серый // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 года. – Минск: БГУИР, 2022. – С. 93–94.

3. Серый, А. И. О связи дисциплины «Технические средства и методы защиты информации» с разделами физики / А. И. Серый // Актуальные вопросы общей и теоретической физики, физики конденсированных сред и астрофизики: сб. материалов регион. науч.-практ. семинара, посвящ. 70-летию со дня рождения А. Ф. Ревинского, Брест, 12 апреля 2022 г. – Брест : БрГУ, 2022. – С. 111–112.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

С.П. Способ, К.Е. Макаренко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Что такое информационная безопасность? Определение дано в Концепции Национальной Безопасности Республики Беларусь, утвержденной Указом Президента РБ от 9 ноября 2010 г. № 575. в соответствии с которой под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Данное понятие является основным для определения компетенции государственных органов по обеспечению информационной безопасности.

Правовое обеспечение информационной безопасности базируется на:

– Конституции Республики Беларусь от 15 марта 1994 г. (с изменениями и дополнениями от 24.11.1996 и 17.10.2004), в соответствии со статьей 34 которой, гражданам гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды;

– Гражданском кодексе Республики Беларусь, Кодексе Республики Беларусь об административных правонарушениях, Уголовном кодексе Республики Беларусь, Трудовом кодексе Республики Беларусь, Налоговом кодексе Республики Беларусь;

– Законе Республики Беларусь от 21.06.2008 № 418-З «О регистре населения»;

– Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

– Законе Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения»;

– Законе Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

– Указах Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», от 01 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь», от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»; постановлениях Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192», от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»;

– Приказах (от 02.08.2010 № 60, от 16.11.2010 № 82, от 17.12.2010 № 92) и постановлениях (от19.02.2015 №6/8) Оперативно-аналитического центра при Президенте Республики Беларусь.

В Республике Беларусь нужно принять документ, комплексно регулирующий сферу информационных отношений и государственную политику в сфере обеспечения информационной безопасности [1, 2].

Список литературы

1. Закон Республики Беларусь от 10 ноября 2008г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/laws-rb/455-z.pdf. – Дата доступа: 07.05.2024.

2. Конституция Республики Беларусь Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=v19402875. – Дата доступа: 07.05.2024.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ И ИХ ОТПРАВИТЕЛЯ НА ОСНОВЕ АЛГОРИТМА ГОСТ 28147-89

А.М. Тимофеев[1], А.А. Корчинский[2], Д.А. Телипко[2]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

Одной из основных задач в сфере информационной безопасности является аутентификация пользовательских данных и их отправителя [1]. Для решения этой задачи, в частности, используют криптографические методы и средства, основанные на применении электронных цифровых подписей (ЭЦП) [1, 2]. Однако известные алгоритмы ЭЦП требуют достаточно больших вычислительных ресурсов легитимных пользователей за счет выполнения таких операций, как, например, генерация больших простых чисел, выселение корней квадратных по простому и по составному модулям, возведение в степень больших чисел в большую степень и др. В этой связи целесообразно создавать криптосистемы, которые позволяют решать задачи аутентификации пользовательских данных и их отправителя и, вместе с тем, по сравнению с существующими криптосистемами, более простые в реализации, что являлось целью данной работы. В качестве объекта исследования выбран алгоритм ГОСТ 28147-89. Создана компьютерная программа, которая осуществляет криптографические операции, свойственные для криптосистем симметричного типа. Предложена криптосистема, позволяющая выполнять аутентификацию пользовательских данных, а также проверять подлинность их отправителя на основе симметричного блочного алгоритма ГОСТ 28147-89, которая упрощает известные алгоритмы ЭЦП. Применительно к предложенной криптосистеме выполнены исследования по оценке криптостойкости и среднего времени, необходимого для формирования подписи и ее верификации для легитимных пользователей.

Список литературы

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование / Л. К. Бабенко. – М., Издательство Юрайт, 2020.

2. Милославская, Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях / Н. Г. Милославская. – М., Горячая линия-Телеком, 2021.

ИССЛЕДОВАНИЕ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ СИММЕТРИЧНОГО ТИПА

А.М. Тимофеев[1], А.Н. Шишпаренок[2], В.Е. Юруть[2]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*
[2]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

При разработке криптографических систем связи симметричного типа, обеспечивающих конфиденциальность передаваемой информации, одной из наиболее важных задач является оценка криптостойкости таких систем [1]. В этой связи целесообразно создавать программное обеспечение для оценки криптостойкости криптографических систем связи симметричного типа, что являлось целью данной работы. Создана компьютерная программа, которая реализует криптографические алгоритмы симметричного типа и процедуры их криптоанализа. Компьютерная программа написана на языке программирования Rust с использованием библиотек bitvec, itertools, tokio, tracing, thiserror и rayon [2, 3]. Пользовательская часть программы выполнена в виде набора подпрограмм, предусматривающих возможность выбора исследуемого алгоритма, режима его функционирования и экстраполяции полученных результатов для оценки достаточно высокой криптостойкости (10 и более лет). Выполнены исследования по оценке криптостойкости алгоритмов симметричного типа.

Список литературы

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование / Л. К. Бабенко. – М., Издательство Юрайт, 2020.

2. Blandy, J. Programming Rust / J. Blandy. – Sebastopol, Ca: O'Reilly Media, 2021.

3. Klabnik, S. The Rust Programming Language / S. Klabnik. – San Francisco, Starch Press, 2021.

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ

М.В. Тимошенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Чем глубже цифровые технологии проникают в нашу жизнь, тем важнее становится защита огромных объемов конфиденциальных данных. В связи с этим появляется чрезвычайная актуальность изучения криптографии, в том числе потому что она представляет собой захватывающее и важное поле, которое объединяет математику, информатику и кибербезопасность. В виртуальном пространстве криптография находит широкое применение: это неотъемлемая часть нашей цифровой жизни, в которой нам приходится постоянно заботиться о безопасности личных данных. Криптография использует некоторые низкоуровневые криптографические алгоритмы для достижения одной или нескольких из этих целей информационной безопасности. Среди этих инструментов – алгоритмы шифрования, алгоритмы цифровой подписи, алгоритмы хэширования и другие функции. Алгоритм шифрования – это процедура, которая преобразует сообщение в формате неформатированного текста в зашифрованный текст. ЭЦП (электронная цифровая подпись) – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа,

служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства. Криптографическая хэш-функция – это инструмент для преобразования произвольных данных в «отпечаток» фиксированной длины. Хэш-функции создаются таким образом, чтобы было сложно найти два различных набора входных данных, дающих один и тот же отпечаток, и чтобы было сложно найти сообщение, отпечаток которого совпадает с фиксированным значением [1].

Для реализации криптографических алгоритмов была разработана программа CryptoEtalon на фреймворке Qt [2], использующая Bee2 [3] – криптографическая библиотека, реализующая стандартизированные в Республике Беларусь криптографические алгоритмы и протоколы. CryptoEtalon – это средство проверки стандартов защиты информации, позволяющее пользователю на основе полученных данных из программы тестировать и оценивать криптографические алгоритмы на их стойкость и эффективность, оценивать совместимость между различными системами и устройствами, использующими криптографию, а так же может служить для обучающих целей: ознакомления с принципами криптографии, проверки своих знаний, реализующая следующие функции [4]:

– криптографические алгоритмы на основе sponge-функции в соответствии с СТБ 34.101.77-2020.

– алгоритмы шифрования данных и контроля целостности в соответствии с СТБ 34.101.31-2020;

– алгоритмы выработки электронной цифровой подписи в соответствии с СТБ 34.101.45-2013;

– алгоритмы генерация псевдослучайных чисел в соответствии с СТБ 34.101.47-2017;

– алгоритмы разделение секрета в соответствии с СТБ 34.101.60-2014;

– формирование общего ключа на основе эллиптических кривых в соответствии с СТБ 34.101.66-2014.

Список литературы

1. Что такое криптография? [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/what-is/cryptography/. – Дата доступа: 18.04.2024

2. Ot Group [Электронный ресурс]. – Режим доступа: https://www.qt.io/ – Дата доступа: 18.04.2024

3. Библиотека Bee2 [Электронный ресурс]. – Режим доступа: https://apmi.bsu.by/blog/cryptology/bee2.html. – Дата доступа: 18.04.2024

4. Национальный фонд технических нормативных правовых актов [Электронный ресурс]. – Режим доступа: https://tnpa.by/#!/SimpleSearch/search_value=криптография/tab=TabOne/page=/status=/state=/num_of_records= – Дата доступа: 18.04.2024.

ИСПОЛЬЗОВАНИЕ МАШИННОГО ЗРЕНИЯ ДЛЯ ОЦЕНКИ 3D-ПОЗЫ ЧЕЛОВЕКА

А.Ф. Типун, О.А. Хацкевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Широкое использование машинного зрения позволяет резко повысить безопасность людей, объектов и активов. Трехмерное представление фигуры предоставляет дополнительную информацию о глубине по сравнению с двухмерным представлением. Оценка позы человека 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.

Трехмерная оценка позы человека сталкивается с дополнительными проблемами, включая отсутствие реальных наборов трехмерных данных, неоднозначность глубины, большой спрос на обширную информацию о позе (например, сдвиги и вращения), большое пространство состояний поиска для каждого сустава. Как правило, структура человеческого тела очень сложна, и на практике приходится использовать разные модели. 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.

Использование представленной технологии позволит улучшить «диалог» между «машиной» и человеком в его естественной среде обитания. И без того автоматизированные процессы можно полностью освободить от участия человека, обезопасить их.

ОЦЕНКА ИЗМЕНЕНИЯ ВРЕМЕНИ ЗАДЕРЖКИ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ ПОД ДЕЙСТВИЕМ РАДИОПОМЕХ

Н.А. Титович, З.Н. Мурашкина

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Одним из наиболее эффективных путей обеспечения ЭМС является учет при проектировании сравнительной информации о восприимчивости каждой интегральной микросхемы (ИМС). Рациональная защита наиболее уязвимых цепей за счет выбора менее восприимчивых логических элементов (ЛЭ) позволяет значительно снизить затраты на обеспечение ЭМС на последующих этапах разработки.

При исследовании восприимчивости простых ИМС по критерию функционального сбоя точную оценку изменения времени задержки ЛЭ сделать трудно. Повысить точность позволяет метод «кольцевого генератора» (КГ). Если нечетное число n логических инверторов соединить последовательно в кольцевую схему, то за счет задержки распространения сигнала в элементах возникает положительная обратная связь и схема начинает работать, как автогенератор. По частоте генерации f_0 можно определить среднее время задержки распространения ЛЭ $t_{з\,р\,ср} = 1/2nf_0$. При воздействии ЭМП на все ЛЭ одновременно изменяется их время задержки распространения, а соответственно и частота генерации КГ. По начальному f_0 и новому f_1 значению частоты можно определить среднее значение изменения времени задержки распространения $\Delta t_{з\,р\,ср} = (1/f_0 - 1/f_1)/2n$. Наиболее точную оценку изменения $\Delta t_{з\,р\,ср}$ позволяет получить действие ЭМП по цепи питания ЛЭ.

С целью получения сравнительной информации о восприимчивости были проведены исследования ТТЛШ и КМОП ЛЭ И-НЕ, ИЛИ-НЕ, НЕ к воздействию ЭМП, превышающих их граничную рабочую частоту. В соответствии со стандартом IEC 62132 применялись два способа подачи ВЧ помехи: ТЕМ-камеры и прямого введения мощности. Сравнение способов подачи ЭМП показало, что воздействие на перпендикулярно расположенную рамку площадью 0,002 м^2 электромагнитного поля с напряженностью 100–150 В/м эквивалентно наведенному ВЧ напряжению помехи соответственно 4–6 В. Ниже приводится сравнительная оценка восприимчивости различных ЛЭ при воздействии помех и полей с частотой 200 МГц.

Недопустимые изменения времени задержки распространения на 1–2 нс у ЛЭ 2И-НЕ серий 155, 531, 555, 7400, 4011 происходят при уровнях ВЧ помех в 2–4 В (50–100 В/м), что в несколько раз меньших тех, которые вызывают критические

отклонения от нормы уровней логических нуля и единицы. В то же время у ЛЭ серии 1533 и 1554 при таких уровнях ВЧ ЭМП изменения $t_{з\,р\,ср}$ почти не происходит и уровни нуля и единицы более критичны к действию помехи. Очевидно при разработке фрагментов быстродействующих схем для уменьшения вероятности сбоев по причине «гонок сигналов» лучше использовать ЛЭ серии 1533. Изменения $t_{з\,р\,ср}$ ЛЭ 2ИЛИ-НЕ при таких же уровнях помех также значительно ниже, чем у 2И-НЕ. У микросхемы 1533ЛЕ1 наблюдалось его уменьшение до –2 нс. При увеличении напряженности поля до 100–200 В/м (4-8 В) Δt ЛЭ 2И-НЕ возрастает на 6 и более наносекунд, а у 2ИЛИ-НЕ серий 4001 и 4011 оно резко уменьшается на 6–8 нс. Описанные выше зависимости изменения $t_{з\,р\,ср}$ имеют место как для случая включения трех элементов в схему КГ, так и для $n = 5$ и 7.

Для КМОП микросхем 4001, 4011 и 4069 исследования выполнены также и для различных напряжений их питания – 5, 10 и 15 В. Для повышения помехоустойчивости КМОП схем необходимо увеличивать напряжение питания до 10–15 В. В этом случае под действием ЭМП $t_{з\,р\,ср}$ изменяется незначительно (возрастает на 0,5–1 нс).

МОНОДИСПЕРСНЫЕ ШАРОВЫЕ ПОЛИМЕРНЫЕ ГРАНУЛЫ С ПРОВОДЯЩИМ СЛОЕМ МЕДИ ДЛЯ ЭКРАНИРОВАНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

А.К. Тучковский, И.А. Врублевский

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время в качестве экранов электромагнитного излучения используются металлические листы, фольга или фольгированные пленки, металлизированные ткани и токопроводящие краски. Проволочные сетки, металлизированные ткани применяются для ослабления электромагнитного излучения в широком диапазоне частот, от десятков МГц до десятков ГГц с затуханием электромагнитного поля до 70 дБ. Основным недостатком таких способов является большой вес, высокая стоимость и трудности с возможностью модификации конструкции.

В настоящей работе предложено для экранирования электромагнитного излучения использовать полимерные микрогранулы с проводящим слоем меди. Применение токопроводящего слоя на основе меди дает ряд преимуществ. Проводящие гранулы могут быть хорошо распределены в матрице из силикона, что позволяет создавать между основой и экранирующей поверхностью большое количество низкорезистивных соединений. Перед осаждением меди на полимерные гранулы первоначально проводилась обработка поверхности в изопропиловом спирте с последующей сушкой путем нагревания в вакууме. Затем проводилась активация поверхности полимерных гранул в 5 % водном растворе $AgNO_3$ в течение 10 мин. После промывки водой и сушки полимерных гранул медь осаждалась из раствора на основе солей меди. Для улучшения антикоррозионных свойств поверхность полимерных гранул со слоем меди электрохимически покрывалась слоем никеля из раствора солей никеля.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В КОНТЕКСТЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Н.А. Урбан

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Криптография является одной из основ информационной безопасности. Выработка хэш-значения используется для проверки целостности и подлинности информации, а также в других криптографических алгоритмах [1]. Шифрование позволяет передавать данные в безопасном виде. В симметричных криптосистемах для зашифрования и расшифрования используется один и тот же секретный ключ. Без доступа к ключу невозможно расшифровать данные [2]. В асимметричных криптосистемах для зашифрования используется открытый ключ, а для расшифрования – закрытый. По сравнению с симметричным шифрованием такой алгоритм является более медленным, однако он лишен необходимости передавать секретный ключ. Для выработки электронной цифровой подписи (ЭЦП) используется секретный ключ, а для ее проверки – открытый. ЭЦП позволяет обеспечить контроль целостности и подлинности передаваемых данных [3].

В рамках дипломного проектирования была разработана программа, позволяющая вычислять хэш-значения от файла, вырабатывать и проверять значения ЭЦП файла. Программа обладает возможностью формирования и проверки файла контроля целостности, который можно использоваться для реализации требований к защите объектов (ЗО), самотестированию (СТ), обновлению программ (ОП) СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности». Она может быть использована в системах электронного документооборота для проверки целостности и подлинности передаваемых файлов различными организациями как при внешнем, так и при внутреннем обмене информацией, а также в обучающих целях для понимания работы криптографических алгоритмов.

При разработке программы использовалась библиотека Bee2 [4]. Bee2 – это криптографическая библиотека, распространяющаяся бесплатно под лицензией Apache 2.0 [5]. С помощью этой библиотеки в программе были реализованы функции выработки хэш-значения, формирование и проверка файла контроля целостности информации в соответствии с СТБ 34.101.31-2020, выработки значения электронной цифровой подписи в соответствии с СТБ 34.101.45-2013.

Разработанная программа позволяет реализовать требования безопасности к средствам криптографической защиты информации, в соответствие с СТБ 34.101.27-2022 и впоследствии может быть сертифицирована как средство криптографической защиты информации.

Список литературы

1. Что такое криптография? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptography/. – Дата доступа: 17.04.2024

2. СТБ 34.101.27-2022 Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности.

3. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи», 07.05.2021, № 113-З // Национальный правовой Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/. – Дата доступа: 17.04.2024

4. Библиотека Bee2 [Электронный ресурс]. – Режим доступа: https://apmi.bsu.by/blog/cryptology/bee2.html. – Дата доступа: 17.04.2024

5. Agievich/bee2: A cryptographic library [Электронный ресурс]. – Режим доступа: https://github.com/agievich/bee2/. – Дата доступа: 17.04.2024

ВОЗМОЖНОСТИ КИБЕРПОДРАЗДЕЛЕНИЙ СТРАН НАТО ПО ПРОВЕДЕНИЮ СПЕЦИАЛЬНЫХ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА ДЕЗОРГАНИЗАЦИЮ УПРАВЛЕНИЯ

Л.Л. Утин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В последние годы вопросы проблема обеспечения информационной безопасности государства особенно актуальна, что обусловлено недружественной политикой зарубежных стран в отношении Республики Беларусь. При этом отмечается возрастающее количество попыток специализированных группировок дестабилизировать все сферы развития общества путем несанкционированного вмешательства в информационные сети и системы различного назначения.

Учитывая непрерывное развитие методов преодоления систем защиты информационных сетей следует отметить, что гарантированное обеспечение информационной безопасности в современных условиях затруднено. Это обусловлено в первую очередь тем, что применяемые при построении информационных сетей программные и аппаратные средства могут иметь встроенные уязвимости, так как в большинстве случаев создаются на базе импортных комплектующих, способы активации которых и последствия подробно рассмотрены в [1].

Впервые уязвимости информационных сетей использовали вооруженные силы стран НАТО в ходе проведения операции в Югославии в 1999 году с целью отключения телефонной связи [2]. Эффективность проведения странами НАТО мероприятий по дезорганизации управления в ходе информационного конфликта в Югославии, а далее в 2003 году в Ираке [3] способствовали увеличению затрат на разработку новых форм и методов борьбы в информационном пространстве.

В докладе рассматриваются возможности киберподразделений отдельных стран НАТО по проведению специальных операций, направленных на дезорганизацию управления и предлагаются основные направления по совершенствованию системы защиты Вооруженных Сил.

Список литературы

1. Утин, Л. Л. Анализ возможных способов активизации компьютерных закладок / Л. Л. Утин, Е. Л. Остромухов // Управление защитой информации. – 2003. – Т. 7. – № 4. – С. 423–427.

2. Белозеров, В. Киберкомандование вооруженных сил Франции / В. Белозеров // Зарубежное военное обозрение. – 2022. – №9

3. Литвинов, Е. В. Опыт применения информационных технологий вооруженными силами стран НАТО в военных конфликтах / Е. В. Литвинов // Военная мысль. – 2024. – № 1.

ЭЛЕКТРОХИМИЧЕСКОЕ ОСАЖДЕНИЕ БУФЕРНОГО СЛОЯ НА ОСНОВЕ ОКСИСУЛЬФИДОВ ЦИНКА-ОЛОВА ДЛЯ ФОТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ

Е.А. Уткина[1], А.И. Воробьева[1], М.В. Меледина[1], А.А. Ходин[2]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2] *ГНПО «Оптика, оптоэлектроника и лазерная техника» НАНБ, Минск, Беларусь*

Для создания современных фотоэлектрических преобразователей исследуются полупроводниковые материалы на основе оксисульфидов цинка-олова для использования в качестве бескадмиевого буферного слоя [1, 2].

В данной работе для осаждения оксисульфида олова $Zn(O,S)_x$ исследован потенциостатический режим электрохимического осаждения при оптимальном напряжении 1,2 В, установленном на основе полученных хроновольтамперограмм, в электролите состава: 33 мМ $SnCl_2$ и 91 мМ $Na_2S_2O_3{\cdot}5H_2O$ в дистиллированной воде при установленной оптимальной температуре 35°C, pH = 2,5:

$S_2O_3^{2-} \rightarrow S^{2-} + SO_3^{2-}$

$Sn^{2+} + S^{2-} + O^{2-} \rightarrow SnS + SnO \rightarrow Sn(S,O)_2$

При пропускании воздуха через электролит во время осаждения, а также при участии кислорода тиосульфата натрия происходит формирование SnO_2, и при осаждении SnS происходит преобразование в $Sn(S,O)_2$.

Для осаждения буферного слоя оксида цинка ZnO использовался электролит следующего состава: 1 мМ $Zn(NO_3)_2{\cdot}6H_2O$ и 0,1 М KCl при значении pH = 5,5. Дополнительно для формирования пленки на основе оксисульфида цинка использовали раствор натрия серноватистокислого в качестве источника серы. Разложение (восстановление) тиосульфат-ионов ($S_2O_3^{2-}$) на катоде в кислой среде происходит по предлагаемой реакции:

$S_2O_3^{2-} + 4H^+ + 6e = 2H_2O + S^{2-} + O^{2-} + S.$

Концентрация тиосульфата поддерживалась в электролите на низком уровне 0.02 М $Na_2S_2O_3{\cdot}5H_2O$ для сохранения прозрачности раствора. В диапазоне катодных потенциалов 1,4 – 1,5В плотность тока увеличивалась быстрее, что указывает на восстановление Zn^{2+} и постепенное образование $Zn(O,S)_2$ с высоким содержанием серы на катоде в соответствии с реакцией:

$2Zn^{2+} + S^{2-} + O^{2-} = ZnS + ZnO \rightarrow Zn(S,O)_2$

Микроморфология полученных пленок оксисульфида олова характеризуется наличием развитых квази-2D наноструктур преимущественно в виде нанопластин. Результаты рамановского анализа структур указывают на вероятное присутствие фаз Zn(O,S) и ZnS со слабо выраженными полосами при 685 и 738 $см^{-1}$. Широкие полосы указывают, в частности, на существенное разупорядочение структуры.

Полученные результаты важны как для последующих исследований процессов низкотемпературного интеркаляционного легирования полупроводников, так и при разработке новых фото- и хемочувствительных элементов.

Список литературы

1. Electrochemical deposition and characterisation of ZnOS thin films for photovoltaic and photocatalysis applications / O. K. Echendu [et al.] // J. of Alloys and Comp. – 2018. – Vol. 769. – P. 201–209.

2. $Sn(O,S)_2$ thin films by chemical bath deposition for Cd-free CIGS thin film solar cells / J. Kim [et al.] // 2013 IEEE 39th Photovoltaic Specialists Conference (PVSC). – 2013. – P. 1131–1135.

КРИТЕРИИ ДЛЯ ВЫБОРА И РАЗРАБОТКИ СРЕДСТВ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ

П.А. Фильченков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Критериями для выбора и разработки средств аудита безопасности информационных систем (ИС) учреждений здравоохранения (УЗ) являются:

– требования к обеспечению информационной безопасности в УЗ, которые фигурируют в следующих локальных документах УЗ: политика информационной безопасности, регламенты, инструкции и приказы по вопросам обеспечения информационной безопасности ИС;

– состав аппаратного и программного обеспечения ИС УЗ;

– топология ИС.

С учетом перечисленных критериев работникам УЗ, отвечающим за информационную безопасность, необходимо проводить следующее.

1. Категорирование ИС, аппаратно-программного обеспечения ИС, а также средств защиты информации, используемых в ИС.

2. Определение потенциальных угроз и уязвимостей аппаратно-программного обеспечения ИС и средств защиты информации, используемых в ИС, с применением базы данных общеизвестных уязвимостей информационной безопасности CVE (от англ. Common Vulnerabilities and Exposures) [1] и банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России [2].

3. Поиск эксплойтов, которые целесообразно применять для проверки триггеров ИС и систем мониторинга, компилирование их в выполняемую программу (скрипт), для дальнейшей реализации [3].

4. Запуск скомпилированной программы и наблюдение за триггерами, которые должны среагировать на каждый эксплойт. Это действие должно реализовываться 4 способами:

1) за пределами контролируемой зоны УЗ от лица неавторизованного пользователя;

2) за пределами контролируемой зоны УЗ от лица авторизованного пользователя;

3) внутри локальной вычислительной сети УЗ от лица сотрудника учреждения с автоматизированного рабочего места;

4) внутри локальной вычислительной сети УЗ от лица неавторизованного пользователя при условии подмены IP и MAC адресов.

В большинстве случаев программное обеспечение для аудита информационной безопасности ИС разрабатывается под определенные задачи и на основании текущих угроз и уязвимостей.

Список литературы

1. CVE [Электронный ресурс]. – Режим доступа: https://www.cve.org/. – Дата доступа: 05.05.2024.
2. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat-section/. – Дата доступа: 05.05.2024.
3. Дербин, Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности: учебное пособие / Е. А. Дербин, А. В. Царегородцев. – Москва: ИНФРА-М. – 2024. – 267 с.

СМЕШАННОЕ ОБУЧЕНИЕ НА АНГЛИЙСКОМ ЯЗЫКЕ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ТЕОРИЯ ЭЛЕКТРИЧЕСКОЙ СВЯЗИ» ДЛЯ ИНОСТРАННЫХ СТУДЕНТОВ

Т.М. Фильченкова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Смешанное обучение в системе высшего образования Республики Беларусь в условиях цифровой трансформации рассматривается как инновационный способ повышения качества образовательных услуг и эффективности работы профессорско-преподавательского состава учреждения высшего образования, достижения оптимального уровня ресурсозатрат на организацию образовательного процесса, а также обеспечения конкурентоспособности учреждения высшего образования [1].

В образовательной среде учреждения высшего образования смешанное обучение более эффективно, т.к. в результате формируется специалист, обладающий более высоким уровнем профессиональных компетенций, способный самостоятельно совершенствовать свои знания, умения и навыки на протяжении всей трудовой деятельности [2].

Учебная дисциплина «Теория электрической связи» на английском языке для иностранных студентов специальности «Защита информации в телекоммуникациях» преподается на 2 курсе в весеннем семестре. Программой предусмотрен объем в размере 112 академических часов (3 зачетные единицы). В соответствии с учебным планом учреждения высшего образования аудиторных часов – 56 академических часов, из них лекций – 32 академических часа, лабораторных занятий – 16 академических часов, практических занятий – 8 академических часов. Формой текущей аттестации по данной учебной дисциплине является экзамен. Учебная дисциплина «Теория электрической связи» занимает важное место в подготовке будущих специалистов в сфере защиты информации. Изучение данной учебной дисциплины позволяет создать благоприятные условия для формирования профессиональных компетенций, развития самостоятельности, ответственности и организованности. Для изучения учебной дисциплины «Теория электрической связи» иностранные студенты должны ранее усвоить следующие дисциплины: «Линейная алгебра и аналитическая геометрия», «Математический анализ», «Физика».

Преподавание технических учебных дисциплин на английском языке иностранным студентам имеет следующие особенности: 1) английский язык для студентов и преподавателей не является родным (возникают проблемы с восприятием устной речи); 2) специальная лексика учебной дисциплины; 3) метафоричность некоторых специальных терминов; 4) снятие лексической многозначности терминологических единиц. Смешанное обучение на английском языке по учебной дисциплине «Теория электрической связи» для иностранных

студентов позволяет минимизировать указанные выше проблемные аспекты преподавания путем создания электронного образовательного ресурса с визуальными учебными материалами, закрепляющими проверочными тестами.

Список литературы

1. Богуш, В. А. Цифровизация образования: проблемы, вызовы и перспективы / В.А. Богуш, Е.Н. Шнейдеров // Адукацыя і выхаванне. – 2021. – № 1. – С. 14–21.

2. Фильченкова, Т. М. Менеджмент системы электронного обучения в системе высшего образования на примере БГУИР / Т. М. Фильченкова, В. Н. Пунчик // Вышэйшая школа. – 2024. – № 1. – С. 22–28.

КОМБИНИРОВАНИЕ КАСКАДНОЙ МОДЕЛИ И СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ДЛЯ РАЗМЕЩЕНИЯ ИНФОРМАЦИИ В ФАЙЛАХ ИЗОБРАЖЕНИЙ

А.А. Хартанович

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Открытые каналы связи уязвимы для раскрытия, модификации или уничтожения информации. Существующие методы стеганографии для изображений не всегда обеспечивают достаточную защиту из-за потенциальных искажений данных, таких как повреждение, сжатие, масштабирование и другие изменения изображений. Поэтому актуальной задачей является поиск новых методов стеганографического встраивания информации и использование дополнительной защиты для восстановления поврежденных данных с помощью корректирующих кодов.

В кодах с низкой плотностью проверок на четность (LDPC) матрицы проверки на четность являются разряженными и имеется возможность использования графа Таннера – это обеспечивает эффективность коррекции ошибок, особенно при наличии случайных ошибок и аддитивного белого гауссовского шума [1].

Коды Рида-Соломона (РС) особенно эффективны при исправлении пакетов ошибок, возникающих в быстрой последовательности, путем передачи избыточной информации и использования методов перемежения [2].

Использование каскадного подхода, при котором два и более кода применяются последовательно может обеспечить возможность исправления большего количества ошибок. Использование РС кода в качестве внутреннего кода в каскадной схеме обеспечивает возможность исправления пакетных ошибок, а использование кода LDPC в качестве внешнего – обеспечивает эффективность коррекции случайных ошибок. Таким образом данная каскадная модель, в первую очередь, сможет исправить пакеты ошибок, а во вторую – исправит оставшиеся случайные ошибки.

Стеганографический метод дискретного вейвлет-преобразования (ДВП) включает разложение изображения на набор коэффициентов вейвлетов различных масштабов и частот [3]. Встраивание информации посредством применения ДВП может обеспечить некоторую устойчивость к сжатию, обрезке, вращению и масштабированию, сохраняя при этом незаметность, так как сообщение встраивается в коэффициенты преобразования.

Комбинирование каскадной модели на основе РС кода и кода LDPC с последующей стеганографией в изображение через ДВП может обеспечить надежность передачи и скрытия данных даже при значительном повреждении контейнера, что предлагает комплексный подход к возможности исправления большого количества ошибок и восстановления данных.

Список литературы

1. Caire, G. LDPC coding for interference mitigation at the transmitter / G. Caire, D. Burshtein, S. S. Shamai // 40th Annual Allerton Conference on Communications, Control and Computing. – 2002. – P. 217–226.

2. Мак-Вильямс, Ф.Дж. Теория кодов, исправляющих ошибки. / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – С. 287–299.

3. Лобач, В. И. Применение вейвлет-анализа в обработке изображений и стеганографии / В. И. Лобач // Информационные технологии и системы: материалы международной научной конференции, Минск, 24 октября 2012 г. – С. 240–241.

НОРМАТИВНЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ И КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

В.М. Хиль, Е.И. Шаронова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

В современном мире информация стала одним из ключевых ресурсов, требующих надежной защиты. Важность защиты информации особенно актуальна для государственных и коммерческих организаций, где обработка и хранение информации являются неотъемлемой частью их деятельности. Республика Беларусь регулирует аспекты защиты информации в области государственных и коммерческих организаций следующими законодательными актами:

– Законом от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»;

– Постановлением Министерства связи и информатизации Республики Беларусь от 25.06.2015 № 37 «Об утверждении Положения о мероприятиях по обеспечению информационной безопасности в организациях»;

– Приказом Министерства обороны Республики Беларусь от 15.04.2016 № 207 «Об утверждении Порядка и методики проведения работ по защите информации в государственных организациях»;

– Приказом Министерства связи и информатизации Республики Беларусь от 12.08.2020 № 123 «О мерах по обеспечению информационной безопасности в сети Интернет».

Закон Республики Беларусь «Об информации, информатизации и защите информации» определяет основные принципы и положения по защите информации во всех сферах деятельности, включая государственные и коммерческие организации.

Постановление Министерства связи и информатизации Республики Беларусь «Об утверждении Положения о мероприятиях по обеспечению информационной безопасности в организациях» устанавливает требования и рекомендации по обеспечению информационной безопасности в организациях, включая государственные и коммерческие.

Приказ Министерства обороны Республики Беларусь «Об утверждении Порядка и методики проведения работ по защите информации в государственных организациях» устанавливает конкретные процедуры и методики защиты информации в государственных организациях.

Приказ Министерства связи и информатизации Республики Беларусь «О мерах по обеспечению информационной безопасности в сети Интернет» определяет меры по обеспечению информационной безопасности в сети Интернет для государственных и коммерческих организаций [1–4].

Список литературы

1. Закон от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: http://pravo.by/main.aspx?guid=3871&p0=200800455. – Дата доступа: 07.05.2024.
2. Постановление от 25.06.2015 № 37 «Об утверждении Положения о мероприятиях по обеспечению информационной безопасности в организациях» [Электронный ресурс]. – Режим доступа: http://pravo.by/main.aspx?guid=3961&p0=201503737. – Дата доступа: 07.05.2024.
3. Приказ от 15.04.2016 № 207 «Об утверждении Порядка и методики проведения работ по защите информации в государственных организациях» [Электронный ресурс]. – Режим доступа: http://pravo.by/main.aspx?guid=3961&p0=201603877. – Дата доступа: 07.05.2024.
4. Приказ от 12.08.2020 № 123 «О мерах по обеспечению информационной безопасности в сети Интернет» [Электронный ресурс]. – Режим доступа: http://pravo.by/main.aspx?guid=3961&p0=202000123. – Дата доступа: 07.05.2024.

УСОВЕРШЕНСТВОВАННЫЙ СКРЫТЫЙ КАНАЛ ABC-CHANNEL НА ОСНОВЕ БЛОКЧЕЙН

П.И. Цыркунович

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

Новый подход в области безопасной связи – ABC-Channel, представляющий собой усовершенствованный скрытый канал, основанный на технологии блокчейн, становится ключевым для обеспечения защиты информации в небезопасных сетевых средах. Преимущества блокчейн, такие как децентрализация и анонимность, делают его привлекательным для использования в разработке таких каналов. Гарантировать безопасность этого канала означает обеспечить бесконтактное согласование до начала связи, неотличимые функции транзакций и неотслеживаемые идентификационные данные после связи. ABC-Channel, представляет собой систему скрытой коммуникации на основе блокчейна, которая соответствует трем важным критериям: бесконтактному согласованию каналов, неразличимым характеристикам транзакций и непрослеживаемой идентификации коммуникаций. Помимо высокого уровня безопасности, ABC-Channel проявляет впечатляющие возможности в обеспечении высокой пропускной способности скрытой коммуникации. В результате обширных экспериментов обнаружено, что даже при коэффициенте полноты 0,491 классификатор затрудняется в различении транзакций, сгенерированных ABC-Channel, что приводит к F1-оценке, близкой к 0,5, что сравнимо с случайным угадыванием. Это указывает на то, что злоумышленникам предстоит значительные трудности в точном обнаружении скрытых транзакций. Особенно стоит отметить, что каждая скрытая транзакция в ABC-Channel, имеющая n входов, может передавать сообщение объемом до 256×n бит, что представляет собой передовую возможность по сравнению с другими методами, использующими неявное внедрение в Bitcoin. Более того, ABC-Channel не зависит от конкретных блокчейн-платформ, что позволяет его применение в широком спектре блокчейн-технологий [1].

Список литературы

1. Xiaobo Ma, Pengyu Pan, Jianfeng Li, Wei Wang, Weizhi Meng, Xiaohong Guan: ABC-Channel: An Advanced Blockchain-based Covert Channel [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2403.06261. – Дата доступа: 26.03.2024.

АТАКА ОТРАВЛЕНИЯ ПРОТОКОЛОВ LLMNR/NBT-NS И ПРОТИВОДЕЙСТВИЕ ЕЙ

Е.А. Шитик

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

LLMNR и NTB-NS – это протоколы, которые используются Windows, чтобы искать хосты по DNS-имени при сбое DNS-запросов в сети. Например, при необходимости идентификации определенного хоста, компьютер обращается к другим устройствам в сети с запросом, знают ли они этот хост, используя протокол LLMNR. Этот протокол по умолчанию активирован в Active Directory, хоть это и небезопасно, так как на запрос может ответить устройство, скомпрометированное злоумышленником. Приоритет способов разрешения имен в Windows: localhosts, Hosts, DNS, LLMNR, MDNS, NBT-NS. Протоколы LLMNR и NBT-NS предназначены для определения адресов хостов путем отправки мультикастных или широковещательных запросов по сети. Во время такой активности и возможна атака. С помощью таких инструментов, как Responder, злоумышленники могут наблюдать за сетевым трафиком, выявляя запросы LLMNR и NBT-NS, и отвечать на них, маскируясь под требуемый хост. В результате устройство, отправившее запрос, будет полагать, что нашло нужный хост, и попытается установить с ним соединение через SMB, при этом отправив хеш-пароля пользователя.

В докладе проводится анализа возможностей злоумышленника по организации атака отравления протоколов LLMNR и NBT-NS. Представлены методы, позволяющие детектировать проявления атаки на элементы сетевой инфраструктуры. Также представлены рекомендации по созданию базовых конфигураций для противодействия атакам отравления протоколов LLMNR и NBT-NS. Атаки с отравлением LLMNR и NBT-NS представляют значительные угрозы для сетевой безопасности. Внедряя рекомендации, изложенные в этой статье, вы можете защитить свою сеть от этих типов атак. Для защиты от отравления LLMNR, вы можете отключить LLMNR для всех компьютеров в домене, используя групповые политики. Для защиты от отравления NBT-NS, вы можете вручную отключить NBT-NS для каждого сетевого адаптера.

Список литературы

1. PoisonedCredentials – разбор задания с платформы CyberDefenders [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/775414/. – Дата доступа: 04.05.2024.

2. How To Protect Against LLMNR And NBT-NS Poisoning / informer.io [Электронный ресурс]. – Режим доступа: https://informer.io/resources/llmnr-and-nbt-ns-poisoning. – Дата доступа: 04.05.2024.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МУЛЬТИКЛЮЧЕВОЙ СИСТЕМЫ ТЕКСТОВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ЦВЕТОВЫХ КООРДИНАТ HSL

Н.П. Шутько
Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Стеганография – одно из важнейших направлений в области защиты авторского права посредством размещения невидимой идентификационной информации в документах различного типа.

В работах [1, 2] был предложен и проанализирован метод текстовой стеганографии, основанный на модификации цветовых координат HSL.

Для дальнейшего исследования воспользуемся математическим описанием цветового пространства, изложенном в фундаментальном научном исследовании М. М. Гуревича [3].

При использовании этой модели относительно указанного стеганографического метода любой цвет Φ' может быть представлен в цветовом пространстве с помощью вектора, описываемого уравнением: $\Phi' = hH + sS + lL$, где H, S, L – соответственно тон (Hue), насыщенность (Saturation) и яркость (Lightness); h, s, l – количественные (весовые) коэффициенты в выбранной шкале, которые указывают число единиц каждого из трех параметров в составе цвета Φ'.

Если текст-контейнер состоит из Z символов, то формально цветовой параметр каждого t-го символа, Φ'_t, может быть представлен как совокупность коэффициентов h_t, s_t, l_t: $\Phi'_t = \{h_t, s_t, l_t\}$, $1 \le t \le Z$, где t – порядковый номер символа в текстовом документе-контейнере.

Таким образом, оригинальность метода состоит в том, что процессы осаждения/извлечения информации осуществляются при сравнительном изменении / анализе цветовых параметров пар соседних символов: $\{h_t, s_t, l_t\}$ и $\{h_{t+1}, s_{t+1}, l_{t+1}\}$.

При этом цветовые координаты $\{h_t, s_t, l_t\}$ являются базой для осаждения / извлечения определенного знака («0» или «1») сообщения. Изменение параметра соседнего символа оценивается по отношению к этому базовому.

Список литературы

1. Шутько, Н. П. Использование цветовых координат HSL для защиты и передачи авторской информации / Н. П. Шутько // Информационные технологии: материалы 86-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января – 12 февраля 2022 г. – Минск: БГТУ, 2022. – С. 125-128.

2. Шутько, Н. П. Особенности моделирования и реализации комбинированного метода текстовой стеганографии / Н. П. Шутько // Информационные технологии в промышленности, логистике и социальной сфере (ITI*2023): тезисы докладов XII Международной научно-технической конференции, Минск, 21–22 сентября 2023 г. – Минск: ОИПИ НАН Беларуси, 2023. – С. 177-180.

3. Гуревич, М. М. Цвет и его измерение / М. М. Гуревич. – М.;Л.: Изд-во АН СССР, 1950. – 267 с.

ИЗОЛИРОВАННЫЕ ТОКОПРОВОДЯЩИЕ КАНАЛЫ НА ПОДЛОЖКАХ ИЗ АНОДНОГО ОКСИДА АЛЮМИНИЯ

А.В. Якушев, Д.В. Ревенько, С.А. Биран, А.В. Короткевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Композиционные наноструктуры из анодного оксида алюминия можно использовать для формирования межслойного вертикального электрического соединения различных слоев без дополнительных операций формирования отверстий в межслойной изоляции, что позволяет получать на поверхности последующие слои с хорошей планаризацией, для формирования различных устройств, используемых в системах защиты информации.

Изолированные токопроводящие каналы получали на подложках из алюминия марки А0Н толщиной 0,9 мм. Для утонения подложек до 0,4 мм и улучшения качества поверхности подложки подвергали длительному травлению в NaOH. После этого на поверхности подложек формировали маску из фоторезиста для локального анодирования. Анодирование проводили в потенциостатическом режиме в растворе лимонной кислоты, после чего удаляли фоторезистивную маску. Далее проводили пористое анодирование при постоянном напряжении 90 В в электролите на основе ортофосфорной кислоты в течении 10 мин. Это позволяет сформировать на поверхности поры с большим диаметром, что улучшит адгезию фоторезиста к поверхности. После этого на поверхности формировали маску из фоторезиста.

Использование комбинированной маски из фоторезиста и пористого анодного оксида позволяет увеличить время анодирования до пробития фоторезиста. Сквозное пористое анодирование проводили в два этапа в растворе на основе щавелевой кислоты при постоянной температуре 19°С. На первом этапе анодирование проводили в гальваностатическом режиме до момента пока напряжение анодирования не достигало 100 В, после этого переходили в потенциостатический режим для избегания прогорания образца.

Значение токов утечки фиксировали с помощью измерителя характеристик полупроводниковых приборов Л2-56. Контакт к подложке осуществляли с помощью зондов с вольфрамовыми иглами: один из зондов притирали к токопроводящему каналу, а другой к внешнему слою алюминия. Значения токов утечки составляли от 11 до 65 нА при напряжении 1000 В.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Ярмольчик, С.П. Способ

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Технические средства защиты информации играют важную роль в современном мире, где данные становятся все более ценными и подвержены угрозам со стороны злоумышленников. В данной теме будут рассмотрены основные аспекты и принципы работы технических средств защиты информации.

Одним из наиболее распространенных технических средств защиты информации являются фаерволы. Фаервол (брандамуэр) – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Они служат первой линией обороны от внешних атак и помогают предотвратить несанкционированный доступ к компьютерным системам.

Другим важным техническим средством защиты информации являются антивирусные программы. Они предназначены для обнаружения, блокирования и удаления вредоносных программ, таких как вирусы, черви, троянские программы и шпионское ПО. Антивирусные программы регулярно обновляют свою базу данных, чтобы распознавать новые угрозы и обеспечивать надежную защиту от вредоносного программного обеспечения.

Биометрические системы защиты также заслуживают внимания. Они основаны на использовании уникальных физических или поведенческих характеристик человека, таких как отпечатки пальцев, радужная оболочка глаза, голос и другие, для идентификации и авторизации пользователей. Благодаря высокой надежности биометрические системы защиты предотвращают несанкционированный доступ к информации.

Наконец, стоит отметить системы резервного копирования и восстановления данных, которые помогают защитить информацию от потери или повреждения. Эти системы создают резервные копии данных и обеспечивают возможность восстановления информации в случае аварий, сбоев или атак.

В заключение можно сказать, что в современном цифровом мире, где информация играет ключевую роль, важно понимать и применять эффективные технические средства защиты информации. Они помогают предотвратить утечку конфиденциальных данных, защищают от вирусов и мошенничества, обеспечивают целостность и доступность информации.

Однако следует отметить, что технические средства защиты информации не являются универсальным решением. Важно также учитывать социальные и организационные аспекты безопасности информации, обучать сотрудников правилам использования информационных ресурсов, применять политику безопасности и регулярно аудитировать системы на предмет выявления уязвимостей.

Технические средства защиты информации – это лишь один из аспектов обеспечения безопасности. Но при правильном применении и интеграции с другими мерами защиты они способны значительно повысить уровень безопасности данных и обеспечить сохранность важной информации.

РАЗРАБОТКА И ВНЕДРЕНИЕ МЕТОДОВ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.Д. Ярмош, И.С. Тарасюк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Целостность данных определяет их точность, полноту и непротиворечивость и влияет на эффективность функционирования системы и доверие к ее результатам.

Контроль целостности данных в основном осуществляется с помощью хэш-функций. Хэш-функции генерируют уникальные контрольные суммы для данных, которые позволяют проверить целостность путем сравнения контрольной суммы, сгенерированной с использованием хэш-функции, с сохраненным значением контрольной суммы. Также для аутентификации данных и проверки их целостности с помощью ключей шифрования используются цифровые подписи. Эти методы обеспечивают защиту от несанкционированных изменений данных.

В информационных системах важным аспектом контроля целостности данных является проверка на уровне базы данных. Базы данных обладают мощными средствами для контроля целостности данных, такими как ограничения целостности, транзакции и журналирование. Это позволяет обнаруживать и исправлять ошибки,

связанные с целостностью данных, и поддерживать их в согласованном состоянии.

Внедрение механизмов контроля целостности данных требует комплексного подхода и учета специфических требований каждой информационной системы. При выборе методов контроля целостности необходимо учитывать структуру системы, объем данных, требования к производительности и уровень безопасности. Эффективное внедрение механизмов контроля целостности данных позволяет предотвратить несанкционированный доступ, обнаружить ошибки и повреждения данных, а также обеспечить соответствие требованиям законодательства и нормативных актов. Внедрение механизмов контроля целостности данных должно осуществляться на всех уровнях информационной системы. Это требует тесного взаимодействия между разработчиками, системными администраторами и специалистами по информационной безопасности.

Постоянное обновление и адаптация механизмов контроля целостности данных являются необходимыми, учитывая постоянное развитие информационных технологий и возрастание угроз информационной безопасности. Необходимо следить за новыми методами атак и уязвимостями, а также внедрять соответствующие меры защиты и обновления.

Дальнейшие исследования в области контроля целостности данных должны быть направлены на разработку новых методов, а также на адаптацию существующих механизмов к новым вызовам и угрозам. Только таким образом можно гарантировать безопасность и надежность данных в информационных системах и обеспечить их эффективное функционирование.

Список литературы

1. Xu, D. A Data Quality Assessment and Control Method in Multiple Products Manufacturing Process / D. Xu, Z. Zhang, J. Shi // 2022 5th International Conference on Data Science and Information Technology (DSIT), Shanghai, China, 2022. – P. 1–5.

2. Zhang, C. Data Integrity Verification Algorithm of Accounting Informatization Cloud Based on Genetic Optimization Neural Network / C. Zhang, D. Liang // 2023 Asia-Europe Conference on Electronics, Data Processing and Informatics (ACEDPI), Prague, 2023. – P. 68–72.

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ДИСКРЕТНОЙ КВАНТОВОЙ КАРТЫ

А.В. Сидоренко, Е.А. Высотская

Белорусский государственный университет, Минск, Республика Беларусь

Появление быстродействующих квантовых компьютеров, квантовых вычислений способствует разработке новых методов защиты информации. Квантовые вычисления в своей работе применяют такие квантовые явления, как квантовое состояние, суперпозиция и запутанность в квантовых системах.

В данной работе рассматриваются основные аспекты применения дискретной квантовой карты совместно с алгоритмами шифрования RSA и SHA-3. Рассматриваются: генерация ключей с помощью алгоритма RSA; использование алгоритма SHA-3 для обработки исследуемой последовательности и получения хеш-значения функции; процесс интеграции SHA-3 в процессы шифрования и дешифрования.

Применение дискретной квантовой карты для шифрования данных является одним из главных подходов к вантовому шифрованию. Дискретная квантовая карта включается для формирования новой математической модели, когда случайная

последовательность данных генерируется от квантовой логистической карты. Квантовая логистическая карта увеличивает резистентность системы к выбранным атакам на исходное изображение и способна эффективно защитить передаваемую информацию от квантовых атак.

Экспериментально полученные результаты и их анализ показывает, что применение квантовой дискретной карты позволяет улучшить безопасность передаваемой информации.

ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

А.В. Сидоренко, И.В. Сергеев

Белорусский государственный университет, Минск, Республика Беларусь

Распространение информационных технологий в различных сферах деятельности человека способствует разработке новых методов защиты информации. Ключевую роль в защите цифровой информации, особенно в свете развития технологий мобильной связи 5G, Интернета вещей IoT, где безопасность передачи данных приобретает особую актуальность, играют алгоритмы шифрования, основанные на принципах динамического хаоса.

В данной работе рассматривается разработка и создание программного продукта для шифрования и дешифрования информации в виде изображений на основе хаотических отображений. В работе применяются отображения кота Арнольда, Хенона, а также логистического отображения. Для демонстрации возможностей использования алгоритмов: кота Арнольда, Хенона, использования логистического отображения реализована компьютерная программа на языке Python. В качестве тестовых иображений применяются: Horizon Zero.png размером 250×250 пикселей, Peppers.png, размером 435×435 пикселей, Squirrel.png, размером 3849×2160 пикселей.

Полученные результаты тестирования разработанной компьютерной программы с построением гистограмм изображений, автокорреляции трех разных изображений с применением в качестве ключа буквенных, числовых и смешанных последовательностей показали позитивные результаты в отношении шифрования и дешифрования.

ДЛЯ ЗАМЕТОК

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XXII Белорусско-Российской научно–технической конференции
(Минск, 12 июня 2024 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 21.05.2024. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 12,32. Уч.-изд. л. 10,5. Тираж 100 экз. Заказ 75.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/238 от 24.03.2014, № 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск