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
XXI Белорусско-российской научно-технической конференции
(Минск, 6 июня 2023 г.)

Минск БГУИР 2023

УДК 004.056.5
ББК 32.972.5
Т38

Т38 **Технические** средства защиты информации : тез. докл. XXI Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 6 июня 2023 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2023. – 104 с.
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

USE OF NON-BINARY VT-CODES IN NETWORK TRAFFIC WATERMARKING

B. Assanovich

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

According to the current level of telecommunications development, 5G communication systems are expected to provide higher data rates, lower latency and improved scalability. To ensure the security and reliability of generated data traffic 5G networks must be designed to support security protocols and reliable communication applications. The error correcting codes have found many other uses, including watermarking and intrusion detection, cryptography and information security. The input patterns, which are easily identified when the watermarked flows cross an observation point, allow the creation of a mechanism to scan the network for the harmful activity.

If the embedded watermark is both reliable and unique, it is possible to analyze the watermarked return traffic and trace it back at intermediate nodes. This TA approach is referred to as the "flow watermarking" (FW). FW is often implemented on the basis of inter-packet-delay (IPD) schemes, where watermark bits are embedded in the intermediate packet time which allows to hide traffic artifacts from an attacker.

Most FW technologies use a carrier that modulates the transfer of watermark data. Many FW schemes use the quantization-index modulation (QIM) watermarks into IPDs and added a layer of ECC to handle watermark desynchronisation and substitution errors.

To embed the watermark, the IPD flow is modified so that each IPD is converted to an interval according to the even/odd multiplier of the quantization interval $\Delta/2$, depending on the value of the 0/1 bit. Existing approaches for the implementation of binary QIM are well known and are given in [1]. One of the known FW scheme for embedding watermarks is based on the use of binary Varshamov-Tenengolz (VT) codes, which are subcodes of linear codes. This scheme uses linear codes with an attached marker and optional matrix interleaving to deal with bursting errors.

The evaluation of true positive rates (TPR) in the detection of watermarks have shown that they not do not exceed 10 %, but the TPR value drops to 66 % when the packet loss is 20 %, which is rare in a network environment. To eliminate artifacts caused by binary quantization of delays in the delivery of network packets and improve the detection of watermarks in traffic control, we proposed switching to multilevel QIM and using non-binary VT codes.

These codes have attracted interest, as evidenced by the publication [2], where an encoding method was proposed for a non-binary systematic VT code. The coding principle for these codes is similar to known binary ones. However, a systematic representation requires recoding the bit representation of symbols into a non-binary equivalent for their dyadic (multiple of a power of 2) representation. Therefore, the growing complexity of encoding-decoding is a price to pay for the resulting efficiency.

References

1. B. Assanovich et all. Information Encoding for Flow Watermarking and Binding Keys to Biometric Data [Electronic resource] –. Access mode: https://www.intechopen.com/online-first/86246. – Date of access: 01.05.2023.

2. Abroshan M., Venkataramanan R., Fabregas A.G.I. Efficient Systematic Encoding of Non-binary VT Codes // 2018 IEEE International Symposium on Information Theory (ISIT). 2018. P. 91–95.

TECHNIQUES FOR ANALYZING OF INFORMATION SYSTEM VULNERABILITIES

K.A. Nguyen

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

Techniques for analyzing the vulnerabilities of information systems based on the use of the OpenVAS vulnerability scanner have been developed. The first of the developed technique includes the following steps.

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

Step 2. Complete the virtual machine installation process.

Step 3. Get access to the resources of the installed virtual machine using the following credentials: login – admin, password – admin.

Step 4 Create a new web administrator account.

Step 5. Enter the IP address of the device web interface.

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

The second of the developed technique includes the following steps.

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

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

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

Step 4. Generate a password for the first login.

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

Step 6. Generate a new administrator password.

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

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

INCREASING THE RELIABILITY OF THE INTERNET OF THINGS

H.H. Sudani

Iraqi Ministry of Science and Technology, Baghdad, Iraq

The Internet of Things (IoT) is an emerging technology working with multiple sensors and wireless communication protocols. People are utilizing smart & intelligent devices towards comfort life using IoT. Home automation is one among them coordinating with the actuators and sensors connected within the network. The IoT network has many layers like a controller, device, gateway, server, and application layer. The device layer is connected with many small-sized numbers of devices and there are chances to occur faults in this layer. The definition of IoT is fundamental in understanding the problem of reliability within the paradigm. The Internet of Things (IoT) aims to transform the human society toward becoming intelligent, convenient, and efficient with potentially enormous economic and environmental benefits. Reliability is one of the main challenges that must be addressed to enable this revolutionized transformation. The Internet has transformed the way people communicate with each other. The Internet of Things (IoT) aims to take this stride further to seamlessly connect people and various things, transforming society toward becoming intelligent, convenient, and efficient (ICE) with potentially enormous economic and environmental benefits. The IoT has developed rapidly, spanning diverse application

domains from healthcare to home automation, environmental monitoring to smart energy, and intelligent transportation to smart buildings, smart manufacturing smart agriculture, and smart military to the smart ocean [1].

Due to the safety-critical or mission-critical nature of the IoT applications, it is imperative that the IoT system operate reliably throughout the intended mission time. In other words, reliability is one of the crucial requirements for the adoption of the IoT in critical applications [2]. Reliability analysis and design are therefore indispensable step before IoT systems can be widely deployed for safety-critical and mission-critical applications. The reliability of the smart grid itself is of great importance. The safety-critical or mission-critical nature of IoT applications and the rapid growth of data generated require highly reliable and efficient data storage and processing solutions. Cloud computing is one such solution that has played a crucial role in the recent IoT developments [3]. Additional new aspects of system complexity and dynamics may arise, making the existing reliability models and solutions inadequate or inaccurate. New and efficient reliability models and tools are expected for capturing the new features and behaviors, leading to more effective and accurate IoT system reliability analysis, optimization, and design. The ultimate goal is to transform our society toward being ICE (intelligent, convenient, and efficient).

References

1. Sakhnini J., H. Karimipour, A. Dehghantanha [et al.]. Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey // Internet of Things. 2019. 100111.

2. J. Kempf, J. Arkko, N. Beheshti, K. Yedavalli, “Thoughts on Reliability in the Internet of Things” [Electronic resource]. – Access mode: https://pdfs.semanticscholar.org/32f3/ddb8fe2d6acc0f04c9 d515edd4913d7afabf.pdf. – Date of access: 01.05.2023.

3. Botta A., de Donato W., Persico V. [et al.]. Integration of Cloud computing and Internet of Things: A survey // Future Generation Computer Systems. 2016. Vol. 56. P. 684–700.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ БЛОКЧЕЙН

В.А. Абрамова, Н.И. Белодед

Академия управления при Президенте Республики Беларусь, Минск, Беларусь

В 21 веке, веке стремительного развития информационных технологий, обмен информацией играет важную роль. Однако этот процесс имеет как преимущества, так и ряд недостатков. И чем важнее информация, тем больше желающих ее «заполучить», воспользоваться в своих целях. Именно поэтому нужно знать, что такое криптография и как с ее помощью можно защитить важную для вас информацию.

Говоря простым языком, криптография – наука о методах шифрования информации. Для этого криптографы используют различные математические принципы, которые позволяют добиться высокой сохранности, целостности и подлинности информации.

Современная криптография включает в себя разные направления, самыми популярными являются системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации.

Используя цифровые подписи, каждый пользователь может потратить средства только со своего кошелька и только один раз. Этот принцип и лежит в основе самого принципа «электронных денег».

Механизм хэш-функций обеспечивает один из вариантов подтверждения алгоритма консенсуса – PoW (Proof of Work), а также – достоверность процесса майнинга, отвечающего как за генерацию новых монет в сети Биткоин, так и за проверку уже совершенных транзакций. В конкретной ситуации используется криптографическая функция SHA-256.

Именно криптографические методы защиты информации были положены в основу функционирования первой сети блокчейн – Биткоин.

Главной особенностью блокчейна является отсутствие централизованного управления. Это значит, что каждый узел распределенной системы делает записи в своей версии реестра независимо от других узлов и синхронизируется с ними в рамках одноранговой сети. Записи соединяются в инкрементальную цепочку блоков с использованием криптографических алгоритмов.

Блокчейн эффективно выполняет два из трех ключевых аспектов информационной безопасности – целостность и доступность информации. Благодаря децентрализованной топологии и криптографическим механизмам враждебные манипуляции данными становятся весьма дорогостоящими и затруднительными.

Но есть и недостаток традиционной технологии блокчейн. Он заключается в том, что технология не позволяет обеспечить третий аспект – конфиденциальность данных. Это приводит к редким, но все же взломам кошельков и «хищению» информации, электронных денег.

Существуют смарт-контракты, которые существенно расширяют возможности блокчейн-сетей, но в то же время приводят к немалому количеству новых атак.

Смарт-контракт - алгоритм, предназначенный для автоматизации процесса исполнения контрактов. Принцип его действия заключается в следующем: содержание договора записывается в виде кода в компьютерной программе, отслеживающей и обеспечивающей исполнение обязательств. Стороны сделки прописывают в таком контракте условия, а также санкции за их невыполнение. Смарт-контракты обладают такими преимуществами, как прозрачность сделки, защита от внесения изменений, не утвержденных сторонами, возможность совершения сделок анонимно. Умные контракты легли в основу множества блокчейн проектов и инициатив.

Таким образом, без понимания принципов работы криптографии, невозможно эффективное совершенствование сетей блокчейн в целом. Всестороннее изучение базовых криптографических методов защиты информации в технологии блокчейна необходимо для глубокого понимания безопасности и конфиденциальности систем, основанных на технологии блокчейн. Так, например, более поздние сети используют более эффективные протоколы кодирования, нежели SHA-256. С каждым днем это направление развивается, процесс не стоит на месте.

Список литературы

1. Балдов Д.В., Петрова С.Ю., Лебедев А.А. Использование технологии блокчейн для защиты данных // International Journal of Open Information Technologies. 2021. № 9.

2. Грошева Е.К., Невмержицкий П.И. Блокчейн – новая революция // Бизнес-образование в экономике знаний. 2018. №1 (9).

3. Сафарли Н.Э. Смарт-контракт: понятие, правовая природа, особенности заключения и исполнения // Legal Concept. 2019. № 4.

ПРОГРАММА ДЛЯ ИЗУЧЕНИЯ ШИФРОВ ПРОСТОЙ ЗАМЕНЫ

А.М. Абросимов, М.Б. Абросимов

ФГБОУ ВО Саратовский государственный технический университет имени Гагарина Ю.А., Саратов, Россия

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

Знакомство с шифрами для старшеклассников или студентов младших курсов начинается обычно с простейших шифров простой замены, которыми являются шифры Цезаря и Атбаш [1]. Часто связанные с такими шифрами задачи встречаются и на олимпиадах по криптографии. Для удобства знакомства с шифрами Цезаря и Атбаш была разработана описываемая далее программа, которая позволяет выполнять шифрование, расшифрование, а также помогает в дешифровании.

В классическом варианте шифр Цезаря выполняет замену буквы алфавита на букву, которая расположена в алфавите со сдвигом на заданное число позиций. Таким образом, для русского языка ключом является число от 1 до 33.

В шифре Атбаш происходит замена буквы на букву, которая расположена в такой же позиции как исходная, но с конца алфавита. В исходном варианте шифра Атбаш ключа нет.

В описанных вариантах шифров Цезаря и Атбаш дешифровка не представляет сложности. В Интернете доступны онлайн-калькуляторы, которые справляются с этой задачей. Усилением шифров Цезаря и Атбаш является перемешивание алфавита, которое состоит в том, что в определенную позицию записывается ключевое слово, не содержащее повторяющихся букв, а после выписываются оставшиеся буквы алфавита. В таком варианте дешифровка становится нетривиальной задачей. Если криптограмма является достаточно большой по размеру, то можно применять методы частотного анализа [1], в том числе и автоматизированные с использованием словаря [2]. Однако для коротких криптограмм (длиной меньше 800 символов) это сделать сложно.

Разработанная программа позволяет выполнять шифрование и расшифрование шифрами Цезаря и Атбаш с перемешиванием алфавита. Однако основной интерес представляет функция дешифровки и определения ключа, который был использован при шифровании. Эта функция реализована в полуавтоматическом режиме и позволяет облегчить формирование гипотез и их проверку для выполнения дешифровки, что оказывается наиболее интересным в процессе обучения и понимания криптоанализа для старшеклассников, студентов младших курсов, обучающихся по информационной безопасности, либо студентов иных направлений, у которых есть предмет по информационной безопасности.

Список литературы

1. Введение в криптографию / Под общ. ред. В.В. Ященко. М.: МЦНМО, 2012. 348 с.

2. Абросимов М.Б., Коннова А.Д., Толмилов Д.А. О криптоанализе шифров простой замены с использованием словаря // Технические средства защиты информации : тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 14.

XXI МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО КРИПТОГРАФИИ SARCRYPT

М.Б. Абросимов, В.Н. Салий, А.В. Жаркова, А.А. Лобов,
О.В. Моденова, А.С. Конюшенко, В.А. Маскаев, Р.А. Романов

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

В 2002 году в Саратовском научном исследовательском государственном университете имени Н.Г. Чернышевского появилась специальность «Компьютерная безопасность» и была создана выпускающая кафедра. В том же году была проведена и первая олимпиада по криптографии для старшеклассников. Изначально основной целью проведения олимпиады ставилась задача привлечения заинтересованных школьников для поступления на направления обучения, связанные с информационной безопасностью. На протяжение всех последующих лет конкурс на эту специальность был достаточно высокий, однако достаточно высокий процент студентов отсеивался после первых лет учебы. В связи с чем к участникам олимпиады была добавлена категория студентов, для выявления талантливых ребят, обучающихся по направлениям информационной безопасности, и повышения их мотивации.

Первые годы олимпиада проводилась только для учеников 9–11 классов в 4 тура. Каждый тур состоял из 5 задач, на решение которых отводилось 2 недели. Студенты или ученики других классов могли принимать участие в олимпиаде вне конкурса. С 2019 года олимпиада стала проводиться для трех категорий участников: учеников 6–8 классов, 9–11 классов и студентов. Олимпиада стала проходить в два тура. В первую полную неделю декабря проводится дистанционный тур (отборочный), а в январе проводится очный тур на базе факультета компьютерных наук и информационных технологий Саратовского научного исследовательского государственного университета имени Н.Г. Чернышевского. 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 связи со сложной эпидемиологической обстановкой в 2019–2020, 2020–2021 и 2021–2022 годах второй тур олимпиады проводился в режиме онлайн на базе платформы ZOOM. В 2022–2023 учебном году дистанционный тур проводился с 5 по 11 декабря 2022 г. В отборочном туре приняли участие 64 ученика 6–8 классов, 162 ученика 9–11 классов и 58 студентов из городов России, Республики Беларусь, Республики Молдовы, Республики Казахстан и Туркменистана. Победители первого тура получили приглашение на второй тур, который состоялся 29 января 2023 г.

Впервые второй проводился в очно-распределенном формате. Для очных участников олимпиада проводилась в Саратовском научном исследовательском государственном университете имени Н.Г. Чернышевского, а для остальных участников – на платформе Контур.Толк. Во II туре приняли участие 106 участников из России, Республики Молдовы, Республики Казахстан и Туркменистана. Все участники I–II туров получили электронные дипломы, а их руководители – грамоты. Итоги обоих туров олимпиады можно посмотреть на сайте [1].

Список литературы

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

ОБУЧЕНИЕ СТУДЕНТОВ ПРИЕМАМ РАБОТЫ С ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОБНАРУЖЕНИЯ, ПОИСКА И ПОДАВЛЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ ПРИ ПРОВЕДЕНИИ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

В.М. Алефиренко

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

В соответствии с учебным планом специальности «Электронные системы безопасности» лабораторные занятия (работы) по дисциплине «Методы и технические средства обеспечения безопасности» проводятся на 3 курсе в 5 и 6 семестрах [1].

Одна из работ посвящена изучению технических характеристик различных видов технических средств обнаружения, поиска и подавления закладных устройств и приемов работы с ними. В качестве изучаемых устройств использовались: индикатор электромагнитного поля, интерсептор, портативный частотомер ROGER RFM-31, сканирующий детектор-приемник XPLORER, сканирующий приемник IC-R5, радиоприемное устройство AR3000A, генератор шума Гром ЗИ-4, портативный глушитель сотовых телефонов СТРАЖ Мини 3G, направленный микрофон СУПЕР УХО-50, а в качестве объектов обнаружения, поиска и подавления использовался малогабаритный радиомикрофон, а также различные модели мобильных телефонов самих студентов.

Студентам ставились следующие задачи.

1. Провести сканирование диапазонов радиовещательных станций ДВ, СВ, КВ, УКВ и отметить частоты работающих станций, их название, дату и время фиксации.

2. Определить зону подавления генератора электромагнитного шума, используя сканирующий приемник, индикатор поля или интерсептор с представлением полученных результатов на плане помещения и этажа в соответствующем масштабе.

3. Провести поиск скрытого радиомикрофона, используя последовательно индикатор поля или интерсептор (метод акустической завязки), частотомер (измерение частоты), сканирующий приемник (идентификация сигнала) и определить расстояния, на которых осуществляется «захват» сигнала радиомикрофона с указанием взаимного расположения используемых приборов и радиомикрофона.

4. Провести исследования возможности подавления мобильных телефонов различных моделей и различных операторов в различных режимах (поиск сети, вызов, разговор, а также 2G, 3G, 4G) с помощью подавителя мобильных телефонов и определить расстояния, на которых происходит полное или частичное подавление сигнала соответствующего режима работы.

5. Проверить заявленные параметры направленного микрофона (расстояние и угол) с приведением графических построений и формулы, связывающей расстояния и углы, соответствующих расчетов и результатов исследований.

Результаты по каждому заданию представлялись в табличной форме с указанием всех необходимых исходных данных и соответствующих полученных результатов исследований, а также с представлением поясняющих рисунков и выводов в конце задания.

Список литературы

1. Алефиренко В.М. Интеграция научных исследований при проведении лабораторных занятий по дисциплине «Методы и технические средства обеспечения безопасности» // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 16–17.

АНАЛИЗ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ПЕРЕНОСНЫХ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ПОДАВЛЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С ПОМОЩЬЮ КОМПЛЕКСНОГО ГЕОМЕТРИЧЕСКОГО ПОКАЗАТЕЛЯ КАЧЕСТВА

В.М. Алефиренко, А.Д. Денскевич, А.М. Асиненко

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

В работе [1] проведены результаты сравнительного анализа технических характеристик переносных радиоэлектронных средств подавления (ПРСП) беспилотных летательных аппаратов (БПЛА) с помощью комплексного арифметического показателя качества, представляющего собой сумму произведений значений нормированных единичных показателей и соответствующих им нормированных коэффициентов значимости. Наряду с арифметическим показателем, существуют и другие, например, геометрический показатель, представляющего собой корень степени числа единичных показателей из произведений значений нормированных единичных показателей в степени соответствующих им нормированных коэффициентов значимости. В связи с этим, представляет интерес проведения исследований с помощью геометрического показателя и сравнения результатов, полученных с помощью этих показателей [2].

Как и в работе [1] для сравнения были выбраны следующие модели ПРСП: Аргумент-2, ПАРС, Дрон 1200, Гарпун-2М, Novasky SC-J1000m, Drone Hunter XR, QLY-F069, Droneshield MKIII, Vodasafe DJ600, Greetwin GW-UAV90Pro и ряд других, выпускаемых различными фирмами. Всего для сравнения было выбрано 32 модели. В качестве единичных показателей для ПРСП использовались такие технические характеристики как дальность подавления, время непрерывной работы, диапазоны частот блокирования, диапазон рабочих температур, вес и габаритные размеры. Предварительно было проведено нормирование единичных показателей и соответствующих им коэффициентов значимости.

Как показали результаты расчетов, наилучшие значения показателей качества были у модели Greetwin GW-UAV90Pro (0,58), на втором месте – Greetwin GW-UAV70 (0,54) и на третьем месте – DroneShield Tactical (0,53). По арифметическому показателю эти модели занимали соответственно 11 место (0,47), 3 место (0,54) и 28 место (0,37). Такой разброс результатов объясняется тем, что каждый комплексный показатель представляет только относительные, а не абсолютные результаты распределения уровня качества исследуемых приборов в рамках используемых в нем математических операций. Поэтому, для более точного определения уровня качества приборов можно использовать несколько комплексных показателей с последующим суммированием результатов, полученных по каждому прибору. В этом случае первое место будет занимать Greetwin GW-UAV70 (1,08), второе – Greetwin GW-UAV90Pro (1,05) и третье – DroneShield Tactical (0,9). Таким образом, из 32 ПРСП лучшей по уровню качества является модель Greetwin GW-UAV70.

Список литературы

1. Алефиренко В.М., Денскевич А.Д. Комплексный анализ технических характеристик переносных радиоэлектронных средств подавления БПЛА // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. С. 15.

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

МОДЕЛИРОВАНИЕ СЛЕДЯЩЕГО ИЗМЕРИТЕЛЯ НАПРАВЛЕНИЯ

И.В. Баженова

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

Определение направления движения объектов радиотехническими средствами, основано на прямолинейном распространении радиоволн в однородной среде и сводится, таким образом, к определению направления прихода радиоволн, излучаемых или отражаемых от объектов, путем сравнения амплитуды, фазы или частоты колебаний, возбуждаемых в антенной системе [1]. Определение направления прихода электромагнитных волн, отраженных от объекта, называется радиопеленгацией. Существуют следующие амплитудные методы пеленгации: метод максимума, метод сравнения и метод минимума. 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. В следящих измерителях с одновременным сравнением сигналов (называемых моноимпульсными системами) определение угловой координаты производится по результатам сравнения параметров сигналов, принимаемых одновременно двумя разнесенными в пространстве антеннами. В следящих измерителях с последовательным сравнением сигналов (называемых часто системами с коническим сканированием) прием сигналов от цели ведется на одну антенну, диаграмма направленности которой совершает периодическое колебание относительно равносигнального направления, не совпадающего с осью диаграммы направленности. В результате вращения игольчатого луча в пространстве образуется конус, в центре которого создается равносигнальное направление. Поэтому такое сканирование называется коническим сканированием. 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.

Список литературы

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

ПОДХОДЫ К КОНСТРУИРОВАНИЮ ПРИБОРОВ СВЧ

И.В. Баженова

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

При многомодовом взаимодействии возможна одновременная реализация на разных модах различных процессов излучения: на одних – черенковского, на других – гирорезонасного, на третьих – ондуляторного и т. д. В такой ситуации возможны два противоположных подхода при конструировании приборов: а) использование методов селекции рабочей моды, т. е. отстройка и подавление «паразитных» мод; б) использование кооперации мод при многомодовом взаимодействии релятивистского электронного потока (РЭП) с полем электродинамической системы (ЭДС). Традиционно используется первый подход. Однако, рекордные уровни мощности излучения (30 ГВт) достигнуты в приборах с использованием комбинированного (черенковского и гирорезонансного) излучения при их кооперации [1]. Ввиду этого,

приборы на основе комбинированного кооперативного взаимодействия РЭП с полем представляются более перспективными и актуальными.

Для реализации всех потенциальных возможностей, заложенных в «гладкой» нерегулярной ЭДС при одномодовом и многомодовом взаимодействии РЭП с возбуждаемым в ней полем необходимо создание фундаментальной теоретической базы для адекватного моделирования и оптимизации указанных процессов. Ввиду этого задачами, решаемыми в настоящей исследовательской работе, являются:

1) разработка строгой теории комбинированных процессов излучения релятивистских электронных потоков в многомодовых нерегулярных электродинамических структурах;

2) создание на этой основе математических моделей, методов и компьютерных программ анализа и оптимизации сверхмощных многомодовых приборов СВЧ;

3) определение оптимальных параметров, включая оптимальный профиль электродинамических структур и реализуемые при этом улучшенные выходные характеристики.

Список литературы

1. Батура М.П., Кураев А.А., Синицын А.К. Оптимизация релятивистских ЛБВ-0 на нерегулярных волноводах с учетом высших мод // КрыМиКо 2004: матер. 14-й Междунар. конф., Севастополь, 2004.

УЧЕТ ВРЕМЕННЫХ ОТКАЗОВ ФУНКЦИОНАЛЬНЫХ УСТРОЙСТВ ЭЛЕКТРОННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ В ИНЖЕНЕРНЫХ РАСЧЕТАХ ЕЕ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ

А.А. Батура, С.М. Боровиков, А.В. Будник

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

Для электронной аппаратуры бытового и хозяйственного назначения обычно выполняют оценку эксплуатационной надежности системы с учетом возможного возникновения устойчивых отказов ее функциональных устройств [1–3]. Восстановление работоспособного состояния устройств после возникновения таких отказов достигается путем выполнения ремонта. Вре́менные отказы функциональных устройств, называемые также сбоями [3, 4], представляют собой кратковременную потерю устройством работоспособного состояния вследствие действия на него естественных или искусственных дестабилизирующих факторов (гроза, молния, ураганные порывы ветра, электромагнитное излучение мощных промышленных установок, помехи по сети электропитания, умышленные действия нарушителей и т.п.). После окончания действия дестабилизирующего фактора или снижения его уровня до значения, которое не вызывает нестабильную работу функционального устройства системы, работоспособное состояние устройства восстанавливается без выполнения ремонта, либо при незначительном вмешательстве оператора путем перезагрузки программного обеспечения (для программируемых вычислительных устройств). Расчет надежности электронных систем безопасности без учета возможных временных отказов дает завышенное значение уровня защиты объектов с помощью рассматриваемой системы, что в конечном итоге может негативно отразиться на обеспечении безопасности защищаемого объекта.

В данной работе показано, как в инженерных расчетах можно учесть совместное влияние устойчивых и временных отказов на надежность функциональных устройств и электронной системы безопасности в целом. Особенностью этого учета является

принятие во внимание того факта, что потеря работоспособного состояния функционального устройства системы происходит в случае, если возникает хотя бы один из отказов: либо устойчивый отказ из-за возникшей технической неисправности, либо временный отказ из-за кратковременного воздействия на работу устройства эксплуатационного дестабилизирующего фактора. Учет как устойчивых, так и временных отказов позволит для электронной системы безопасности получить проектные показатели надежности, которые более достоверно характеризуют потенциальные возможности системы по защите объекта в конкретных эксплуатационных условиях.

Список литературы

1. Надежность технических систем: справочник / Ю.К. Беляев [и др.]; под ред. И.А. Ушакова. М.: Радио и связь, 1985. 608 с.

2. Боровиков С.М., Цырельчук И.Н., Троян Ф.Д. Расчет показателей надежности радиоэлектронных средств. Минск: БГУИР, 2010. 68 с.

3. Боровиков С.М. Теоретические основы конструирования, технологии и надежности. Минск: Дизайн ПРО, 1998. 336 с.

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

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТЕЙ ВОЗНИКНОВЕНИЯ ФАКТОРОВ, ВЫЗЫВАЮЩИХ ВРЕМЕННЫЕ ОТКАЗЫ ЭЛЕКТРОННЫХ УСТРОЙСТВ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

А.А. Батура, А.В. Будник, С.М. Боровиков

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

Для получения более достоверных данных об ожидаемой эксплуатационной надежности электронной системы безопасности необходимо на этапе проектирования принять во внимание не только устойчивые, но и временные отказы [1]. Временные отказы проявляются в виде кратковременной потери устройством работоспособного состояния из-за воздействия на него естественных или искусственных дестабилизирующих факторов. После окончания действия дестабилизирующего фактора работоспособное состояние устройства восстанавливается без выполнения ремонта. Актуальным является вопрос об определении вероятностей возникновения факторов, вызывающих появление временных отказов, а также вероятностей возникновения самих временных отказов функциональных устройств электронной системы безопасности при условии, что имел место данный дестабилизирующий фактор. Одним из наиболее дестабилизирующих естественных факторов является гроза и возникающие при этом электрические искровые разряды в атмосфере. Для учета влияния грозовых разрядов на возникновение временных отказов функциональных устройств электронной системы безопасности необходимо располагать двумя следующими вероятностями:

– возникновения грозы в местности, где расположен защищаемый объект;

– возникновения временного отказа типового функционального устройства электронной системы безопасности в случае наличия грозы.

Для определения первой вероятности применительно к г. Минску и территории Республики Беларусь использованы карты и статистические данные о частоте и интенсивности возникновения гроз за достаточно длинный период времени [2, 3]. Для определения второй вероятности использованы результаты экспериментальных исследований, представленные ОАО «Белэлектромонтаж» [4].

Использование указанных вероятностей позволит при оценке надежности электронной системы безопасности учесть влияние временных отказов (обусловленных электрическими искровыми разрядами в атмосфере, происходящими во время гроз), что обеспечит получение более достоверных показателей эксплуатационной надежности электронной системы безопасности.

Список литературы

1. Батура А.А., Будник А.В., Боровиков С.М. Новый подход к оценке эксплуатационной надежности электронных систем обеспечения безопасности объектов инфокоммуникаций // Современные средства связи: материалы XXVII Международной научно-технической конференции, Минск, 27–28 октября 2022 г. С. 86–88.

2. Количество грозовых дней и других явлений в крупных городах Беларуси [Электронный ресурс]. – Режим доступа: https://terrazn.by/poleznoe/grozovie-dni-v-belarusi/. – Дата доступа: 22.04.2023.

3. Лопух П.С., Бережкова Е.С. Анализ и прогноз пространственно-временного распределения гроз и града на территории Беларуси. Журнал Белорусского государственного университета. География. Геология. 2019. № 1. С. 35–45.

4. Вероятности временных отказов устройств электронных систем безопасности [Электронный ресурс] – Режим доступа: https://belbem.by/veroyatnosti-vremennyih-otkazov-ustroystv-esb/. – Дата доступа: 10.03.2023.

ВЕБ-СКРЕЙПИНГ, МЕТОДЫ ПРОТИВОДЕЙСТВИЯ И ИХ ЭФФЕКТИВНОСТЬ

Т.Е. Белогривая, Р.А. Фортель

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

Веб-скрейпинг является технологией получения данных путем извлечения их со страниц веб-ресурсов. Веб-скрейпинг может быть сделан пользователем компьютера вручную, но обычно данный термин относится к автоматизированным процессам, которые реализованы с помощью кода, выполняющего GET-запросы на сайт.

Основной задачей веб-скрейпинга является сбор данных из интернет-источников. С помощью данной технологии можно не только искать и копировать информацию, но и мониторить обновление информации на веб-сайтах.

Средств противодействия веб-скрейпингу довольно много, но нет ни одного на 100 % эффективного. Пока пользователи сайта могут получить к нему доступ, веб-скрейпер также может это делать, так как он имитирует действия реального пользователя. К тому же, методы противодействия веб-скрейпингу могут мешать реальным пользователям.

Рассмотрим основные контрмеры противодействия автоматизированному сбору данных.

1. Блокировка IP-адресов. Это один из способов противодействия веб-скрейпингу, когда данные крадут постоянно и, как правило, в большом объеме. Здесь речь идет уже не только о текстах, но и других сведениях, представляющих стратегический интерес для конкурентов. Разрешить или запретить доступ к сайту некоторым IP-адресам можно через менеджера IP-адресов на используемом хостинге.

Недостаток: бот может использовать прокси (поддельные IP-адреса).

2. Использование капчи. Этот метод заключается в добавлении капчи на сайт. Триггером вывода капчи может является переход на определенную страница сайта, определенное действие пользователя и многое другое. Однако при использовании данного метода следует понимать, что капча будет мешать реальным пользователям. Самый популярный сервис на данный момент это reCAPTCHA от компании Google.

Недостаток: капчи можно обойти с помощью сторонних сервисов, где реальные пользователи их решают.

3. Электронная почта и номер мобильного телефона. При выполнении определенных действий на сайте проводится проверка по мобильному телефону или электронной почте.

Недостаток: бот может использовать одноразовые электронные ящики или временные мобильные номера виртуальных сотовых операторов.

4. Изменение структуры сайта. Интернет-ресурс может регулярно обновлять структуру сайта. Из-за этого злоумышленнику придется переписывать код сбора данных.

Недостаток: современный веб-скрейпинг не завязывается на структуре сайта, а использует более точные идентификаторы.

Таким образом, хорошо написанный код имитирует активность реального пользователя и вычислить бота очень трудно. Также следует понимать, что, защищаясь от веб-скрейпинга, сайт может оказаться заблокированным для краулеров Google и Яндекса, которые являются такими же ботами. Последствия этого очевидны: сайт частично или полностью потеряет лидирующие позиции в поисковиках.

ВЛИЯНИЕ ТЕМПЕРАТУР В ТЕРМОТРАНСФЕРНОЙ ТЕХНОЛОГИИ НА ЧАСТОТНЫЕ ХАРАКТЕРИСТИКИ КОЭФФИЦИЕНТОВ ОТРАЖЕНИЯ И ПЕРЕДАЧИ УГЛЕРОДОСОДЕРЖАЩИХ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Е.С. Белоусова, О.В. Бойправ, Л.М. Лыньков

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

В работе [1] было обосновано использование термотрансферной технологии для создания углеродосодержащих поглотителей электромагнитного излучения. В данной работе описаны результаты исследования влияния температуры обработки поглотителей электромагнитного излучения в термотрансферном планшетном прессе на частотные характеристики коэффициентов отражения и передачи в диапазоне 0,7–17,0 ГГц.

По методике, описанной в [1] было изготовлено три образца углеродосодержащих поглотителей, состоящих из волокнистого материала, пропитанного водным раствором поверхностного активного вещества с техническим углеродом. Каждый образец после полного высыхания помещался в термотрансферный планшетный пресс на 10 минут при разных температурах: 50 ºС, 150 ºС, 200 ºС. После извлечения из термотрансферного планшетного пресса образцы были охлаждены, далее осуществлялось измерение коэффициентов отражения и передачи и изучение изменения структуры материала посредством микроскопического анализа. Анализ частотных характеристик коэффициентов отражения и передачи в диапазоне частот 0,7–17 ГГц показал, что температура термотрансферного планшетного пресса не оказывает влияние на частотные характеристики. У всех образцов значения коэффициента отражения, измеренного в режиме короткого замыкания и согласованной нагрузки, коррелируют между собой. Минимальные значения коэффициентов отражения для образцов углеродосодержащих поглотителей были получены на частотах 9,0–11,0 ГГц и составили –9,0…–11,5 дБ. Необходимо отметить, что значение коэффициентов отражения до помещения образцов в термотрансферный планшетный пресс составляло –10,0…–14,5 дБ в диапазоне частот 9,0–16,5 ГГц, что объясняется изменением толщины и структуры образца за счет влияния температуры и давления пресса.

Таким образом, в ходе исследования было установлено, что использование термотрансферного планшетного пресса при изготовлении углеродосодержащих поглотителей способствует закреплению частиц углерода в волокнистой матрице, при этом значение коэффициентов отражения и передачи увеличиваются на 3 дБ и 10 дБ соответственно в диапазоне частот 0,7–17 ГГц.

Исследования выполнены в рамках НИОК(Т)Р «Разработка поглотителей электромагнитного излучения на основе углесодержащих и фольгированных материалов для систем информационной и экологической безопасности. Разработка устройств для подавления помех в цепях радиоэлектронной и электротехнической аппаратуры» по мероприятию 32 «Разработать новые материалы, покрытия и системы для защиты радиоэлектронного, оптоэлектронного и информационного оборудования, биологических объектов от внешних энергетических воздействий, обеспечения их экологической и информационной безопасности, высокой функциональной надежности и работоспособности» подпрограммы 2 «Освоение в производстве новых и высоких технологий» Государственной программы «Наукоемкие технологии и техника» на 2021–2025 годы.

Список литературы

1. Белоусова Е.С., Бойправ О.В., Лыньков Л.М. Применение термотрансферной технологии для создания углеродосодержащих поглотителей электромагнитного излучения // Комплексная защита информации: матер. XXVI науч.-практ. конф., г. Минск 25–27 мая 2021 г. С. 104–106.

ГИБКИЕ СЛОИСТЫЕ ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СВЧ-ДИАПАЗОНА НА ОСНОВЕ ФОЛЬГИРОВАННЫХ МАТЕРИАЛОВ

О.В. Бойправ, Н.В. Богуш, Е.С. Белоусова, М.В. Павлёнок

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

Одной из областей применения поглотителей электромагнитного излучения СВЧ-диапазона является защита средств обработки информации от воздействия электромагнитных помех. При этом создаются условия для поддержания целостности и доступности информации, обрабатываемой с помощью указанных средств. Большая часть изготавливаемых в настоящее время поглотителей электромагнитного излучения СВЧ-диапазона характеризуются упорядоченной структурой, в которую входят плоские или объемные элементы с одинаковыми формой и размерами. Это обусловлено тем, что путем регулирования форм и размеров указанных элементов можно обеспечивать требуемые граничные значения рабочей полосы частот поглотителей, в структуру которых они входят. В связи с этим одно из направлений исследований в области разработки поглотителей электромагнитного излучения СВЧ-диапазона в настоящее время связано с созданием новых или усовершенствованием существующих технологий изготовления поглотителей электромагнитного излучения СВЧ-диапазона, характеризующихся упорядоченной структурой.

Авторами предложена и экспериментально новая технология изготовления обозначенных поглотителей. Эта технология включает в себя следующие этапы.

Этап 1. Откраивание фрагментов от рулона синтетического нетканого материала с учетом того, что размер и форма этих фрагментов должны совпадать с планируемыми размером и формой изготавливаемых поглотителей, а количество этих фрагментов должно превышать в 2,0 раза количество изготавливаемых поглотителей.

Этап 2. Откраивание фрагментов от рулона полимерного фольгированного материала с учетом того, что размер, форма и количество этих фрагментов должны совпадать с планируемыми размером и формой, а также с количеством изготавливаемых поглотителей.

Этап 3. Формирование на основе алюминиевой фольги плоских включений в объем изготавливаемых поглотителей электромагнитного иззлучения.

Этап 4. Упорядоченное распределение сформированных включений по поверхностям половины фрагментов, полученных в результате реализации этапа 1.

Этап 5. Размещение половины фрагментов, полученных в результате реализации этапа 1 и не использованных в рамках реализации этапа 4, поверх распределенных в результате реализации этапа 4 включений.

Этап 6. Термопрессование конструкций, полученных в результате реализации этапов 1–5 при температуре 100,0 °С.

Этап 7. Закрепление по одному из фрагментов, полученных в результате реализации этапа 2, на поверхностях конструкций, спрессованных в результате реализации этапа 6.

Поглотители, изготовленные в соответствии с предложенной технологией, характеризуются значениями коэффициента поглощения электромагнитного излучения в СВЧ-диапазоне, достигающими величины 0,9. Эти поглотители по сравнению с аналогами характеризуются пониженной массой на единицу площади.

Исследования выполнены в рамках научно-исследовательской работы «Эластичные и воздухопроницаемые электромагнитные экраны на основе фольгированных материалов для обеспечения информационной и экологической безопасности» подпрограммы «Физика конденсированного состояния и создание новых функциональных материалов и технологий их получения» государственной программы научных исследований «Материаловедение, новые материалы и технологии» на 2021–2025 годы.

ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО СПЕЦИАЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Т.В. Борботько

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

Широкое использование информационных технологий в производственной деятельности различных организаций обуславливает появление широкого спектра рисков информационной безопасности. Ключевыми проблемами современности становятся обеспечение безопасности информационной инфраструктуры государства и предприятий, совершенствование мер защиты национальных интересов Республики Беларусь в информационной сфере, что обуславливает необходимость подготовки специалистов по информационной безопасности.

В Белорусском государственном университете информатики и радиоэлектроники в партнерстве с рядом организаций, создана система подготовки кадров, которая охватывает следующие аудитории обучающихся: школьники, студенты, специалисты ответственные в организациях за обеспечение информационной безопасности, руководители различных подразделений, обеспечивающие критически важные процессы в организациях с применением информационных технологий, сотрудники организаций – пользователи информационных систем.

Основными функциями системы являются следующие

1. Информационная. Ее реализация заключается в способствовании формирования представления о сфере и направлениях информационной безопасности у молодежи, что должно способствовать появлению интереса к направлению и мотивации выпускника школы в выборе будущей профессии.

2. Образовательная. Обеспечивает формирование знаний, умений, навыков и готовность их использования в трудовой деятельности выпускниками университетов.

3. Повышение осведомленности. Эта функция направлена на совершенствование знаний сотрудников организаций в области информационной безопасности с учетом текущего положения дел в этой сфере.

Созданная система позволяет сотрудникам кафедры защиты информации не только обеспечивать образовательный процесс, но и проводить апробацию новых образовательных программ для последующего использования их материалов в учебном процессе кафедры в рамках университета, а также поддерживать непосредственную связь с заказчиками кадров и своевременно актуализировать содержание учебных дисциплин по специальности «Информационная безопасность».

АТАКИ С ИСПОЛЬЗОВАНИЕМ DNS ПРОТОКОЛА И ПРОТИВОДЕЙСТВИЕ ИМ

Ф.Т. Борботько

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

Для обращения к веб-ресурсам широко используется протокол прикладного уровня DNS, который применяется для преобразования доменных имен в IP-адреса серверов, на которых находятся эти ресурсы. Таким образом, отказ в работе DNS-сервера или сфальсифицированные данные, полученные от него могут привести к невозможности получить доступ к веб-ресурсу.

Для передачи DNS сообщений в основном используется протокол UDP, что существенно облегчает выполнение атак, при которых реализуется подмена ответов от сервера. Достаточно перехватить запрос и послать ответ от имени сервера. После приема такого пакета ответы от сервера будут отбрасываться, так как порт, на который пришел ответ от нарушителя, будет закрыт. На DNS-сервера можно проводить атаки методом «отравления кеша», путем заполнения его ложными записями. Атаки типа отказа в обслуживании (DoS) выполняются путем создания большого количество запросов на поиск адресов случайных доменных имен, в результате чего DNS-сервер будет вынужден обрабатывать только эти запросы.

Для защиты от прослушивания DNS трафика может быть использован DoT (DNS-over-TLS), суть которого заключается в установлении TLS соединения между отправителем и получателем. Также может быть реализован DoH (DNS-over-HTTPS), который передает зашифрованные запросы на преобразование имен через HTTPS соединения, в результате чего такие пакеты выглядят как любые другие веб-запросы. Для защиты от атак на DNS-сервера путем «отравления кеша» может быть использован DNSSEC, который обеспечивает проверку подлинности записей, полученных от серверов более высокого уровня. Это реализуется за счет использования двух ключей. Секретным ключом подписывается запись, а открытым ключом, который содержится в DNS-ответе проверяется подлинность и целостность этой записи.

Список литературы

1. Руководство по безопасности DNS / Habr.com [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/varonis/articles/519108/. – Дата доступа: 30.04.2023.

2. Анализ основных атак на DNS-сервер и методы использования DNSSEC при защите DNS-сервера / Cyberleninka.ru [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/analiz-osnovnyh-atak-na-dns-server-i-metody-ispolzovaniya-dnssec-pri-zaschite-dns-servera/viewer. – Дата доступа: 30.04.2023.

АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ БАНКОВ И НЕБАНКОВСКИХ КРЕДИТНО-ФИНАНСОВЫХ УЧРЕЖДЕНИЙ КАК МЕРА ПОВЫШЕНИЯ КАЧЕСТВА НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

С.Ю. Воробьёв

ОАО «Банковский процессинговый центр», Минск, Беларусь

Концепцией обеспечения кибербезопасности в банковской сфере, утвержденной постановлением Национального банка Республики Беларусь от 20.11.2019 № 466, декларируется направление развития в части придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, что потребует внесение изменений в Банковский кодекс Республики Беларусь (реализация направлений методологического обеспечения деятельности по обеспечению кибербезопасности в банковской сфере позволит усовершенствовать действующее регулирование в данной области). После придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, на постоянной основе будет организован контроль за соблюдением стандартов. Контроль соблюдения стандартов по обеспечению кибербезопасности будет осуществляться как Национальным банком (дистанционный контроль, контроль в рамках проведения аудита, внеплановых проверок), так и банками (контроль со стороны подразделений, ответственных за кибербезопасность, а также контроль в рамках проведения внутреннего аудита).

Концепцией информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1, декларируется заинтересованность государства по взаимодействию с IT-компаниями, Интернет-провайдерами, операторами связи и внешними экспертами в обновлении и развитии механизмов выявления угроз информационной безопасности через IT-аудит, мониторинг киберрисков, поиск уязвимостей и актуальных средств защиты, выработку правил поведения в сети Интернет.

В настоящее время требования к проведению аудита информационной безопасности банков банковской системы Республики Беларусь устанавливаются СТБ 34.101.42-2013 (в соответствии с законодательством данный стандарт носит рекомендательный характер), технические требования и правила Национального банка Республики Беларусь ТТП ИБ 2.1-2020 содержат требования к проведения внешнего и внутреннего аудитов информационной безопасности соответственно.

Также банки и небанковские кредитно-финансовые организации проводят аудиты на соответствие требованиям стандартов, которые не являются обязательными для применения на территории Республики Беларусь, однако применяются последними для повышения зрелости бизнес-процессов, например, ИСО 27001, PCI DSS, Программа безопасности пользователей SWIFT. Для совершенствования бизнес-процессов, оценки текущего уровня зрелости управления последними (включая сферу кибербезопасности) банки проводят внутренний (или внешний с привлечением аутсорсера) IT-аудит в соответствии с международным стандартом, устанавливающим требования к защите и контролю за конфиденциальными данными COBIT.

Для организации высококлассного ИТ-менеджмента в кредитно-финансовых учреждениях, повышения качества оказываемых услуг активное применяется ITIL.

МЕТАЛЛИЗАЦИЯ ПЕРЕХОДНЫХ ОТВЕРСТИЙ В КРЕМНИЕВЫХ ПЛАСТИНАХ ДЛЯ СОЗДАНИЯ ТРЕХМЕРНЫХ МИКРОСТРУКТУР

А.И. Воробьева, Е.А. Уткина

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

При изготовлении современных ИМС наиболее серьезные технологические проблемы связаны с формированием металлических межсоединений. Монтаж кремниевых кристаллов по принципу трехмерной сборки кристаллов (3D-технология) позволяет в значительной мере решить эти проблемы. Одним из основных направлений в развитии технологий 3D интеграции является метод «сквозных отверстий через кремний («Through Silicon Via, TSV -технология)». Это технология обеспечивает не только повышение степени интеграции, но и снижает трудоемкость сборки, улучшает быстродействие и энергопотребление систем [1, 2]. Наиболее перспективным материалом межсоединений является медь благодаря ряду преимуществ перед алюминием, таких как более низкое сопротивление, стойкость к электромиграции, более высокие скорости переключения элементов ИМС [3]. Цель данной работы – исследовать влияние способа подготовки поверхности подложки Si/SiO_2 с глухими отверстиями (активации) и условий непосредственного (прямого) электрохимического осаждения меди в отверстия с барьерным слоем TiN на дне отверстий на микроструктуру, характер границ раздела и поверхности в системе кремний – матрица столбиков меди. Такие исследования позволят упростить технологию формирования переходных отверстий в ИМС и разнообразить процессы формирования различных микроструктур и комбинированных нано-микроструктур на основе медных столбиков в подложке Si/SiO_2. Установлено, что морфология столбиков меди в переходных отверстиях определяется в большей степени процессом изготовления матрицы (в том числе на этапе активации), чем процессом электрохимического осаждения меди. В разработанном методе с активацией поверхности барьерного слоя медь осаждается во все отверстия равномерно и до поверхности. Скорость заполнения зависит от типа электролита, времени обработки и диаметра отверстий. Показано, что активированный слой TiN, который после обработки не содержит оксидов, пригоден для беззатравочного осаждения Cu в отверстия диаметром (500–2000) нм. Осаждение на поверхность TiN с пониженным содержанием оксидов и органических загрязнений приводит к образованию смачивающего слоя Cu и к более быстрой коалесценции зародышей, а также к улучшеннию адгезии между Cu и TiN. Исследован режим непосредственного (без затравочного слоя) электрохимического осаждения меди на поверхность барьерного слоя в отверстия кремниевых пластин, который позволяет провести 100%-ое (во все отверстия) осаждение металла без внутренних пустот. Непосредственное электрохимическое осаждение меди (SECD) на поверхность диффузионного барьерного слоя TiN, Ta, TaN и др. без медного затравочного покрытия может стать технологией следующего поколения для устройств ультравысокого уровня интеграция (ULSI**,** ultra large-scale integration). Такой вариант снижает стоимость изготовления металлизации и повышает качество заполнения контактных переходов и канавок (способность заполнять узкие каналы) в трехмерных микроструктурах различного назначения, в том числе для электроники средств защиты информации.

Список литературы

1. Garrou P., Bower C. and Ramm P. Handbook of 3D Integration. Wiley-VCH. 2008.
2. Ramm P, Klumpp A, Merkel R, et al. 3D system integration technologies // Mat. Res. Soc. Symp. Proc. 2003. Vol. 766. P. E5.6.1–E5.6.12.
3. Radisic A, Lühn O, Philipsen H.G.G., et al. Copper plating for 3D interconnects // Microelectron. Eng. 2011. Vol. 88. P. 701–704.

СПОСОБ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ОЦЕНИВАЕМЫХ ПАРАМЕТРОВ ПО РЕЗУЛЬТАТАМ НАВЕДЕНИЯ САМОЛЕТА НА ВОЗДУШНУЮ ЦЕЛЬ

Д.В. Высоцкий, Е.И. Хижняк

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

В настоящее время наведение истребителей-перехватчиков на воздушную цель осуществляется с автоматизированного пункта наведения авиации (АПНА) путем подачи команд управления. В данном комплексе средств автоматизации (КСА) АПНА предусмотрен режим «Тренаж» для отработки навыков лицами боевого расчета по управлению авиацией. Оценивание результатов наведения осуществляется только по реальному наведению на основании личных наблюдений проверяющего и данных объективного контроля в соответствии с нормативами [1]. При этом показатели решения задачи реального наведения боевым расчетом проверяющий оценивает субъективно и достаточно долго. Следует отметить, что в режиме «Тренаж» АПНА оценивание не производится вовсе по причине отсутствия возможности управления электронной отметкой своего самолета как по командной радиолинии управления, так и голосом. Кроме того, по результатам тренировки нельзя оценить все этапы наведения (отклонение от расчетной траектории, выход на рубеж выполнения задачи, захват цели на сопровождение и т.д.). Авторами был описан способ сопряжения компьютерных симуляторов авиационной техники (САТ) с КСА для проведения тренировки боевого расчета, а также предложена методика выставления автоматической оценки по результатам наведения своего самолета на маневрирующую воздушную цель противника [2, 3]. Одним из основных проблемных вопросов при реализации информационно-технического сопряжения (ИТС) между компьютерными САТ и КСА стало, отсутствие формализованного описания протокола обмена данными между рабочими местами экипажей воздушных судов и сервером воздушной обстановки САТ, а также создание условий для безопасной передачи данных на КСА. Для реализации ИТС между САТ и КСА было решено использовать формализованный протокол [4] который позволит обмениваться данными через модем, или по локальной вычислительной сети. Разработанное авторами программное обеспечение сопряжения САТ с КСА позволило: осуществить фильтрацию сетевого трафика САТ; выделить информацию о координатах местоположения имитируемого воздушного судна; с заданным темпом обмена произвести ее конвертацию к виду, определенному протоколом сопряжения КСА; обеспечить целостность циркулирующей информации.

В основу методики выставления автоматической оценки входят ряд оценочных параметров из нормативов [1]. Внедрение компьютерных САТ в контур автоматизированного управления для тренировки боевого расчета позволило в разы увеличить темп обмена траекторной информацией, повысить достоверность получаемых данных, а также точность определения оцениваемых параметров. Кроме того, использование системы разграничения доступа и защиту информационных каналов ограничило возможность утечки данных.

Список литературы

1. Курс специальной подготовки пунктов управления ВВС и войск ПВО − Приказ команд. ВВС и ВПВО, 22.12.2020 г., № 414. Минск, 2020.

2. Высоцкий Д.В., Хижняк А.В. Применение компьютерных симуляторов авиационной техники для подготовки боевых расчетов АПНА «Спрут» в режиме «Тренаж». Весник Военной академии Республики Беларусь. 2022. № 4 (77). С. 24–31.

3. Шеин А.С. Тренировка боевых расчетов комплекса средств автоматизации 7В800 «Спрут» с использованием авиационного симулятора «DCS» // Сб. 52 науч. конф. БГУИР. 2016. № 33. С. 75.

4. Изделие 7В970. Руководство по эксплуатации. Информационно-техническое сопряжение с ПУ (КП) и РЛС с цифровым выходом. Порядок сопряжения и настройки Ч. 5. 340 с. ЕИРВ.461311.002 РЭ5.

АЛГОРИТМ ФОРМИРОВАНИЯ ОТФИЛЬТРОВАННЫХ ЧЕРЕЗ ШИРОКОПОЛОСНЫЙ ПОЛОСОВОЙ ФИЛЬТР МНОГОУРОВНЕВЫХ ХАОТИЧЕСКИХ СИГНАЛОВ ДЛЯ СКРЫТНЫХ СИСТЕМ СВЯЗИ

А.А. Гавришев

НИЯУ «МИФИ», Москва, Россия

В работе [1] проведен анализ использования отфильтрованных через широкополосный полосовой фильтр многоуровневых хаотических сигналов (МХС) для обеспечения скрытности и надежности функционирования передачи данных в системах радиосвязи. Установлено, что применение для решения указанных задач отфильтрованных с помощью полосового фильтра с широкой полосой пропускания МХС является перспективным подходом и может быть также использовано наряду с другими широко распространенными методами. Вместе с тем, в указанной публикации не раскрыты некоторые вопросы, в частности в явном виде не описывается алгоритм формирования таких сигналов для скрытных систем радиосвязи.

Целью данной статьи является разработка алгоритма формирования отфильтрованных через широкополосный полосовой фильтр МХС для скрытных систем радиосвязи.

С учетом работы [2] и списка литературы к ней, вариант алгоритма может быть представлен в следующем виде:

1) выбирается генератор МХС, описываемый соответствующим математическим выражением;

2) выбираются такие начальные условия и значения управляющих параметров генератора МХС, при которых формируется набор МХС, обладающих положительным максимальным показателем Ляпунова $\lambda_{\max} > 0$;

3) проводится фильтрация через широкополосный полосовой с широкой полосой пропускания полученного набора МХС;

4) проводится оценка сформированного набора отфильтрованных через широкополосный полосовой фильтр МХС по следующим показателям качества:

4.1) вычисляется автокорреляционная функция набора МХС $R(\tau)$, пик-фактор набора МХС ρ, максимальный показатель Ляпунова набора МХС $\lambda_{\max}$, BDS-статистика набора МХС $\bar{w}(\varepsilon)$ и проводится сравнение полученных значений с допустимыми: $R(\tau) < R_{\text{доп}}(\tau)$, $\rho < \rho_{\text{доп}}$, $\lambda_{\max} > 0$, $\bar{w}(\varepsilon) < \bar{w}_{\text{доп}}(\varepsilon)$;

4.2) если сформированный набор отфильтрованных через широкополосный полосовой фильтр МХС удовлетворяет допустимым значениям, то он отбирается, иначе исключается;

5) шаги 1–4 повторяются до тех пор, пока не будет сформирован достаточный набор отфильтрованных через широкополосный полосовой фильтр МХС, удовлетворяющий предъявляемым показателям качества.

Список литературы

1. Осипов Д.Л., Гавришев А.А. Анализ использования отфильтрованных с помощью полосового фильтра хаотических сигналов для передачи данных в системах радиосвязи // Научное приборостроение. 2021. Т. 31. № 2. С. 93–104.

2. Гавришев А.А. Обобщенный алгоритм формирования многоуровневых хаотических сигналов для скрытных систем связи // Сборник материалов X МНК «Математическое и компьютерное моделирование». Омск, 2023. С. 250–252.

ПРОГРАММНЫЙ КОМПЛЕКС РЕГИСТРАЦИОННОГО ЦЕНТРА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ С МЕХАНИЗМОМ ВЫРАБОТКИ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.А. Герасимов

Государственное предприятие «НИИ ТЗИ», Минск, Беларусь

В настоящее время одним из наиболее востребованных облачных сервисов является сервис облачной электронной цифровой подписи. Это обусловлено широким применением облачной (т. е. виртуальной) инфраструктуры в деятельности компаний [1]. С помощью указанного сервиса обеспечивается возможность удаленной выработки значения электронной цифровой подписи. Используемый при этом личный ключ хранится и управляется удаленным сервером от имени подписанта, являющего владельцем этого ключа [2]. Чтобы обеспечить безопасность среды создания электронной цифровой подписи и гарантировать использование личного ключа только под контролем подписанта, поставщик сервиса облачной электронной цифровой подписи должен применять специальные процедуры безопасности и использовать надежные аппаратные средства и программное обеспечение, в том числе для защиты канала связи с подписантом [3].

В связи с вышеизложенным, в Республике Беларусь в рамках опытно-конструкторской работы «Совершенствование инфраструктуры открытых ключей на основе современных web-технологий» по мероприятию 2 программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»), утвержденной постановлением Совета Министров Союзного государства от 11 июня 2018 г № 5 был разработан программный комплекс, реализующий возможности выработки облачной электронной цифровой подписи.

Для безопасного функционирования комплекса используются следующие криптографические стандарты:

– СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности»;

– СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».

– СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

Программные компоненты комплекса характеризуются одними из следующих функций:

– формирование общего секретного ключа в соответствии с СТБ 34.101.66-2014, с помощью которого стороны могут выполнять аутентификацию по протоколу защиты транспортного уровня (СТБ 34.101.65-2014);

– идентификация пользователей, в том числе их регистрация и проверка их идентичности в соответствии с СТБ 34.101.87-2022.

Внедрение программного комплекса позволит повысить эффективность функционирования информационных систем инфраструктуры открытых ключей Республики Беларусь. Для организаций переход на «облачные» сервисы позволит повысить гибкость, создавать более рациональную организацию работы сотрудников и сократить расходы на поддержание собственных серверов.

Список литературы

1. Защищенная виртуальная инфраструктура [Электронный ресурс]. – Режим доступа: https://becloud.by/services/uslugi-rtsod/infrastruktura-kak-usluga-iaas/zashchishchennaya-virtualnaya-infrastruktura/. – Дата доступа: 03.04.2023

2. СТБ 34.101.78-2019. Профиль инфраструктуры открытых ключей.

3. СТБ 34.101.bclo. Требования безопасности к системам облачной подписи.

АНАЛИЗ МЕТОДА РАСШИРЕНИЯ СПЕКТРА

А.С. Гераськин, А.С. Конюшенко, А.В. Никитин

ФГБОУ ВО СГУ имени Н.Г. Чернышевского, г. Саратов, Российская Федерация

Все актуальней становится проблема контроля использования прав собственности на цифровые ресурсы. Одним из более эффективных методов решения является использование стеганографии, а именно цифрового водяного знак (ЦВЗ) – специальной метки, встраиваемой в цифровой контент с целью защиты авторских прав и подтверждения целостности самого документа.

В работе рассматривается внедрение текстовой информации в аудиосигналы методом расширения спектра прямой последовательностью (РСПП). Его идея основана на расширении сигнала данных, умножая его на элементарную посылку. В ее роли выступает псевдослучайная последовательность максимальной длины, модулированная известной частотой.

Для встраивания и извлечения сообщения используется одинаковый ключ – псевдослучайный шум, который удовлетворяет следующему условию: во всем диапазоне частот имеет ровную частотную характеристику (обычно его называют белым шумом).

Внедрение представляет собой следующий алгоритм. Считываются и подготавливаются аудиоданные из файла формата WAV, вводится сообщение M. В качестве контейнера был выбран правый канал стереофайла. Для каждого бита сообщения генерируется псевдослучайная последовательность, в качестве генератора был выбран генератор на основе RSA. Бит сообщения накладывается на выделенный сегмент контейнера с помощью соответствующей сгенерированной последовательности. Модифицированные сегменты далее объединяются в общий вектор, который удлиняется до конца аудиодорожки.

Для извлечения ЦВЗ принимающей стороне необходимо выделить правую дорожку-контейнер, а также иметь исходный аудиофайл. Определение встроенного «0» или «1» происходит на основе анализы разницы сигналов.

Была разработана программа, реализующая предлагаемый алгоритм. Также был проведен анализ эффективности внедрения ЦВЗ, найдены основные параметры: отношение сигнал/шум, интенсивность битовых ошибок, субъективная оценка качества звука.

Из полученных данных можно сделать вывод, что при внедрении в аудиофайл ЦВЗ методом РСПП изменения при прослушивании незначительны при выборе правильного коэффициента внедрения. Также характеристики частоты и амплитуды близки к исходному аудиофайлу.

Список литературы

1. Коробейников А.Г., Даурских А.Г., Павлова Н. В. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра // Научно-технический вестник информационных технологий, механики и оптики. 2009. № 1 (59). С. 82–88.

АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ ВЕБ-САЙТОВ

Е.О. Гурский

Гродненский государственный университет им. Янки Купалы, Гродно, Беларусь

1. Обзор проблем безопасности веб-сайтов, связанных с уязвимостями в коде и настройках сервера.

Примеры уязвимых веб-сайтов: Equifax [1] Роль сканера проблем небезопасности веб-сайтов в предотвращении атак.

2. Разработка сканера уязвимостей веб-сайтов.

Использование инструментов, таких как OWASP ZAP и Burp Suite. Анализ кода и запросов на поиск уязвимостей, таких как SQL-инъекции, уязвимости XSS и CSRF.

Примеры сканеров уязвимостей веб-сайтов: Acunetix [2]

3. Применение сканера уязвимостей веб-сайтов в бизнесе.

Роль сканеров уязвимостей веб-сайтов в обеспечении безопасности бизнеса.

Примеры компаний, использующих сканеры уязвимостей веб-сайтов: Amazon [3].

4. Рекомендации по использованию сканеров уязвимостей веб-сайтов.

Частота использования сканера уязвимостей веб-сайтов. Интеграция сканера уязвимостей веб-сайтов в процессы разработки и тестирования. Необходимость дополнительного анализа результатов сканирования для идентификации реальных уязвимостей.

Список литературы

1. ZDNET. [Электронный ресурс]. – Режим доступа: https://www.zdnet.com/article/ equifax-hack-blamed-for-the-most-comprehensive-identity-theft-in-history/. – Дата доступа: 01.05.2023.

2. Acunetix. [Электронный ресурс]. – Режим доступа: https://www.acunetix.com/. – Дата доступа: 01.05.2023.

3. Top cybersecurity statistics, trends, and facts. [Электронный ресурс]. – Режим доступа: https://www.csoonline.com/article/3153707/amazon-battles-to-stop-sellers-from-hijacking-prime-name.html. – Дата доступа: 01.05.2023.

ОБЕСПЕЧЕНИЕ ПОЖАРНОЙ БЕЗОПАСНОСТИ КАБЕЛЬНЫХ ПРОХОДОК В СТРОИТЕЛЬНЫХ КОНСТРУКЦИЯХ

М.С. Гурский, В.Е. Галузо

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

Борьба с пожарами в первую очередь предполагает проведение пожарно-профилактических мероприятий, направленных на ограничение распространения огня и опасных продуктов горения, обеспечения условий для эвакуации людей и имущества. Важным средством в комплексе указанных мероприятий является использование конструктивной противопожарной защиты для огнезащиты мест прохождения кабельных каналов, коробов, кабелей и проводов через огнестойкие строительные конструкции, ограничивающие распространение пожара по кабельным трассам из одного помещения в другое. Для предотвращения распространения пламени и продуктов горения в примыкающие помещения и сохранения исправности кабелей используют противопожарные проходки. В качестве средств защиты противопожарных проходок используют различные материалы: минераловатные плиты марки СМП-01; огнестойкие подушки на основе силикона и полиуретана; огнезащитные пеноблоки; противопожарные вспучивающиеся подушки типа ППВУ-1; терморасширяющиеся резиновые смеси вида «Крилер»; огнезащитные составы типа «Файрекс-300М»; огнезащитные краски марки КЛ-1, мастики типа АКМ-01 и герметики. Противопожарные растворы, пена, огнезащитные пеноблоки расширяются при воздействии огня и препятствуют распространению огня и продуктов горения в другие помещения. Огнестойкость материалов и их комбинаций может достигать до 4 часов.

При монтаже кабельной продукции стоит не только задача исключения возможности проникновения огня по путям прокладки трасс, но и задача сохранения целостности кабеля и защиты помещений от продуктов горения материалов кабеля при его возгорании. Для решения таких задач используют огнестойкие короба, которые обеспечат защиту по всей длине кабельной трассы. Для металлических коробов в качестве защитного внутреннего материала могут быть использованы минеральная вата, силикат кальция, вспенивающиеся противопожарные покрытия. Если необходима внешняя защита, то лучшим вариантом будет короб из легкого бетона или противопожарных плит. При пожаре в помещениях с кабельными трассами опасность представляет не только распространение огня, но и смертельные токсичные газы, образующиеся при горении кабельной продукции. Для предотвращения такого рода угроз необходимо использовать огнезащитное покрытие кабелей, которое вспенивается при воздействии огня и образует защитную поверхность для кабеля на время до 90 минут, что вполне достаточно для устранения возгорания или эвакуации людей [1–4].

Список литературы

1. Сайт предприятия Теплоэнергозащита. Противопожарные кабельные проходки. [Электронный ресурс] – Режим доступа: https://tozsk.ru/publikatsii/protivopozharnye-kabelnye-prohodki. – Дата доступа: 18.03.2023.

2. Сайт производителя DKC [Электронный ресурс] – Режим доступа: https://www.dkc.ru/ru/. – Дата доступа: 18.03.2023.

3. Сайт производителя OBO Bettermann [Электронный ресурс] – Режим доступа: https://www.obo.global/. – Дата доступа: 18.03.2023.

4. Заделка кабельных проходок в противопожарных стенах и перегородках. ППС-07-2012. ОАО «НИЦ Строительство»: Москва, 2012. 36 с.

ПРОВЕРКА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ НА НАЛИЧИЕ АППАРАТНЫХ СРЕДСТВ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

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

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

В работе приводятся результаты исследований по обнаружению аппаратных средств недекларированных возможностей в вычислительной технике. Показано, что в вычислительной технике могут быть сформированы каналы утечки информации за счет двойного использования отдельных элементов и устройств. С одной стороны эти элементы и устройства выполняют основную функцию в изделии и дополнительно могут использоваться для выполнения функций, не оговоренных их основным назначением и не применяемым отдельно для выполнения этой функции в изделии. Такое решение по образованию каналов утечки информации за счет использования элементов и устройств по дополнительным функциональным возможностям принято называть аппаратными средствами недекларированных возможностей. Такие каналы невозможно заблокировать, так как они скрыты и непонятно это каналы утечки или такое конструкторское решение принято при разработке изделия, при этом полная техническая документация отсутствует или нет доступа к ней.

Каналы утечки информации, образованные аппаратными средствами недекларированных возможностей, по своей сути (по функциональному назначению) являются устройствами передачи и приема радиосигналов (радиопередающими и радиоприемными устройствами). С другой стороны, канал утечки информации может быть организован и для сбора и передачи по радиоканалу, образованному в вычислительной технике аппаратными средствами недекларированных возможностей, речевой информации циркулирующей в заданном помещении. Информация, которая уязвима из-за аппаратных средств недекларированных возможностей, это информация в цифровом виде, обрабатываемая вычислительной техникой и речевая информация в акустическом виде в окружающем вычислительную технику пространстве.

Одним из самых опасных и распространенных каналов утечки речевой информации являются акустоэлектрические каналы утечки информации. Акустоэлектрические каналы возникают вследствие преобразования информационного акустического сигнала в электрический элементами вычислительных технических средств. Явление преобразования получило название «микрофонный» эффект. «Микрофонным» эффектом в большей или меньшей степени обладают керамические конденсаторы, катушки индуктивности, электровакуумные электронные лампы, резисторы.

Передача информации от вычислительной техники к нарушителю может быть организована с использованием электромагнитного поля, т. е. с использованием радиоканала. При этом также для его реализации можно использовать аппаратные средства недекларированных возможностей на базе конструктивных элементов изделий вычислительной техники.

Разработанная методика проверки вычислительной техники на наличие аппаратных средств недекларированных возможностей включает активацию аппаратных средств недекларированных возможностей провоцирующими акустическими и электромагнитными сигналами и анализ отклика на эти воздействия. Отклик аппаратных средств недекларированных возможностей может проявляться в виде изменения их тепловых полей при обработке сигналов, провоцирующих акустических и электромагнитных воздействий.

ВОЗДЕЙСТВИЕ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ НА УГЛЕРОДНЫЙ КОМПОЗИТ

А.Л. Данилюк, А.В. Кухарев

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

Углеродсодержащие композиты в настоящее время весьма активно применяются в качестве радиопоглощающих материалов [1]. В этом плане актуальным является исследование воздействия электромагнитных импульсов (ЭМИ) различной интенсивности на их электродинамические свойства. В данной работе рассмотрены особенности воздействия ЭМИ на углеродный композит в случае, когда такое воздействие не сопровождается явлениями электрического пробоя, а ведет только к появлению наведенных электрических потенциалов, формированию заряженных областей с накоплением заряда, генерации неравновесных носителей заряда, сопровождающейся их рекомбинацией. Указанные процессы приводят к изменению электродинамических параметров углеродного композита, его комплексной диэлектрической и магнитной проницаемости в исследуемом частотном диапазоне 1–200 ГГц. Происходит это при изменении электропроводности композита, а также за счет влияния наведенного напряжения на индуктивность углеродных нитей, импедансы интерфейсов между различными структурными элементами углеродного композита. Особенно чувствительны к изменению зарядовых свойств композита импедансы интерфейсов между его различными структурными элементами, что приводит к изменению резонансных частот LRC контуров, которыми описываются такие импедансы, Также подобную чувствительность проявляют параметры других реактивных элементов, сформированных углеродными нитями, емкостями воздушных (вакуумных) промежутков и активными сопротивлениями структурных элементов композита. Установлено, что формирование заряда и наведенное напряжение может привести к существенному изменению электродинамических параметров, которые весьма чувствительны к вариации импедансов и параметров RLC контуров, в случае если происходит изменение резонансных частот контуров, повлекших за собой существенное изменение комплексной диэлектрической и магнитной проницаемости композита. В конечном итоге как показали наши оценки это повлияет на коэффициенты отражения, пропускания и поглощения, изменит их значения. Также следует учитывать наличие остаточных напряжений и заряда, который не может быть удален в процессе его стекания. Данное обстоятельство должно учитываться при определении коэффициентов отражения, поглощения и пропускания, которые восстанавливают свои первоначальные значения после окончания ЭМИ за время релаксации.

Список литературы

1. Kumar R. [et al]. Carbon. 2021. Vol. 177. P. 304.

МЕТОДИКА КОНФИГУРАЦИИ И ТЕСТИРОВАНИЯ ЗАЩИТЫ ОТ DDOS-АТАК НА МЕЖСЕТЕВОМ ЭКРАНЕ FORTIGATE

М.К. До

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

DDoS (Distributed Denial of Service) – кибератака, направленная на перегрузку серверов или сетей, целью которой является снижение скорости обработки запросов пользователей [1]. В зависимости от типа атаки DDoS подразделяют на TCP SYN flood, UDP flood, Ping flood и другие. DDoS-атака, в отличии от DoS-атаки, является распределенной, и осуществляется посредством использования большого количества компьютеров, находящихся под управлением программного обеспечения, называемого ботнетом. Каждый компьютер в ботнете отправляет запросы на сервер или сеть, что приводит к перегрузке ресурсов и отказу обработки новых запросов. Система защиты Fortigate DoS protection осуществляет поиск конкретных аномалий трафика с целью идентификации опасного трафика, который может быть частью DoS или DDoS-атаки [2]. Под аномалиями трафика понимается трафик, который может включать в себя TCP SYN flood, UDP flood, ICMP flood, сканирование TCP-портов, атаки на TCP, UDP и ICMP-сессии. Трафик, который идентифицируется как часть атаки DoS, блокируется, при этом соединения от законных пользователей обрабатываются.

На основе изучения принципов конфигурации системы защиты Fortigate DoS protection [2] была составлена методика, которая включает следующие этапы:

1. Подключение к веб-интерфейсу межсетевого экрана FortiGate.
2. Создание политики DoS.
3. Конфигурация сенсоров для ICMP, UDP, TCP трафика.
4. Активация политики DoS в политике межсетевого экрана.

Проверка правильности работы политики IPv4 DoS была осуществлена посредством использования утилиты hping3. В результате было установлено, что атака DoS успешно блокируется и отображается в Log-файлах.

Таким образом, посредством реализации разработанной методики и проверки правильности работы политики IPv4 DoS было установлено, что за счет включения защиты от DoS в политику интерфейса межсетевого экрана Fortigate в первую очередь проверяется входящий пакет. Благодаря такому раннему обнаружению политика DoS является очень эффективной защитой, которая использует мало ресурсов. При обнаружении DoS атаки пакеты блокируются еще до проверки другими политиками (антивирус, веб-фильтр и др.). Также необходимо отметить, что составными элементами политики DoS являются сенсоры DoS, которые проверяют сетевой трафик, поступающий на интерфейс, на наличие аномальных параметров, указывающих на атаку.

Список литературы

1. DDoS-атака // АО «Лаборатория Касперского» [Электронный ресурс]. – 2023. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/ddos-distributed-denial-of-service-attack/. – Дата доступа: 23.04.2023.

2. Admin Guides FortiGate/FortiOS 7.0.11 // Fortinet [Электронный ресурс] – 2023. – Режим доступа: https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/954635/getting-started. – Дата доступа: 23.04.2023.

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УПРАВЛЯЮЩИХ СИСТЕМ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

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

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

Автоматизированная система управления технологическими процессами АЭС (АСУ ТП АЭС) играет основную роль в обеспечении безопасной эксплуатации одного из наиболее сложных объектов управления, каким является АЭС. Управляющие системы современных АЭС, которые проектировались и сооружались уже в 21 веке, от аналоговых методов и средств управления перешли к цифровым (дискретным) методам и средствам. Цифровые технологии используются и при модернизации существующих АЭС. Однако использование компьютерной техники и цифровых технологий в управляющих системах АЭС, как называется АСУ ТП АЭС в нормативных правовых актах (НПА), регулирующих ядерную безопасность в Республике Беларусь, сделало эти системы уязвимыми для кибератак. Исторически при проектировании управляющих систем АЭС не уделялось должного внимания компьютерной безопасности в связи с тем, что аналоговые системы являются неуязвимыми для кибератак из-за их жесткой реализации, а также в связи с отсутствием коммуникации с внешними сетями и системами.

Кибератаки на управляющие системы АЭС, использующие цифровые технологии, могут поставить под угрозу ядерную безопасность АЭС и привести к неприемлемым радиологическим последствиям. В связи с чем ряд документов МАГАТЭ [1, 2] определяют необходимость защиты компьютерных систем, включая управляющие системы, объектов использования атомной энергии. Технические руководящие материалы [3], опубликованные в 2018 году в Серии изданий МАГАТЭ по физической ядерной безопасности, содержат рекомендации по применению мер, обеспечивающих компьютерную безопасность в отношении управляющих систем АЭС, на всех этапах их жизненного цикла от проектирования до модернизации. Документ 2020 года [4], изданный в Серии МАГАТЭ по ядерной энергии, включает описание большого числа методов защиты управляющих систем АЭС от кибератак для всех этапов жизненного цикла, а также рассматривает их основные достоинства и недостатки.

Анализ НПА по обеспечению ядерной и радиационной безопасности Республики Беларусь показывает необходимость актуализации их в части установления требований по обеспечению компьютерной безопасности управляющих систем АЭС с целью их гармонизации с документами МАГАТЭ.

Список литературы

1. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series No. 13. Recommendations. – Vienna, IAEA, 2011. 57 p.

2. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T (Rev. 1). Technical Guidance. Vienna, IAEA, 2021. 140 p.

3. Computer Security of Instrumentation and Control Systems at Nuclear Facilities. IAEA Nuclear Security Series No. 33-T. Technical Guidance. – Vienna, IAEA, 2018. 58 p.

4. Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants. IAEA Nuclear Energy Series No. NR-T-3.33. Technical Reports. Vienna, IAEA, 2020. 72 p.

ЛЕГИРОВАНИЕ ГРАФЕНА ХЛОРИДАМИ ЩЕЛОЧНЫХ МЕТАЛЛОВ

Е.А. Дронина, Н.Г. Ковальчук

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

Графен – двухмерный материал, обладающий рядом исключительных свойств таких как, высокая подвижностью носителей заряда, высокая теплопроводность, и баллистическая проводимость при комнатных температурах. Одним из факторов, ограничивающих широкое применение графена в электронных приложениях, является отсутствие в нем запрещенной зоны. Для создания запрещенной зоны в графене и для управления его электрическими свойствами применяются различные методы легирования. Зачастую легирование графена требует высокотемпературного нагрева образца, что в свою очередь приводит к разрушениям углеродных связей [1].

В данной работе предложен низкотемпературный метод легирования образцов графена с помощью хлоридов щелочных металлов. В качестве легирующего материала были использованы калий хлористый (KCl), кальций хлористый ($CaCl_2$) и натрий хлористый (NaCl). Из каждого материала был приготовлен 1 М водный раствор, который, впоследствии, наносился на структуру графен/SiO_2/Si методом центрифугирования при скорости вращения 1000 об/мин в течение 30 секунд. Затем все образцы помещались в муфельную печь при температуре 40°C на 30 минут. Результаты исследования методом картирования спектров комбинационного рассеяния света позволили установить, что легирование водным раствором KCl и $CaCl_2$ как однослойного, так и малослойного (~ 4 слоя) графена, приводит к росту значений концентрации носителей заряда в графене. Вместе с тем, при легировании графена водным раствором NaCl явного изменения в концентрации носителей заряда по сравнению с исходной структурой (графен/SiO_2/Si) не наблюдается. Показано, что предложенный способ позволяет легировать как однослойный, так и малослойный графен с незначительным изменением дефектности и уменьшением прозрачности не более чем на 5%.

Список литературы

1. Kwon K. C. [et al.] Role of metal cations in alkali metal chloride doped graphene. The Journal of Physical Chemistry C. 2014. Vol. 118, No. 15. P. 8187–8193.

СИСТЕМА АУТЕНТИФИКАЦИИ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОЙ МОДЕЛИ БЕЗОПАСНОСТИ RBA

С.А. Зайкова

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

Для ИТ-компаний и организаций, занятых разработкой программных средств и систем несанкционированный доступ к конфиденциальной информации может привести к утечке данных и потере доверия клиентов, что может существенно повлиять на их прибыль. Учитывая важность защиты личной и конфиденциальной информации, крайне важно иметь надежные системы для аутентификации пользователей и обеспечения доступа к конфиденциальной информации только уполномоченных лиц. Аутентификация на основе риска (RBA, Risk-Based Authentication) – это метод, который использует алгоритмы искусственного интеллекта и машинного обучения для оценки уровня риска запроса на вход в систему на основе широкого спектра информации о пользователе и запросе. Информация может включать местоположение

пользователя, его устройство, историю просмотров и поведение. Модели безопасности аутентификации на основе риска – это новый тип метода аутентификации, который направлен на устранение ограничений традиционных методов аутентификации. Такие модели работают путем анализа различных факторов риска для определения уровня риска, связанного с конкретной попыткой аутентификации [1, 2].

Новая система может определить соответствующий уровень аутентификации, необходимый для предоставления доступа к конфиденциальной информации сотрудников ИТ-компании. Кроме того, она может также обеспечить более высокий уровень удобства для администратора и пользователя, минимизируя количество попыток аутентификаци, и уменьшая неудобство традиционных методов (таких как пароли, секретные вопросы и маркеры). Анализируя различные факторы риска, аутентификация на основе риска обеспечивает точную оценку риска, связанного с конкретной попыткой аутентификации. Это позволяет реагировать на потенциальные угрозы безопасности различного типа, включая фишинг. Предлагаемые программные инструменты обеспечивают более высокий уровень безопасности, чем традиционные методы аутентификации, которые уязвимы для подобных атак. Разработка может улучшить пользовательский опыт и повысить степень принятия пользователем системы аутентификации. Аутентификация на основе риска позволяет осуществлять динамическую аутентификацию, которая может регулировать уровень необходимой аутентификации в зависимости от оцененного уровня риска, это повышает безопасность и гибкость системы. Согласно проведенному исследованию, аутентификация RBA обеспечивает более совершенный и безопасный метод аутентификации по сравнению с традиционными методами аутентификации, а также обеспечивает более высокий уровень удобства.

Список литературы

1. Зайкова С.А. Комплексная защита конфиденциальной информации // Информационно-телекоммуникационные системы и технологии. ИТСиТ-2017: материалы Всеросс. научн.-практ. конф., Кемерово, 12–13 октября 2017 г. С. 217–218.

2. Нестерович Е.А., Зайкова С.А. Обеспечение безопасного хранения и защиты информации базы данных от несанкционированного доступа // Технические средства защиты информации: тез. докл. XV Белорусско-российской науч.-техн. конф., Минск, 6 июня 2017 г. С. 64–65.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАНАЛА ЗАЩИЩЕННОЙ СВЯЗИ

Ю.В. Злобина

Частное предприятие «ВитЭлектро», Гродно, Республика Беларусь

На сегодняшний день широкое распространение использования получили волоконно-оптические каналы связи, для описания которых целесообразно использовать математическую модель дискретного канала связи.

Системы связи с возможностью обеспечения конфиденциальности передаваемой информации подразделяются на одноключевые (симметричные), двухключевые (ассиметричные) и системы на основе гибридного метода шифрования данных [1].

Математическая модель защищенной связи позволяет формализовать процессы обмена информацией и определить уязвимости системы, включает в себя описание криптографических протоколов, алгоритмов шифрования и методов аутентификации, позволяет проводить анализ устойчивости системы к различным атакам, включая перехват информации, подделку данных и внедрение вредоносного программного обеспечения. Математическая модель защищенной связи может быть использована для

сравнительного анализа пропускной способности системы передачи конфиденциальных данных между легитимными пользователями без наличия несанкционированного пользователя в системе связи с обеспеченной конфиденциальностью передаваемой информации и при его наличии.

Построение математической модели квантового канала связи строится на том, что передача информации в детекторе осуществляется двоичными символами («0» и «1») [2]. При передаче символа «1» одноквантовый оптический импульс передается в волокно, а при передаче символа «0» – излучение отсутствует. Приемный модуль выполняется в виде счетчика фотонов, который регистрирует фотоны оптического излучения в течение времени передачи синхроимпульса, генерируемого на передающей стороне на время передачи каждого символа. При отсутствии несанкционированного пользователя в системе численные значения вероятностей приема символов «0» и «1», которые определяют вероятность ошибки передачи данных, будут равны.

С помощью построения графов вероятностей получаются выражения, с помощью которых определяется пропускная способность на участке между легитимными пользователями и на участке между легитимной передающей стороной и нелегитимным пользователем.

В присутствии несанкционированного пользователя в системе вероятность ошибки при приеме данных не равна нулю. Это вызвано тем, что вероятность выхода фотона излучения из оптического волокна в результате съема данных при помощи макроизгиба волокна зависит от его диаметра [3]. С уменьшением диаметра макроизгиба волокна увеличивается пропускная способность канала утечки информации. С ростом длины волны оптического излучения увеличивается значение пропускной способности канала утечки информации.

Выражения для оценки пропускной способности на участке между легитимными пользователями учитывают вероятность несанкционированного вывода мощности излучения из оптического волокна, а также параметры счетчика фотонов: вероятность, появления темновых импульсов, квантовую эффективность регистрации

Список литературы

1. Дмитриев С.А. Волоконно-оптическая техника: современное состояние и новые перспективы. М., 2010.

2. Клюев Л.Л. Теория электрической связи. Минск: Техноперспектива, 2008. 423 с.

3. Тимофеев А. М. Оценка влияния интенсивности оптического сигнала на вероятность ошибочной регистрации данных в однофотонном канале связи // Информатика. 2021. Т. 18, № 2. С. 72–82.

ИДЕНТИФИКАЦИЯ ЧЕЛОВЕКА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ НА ОСНОВЕ АНАЛИЗА ПОЧЕРКА

А.И. Калько

Учреждение образования «Барановичский государственный университет», Барановичи, Беларусь

Анализ почерка используется многие годы как средство судебной экспертизы для идентификации людей. Это происходит потому, что каждый человек имеет уникальный стиль письма, отражающий его личность и физиологию. Анализ почерка может использоваться для идентификации людей на основе различных характеристик, таких как ширина линии, давление, угол пера и форма букв. Эти характеристики стабильны и постоянны в различных образцах письма, что делает их идеальными для целей идентификации.

В данном тезисе предлагается система, использующая анализ почерка в режиме реального времени для идентификации человека.

Система состоит из двух частей: устройства для захвата почерка и алгоритма анализа почерка. Устройство для захвата почерка представляет собой цифровую ручку, которая захватывает почерк при его написании. Цифровая ручка подключена к компьютеру, который выполняет алгоритм анализа почерка в режиме реального времени.

Алгоритм анализа почерка использует техники машинного обучения для анализа захваченного почерка и сравнения его с образцами почерка в базе данных. Алгоритм обучается на образцах почерка каждого человека, который планируется идентифицировать, и на основе этих образцов строится уникальная модель почерка каждого человека. Эта модель используется для идентификации человека в режиме реального времени.

Одним из ключевых преимуществ системы является возможность быстрой идентификации в режиме реального времени. Пользователь может написать свой образец почерка, и в течение нескольких секунд система сравнит его с образцами в базе данных и определит, кто этот пользователь [1].

Проведен ряд экспериментов для оценки производительности и точности нашей системы. Для этого мы использовали набор данных с образцами почерка от нескольких человек и проверили, как быстро и точно система идентифицирует каждого человека.

Результаты показали, что система имеет высокую точность и быстродействие [2]. Система успешно идентифицировала каждого человека в течение нескольких секунд после написания образца почерка. Более того, система обнаруживает попытки мошенничества, такие как подделка почерка.

В данном тезисе представлена система для идентификации человека в режиме реального времени на основе анализа почерка [3]. Система имеет высокую точность и быстродействие, что делает ее идеальной для применения в различных приложениях, таких как системы безопасности, контроль доступа и банковские транзакции.

Однако, система имеет некоторые ограничения, в том числе необходимость наличия базы данных образцов почерка каждого человека, которого необходимо идентифицировать. Также, необходимость использования цифровой ручки для захвата почерка может быть проблемой для пользователей, не знакомых с этой технологией.

В целом, система представляет собой перспективное решение для идентификации человека в режиме реального времени на основе анализа почерка. Дальнейшие исследования могут расширить возможности системы, например, разработать алгоритмы, которые бы позволили идентифицировать человека по нескольким образцам почерка, снятым в разное время и в различных условиях.

Список литературы

1. Сандруцкий Д.И., Колдушко С.Д., Калько А.И. Применение криптографических систем при создании мессенджера // Студенческий. 2017. № 16(16). С. 14–16.

2. Наранович О.И., Калько А.И. Автоматизированная система сегментации изображения // Актуальные проблемы и пути развития энергетики, техники и технологий: сб. трудов VII Междунар. науч.-практ. конференции, Балаково, 23 апреля 2021 г. Т. 1. С. 217–222.

3. Программный компонент модуля обучения широких нейронных сетей для идентификации пользователя: свидетельство Российской Федерации о государственной регистрации программы для ЭВМ № 2022618776 / Д.А. Трокоз, И.Г. Сергина, А.И. Калько [и др.]; заявл. 18.05.2022; опубл. 27.05.2022.

СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Н.О. Карнильчик

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

Было проведено сравнение блочного алгоритма шифрования информации ГОСТ 28147-89 с 256-битовым ключом и 32 раундами на основе сети Фейстеля с алгоритмами защиты информации ГОСТ Р 34.10-2012 с использованием схемы Миягучи-Пренеля и ГОСТ Р 34.12-2018. С точки зрения безопасности ГОСТ 28147-89 считается чрезвычайно надежным и проверялся экспертами на протяжении многих лет. Он использует алгоритм с симметричным ключом, что означает, что один и тот же ключ используется как для шифрования, так и для дешифрования.

Был рассмотрен блочный алгоритм шифрования ГОСТ 28147-89, который был усовершенствован в алгоритме стандарта 1994 г. Описано теоретическое представление сети Фейстеля и приведена ее схема в виде графического способа описания алгоритма. Реализован блочный алгоритм шифрования с 256-битовым ключом и 32 раундами на основе сети Фейстеля для платформы «Windows», язык реализации C++20. Так же реализован алгоритм шифрования информации стандарта 1994 с использованием блочного алгоритма ГОСТ 28147-89 с 256-битовым ключом и 32 раундами на основе сети Фейстеля. Приведены различия реализаций алгоритмов шифрования информации из стандартов 2012 года с использованием схемы Миягучи–Пренеля и 2018.

Продемонстрировано применение отечественного блочного алгоритма шифрования информации и теоретической криптостойкости, и оценена скорость с разными размерами ключей и сетей Фейстеля: с 256-битовым ключом и 64 раундами на сети Фейстеля: с 256-битовым ключом и 32 раундами на сети Фейстеля, с 128-битовым ключом и 32 раундами на сети Фейстеля, с 64-битовым ключом и 32 раундами на сети Фейстеля и с 64-битовым ключом и 16 раундами на сети Фейстеля. В данной работе изучены возможности ускорения и оптимизации алгоритма шифрования ГОСТ 28147-89 [1–3].

Список литературы

1. Ищукова Е.А., Панасенко С.П., Романенко К.С. [и др.] Криптографические основы блокчейн-технологий. М.: ДМК Пресс, 2022. 302 с.

2. Рубин Ф. Криптография с секретным ключом. М. ДМК Пресс, 2022. 386 с.

3. Омассон Ж.-Ф. О криптографии всерьез. М.: ДМК Пресс, 2021. 328 с.

АППАРАТНАЯ РЕАЛИЗАЦИЯ МОДУЛЯ ПРЕОБРАЗОВАНИЯ 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. Данная функция используется для проверки целостности данных, а также в рамках других криптографических алгоритмов и протоколов в различных приложениях, связанных с защитой информации. Поскольку функция SHA-512 использует в своей работе 64-битные слова, она является самой сильной среди функций семейства SHA-2 с точки зрения устойчивости к коллизиям и взлому. Чтобы соответствовать ограничениям

реального времени в современных приложений, возникает необходимость высокопроизводительных аппаратных реализаций алгоритма SHA-512. Эти реализации должны быть нацелены на обеспечение требуемых показателей пропускной способности и пропускной способности/объема ресурсов с помощью соответствующих методов оптимизации. В докладе рассматривается аппаратная реализация модуля преобразования хэш-функции SHA-512 на базе FPGA.

Поскольку критический путь алгоритма SHA-512 находится в раунде преобразования, основная оптимизация относится к этому модулю. Модуль преобразования реализуется с использованием набора одновременно применяемых методов оптимизации [1]. Эти методы включают как методы алгоритмического уровня (развертывание цикла, предварительное вычисление, ресинхронизация), так и методы схемного уровня, такие как перераспределение ресурсов и использование специальных модулей сумматоров с сохранением переноса (CSA).

Основной особенностью рассматриваемой реализации заключается в применении развертывания цикла в алгоритме SHA-512 [1]. При этом, как показано в [1], наилучшее значение показателя пропускная способность/объем ресурсов достигается при коэффициенте развертывания, равном 2. В этом случае два последовательных раунда объединяются вместе, образуя один новый раунд, который реализует одну операцию за итерацию, где значения рабочих переменных a(t+1) - h(t+1)) вычисляются на основе значений a(t-1) - h(t-1). При таком объединении критический путь одной итерации алгоритма становится длиннее, однако при этом число итераций уменьшается с 80 до 40.

На следующем этапе [1] осуществляется перераспределение компонентов архитектуры и использование сумматоров с сохранением переноса CSA, что приводит к уменьшению задержки критического пути.

Характеристики реализации по отчету средств синтеза пакета Vivado 2021.2 для кристалла FPGA Virtex UltraScale+ xcu250-figd2104-2L-e: 832 триггеров секций, 1051 просмотровая таблица (LUT), тактовая частота – 500 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. P. 70–82.

АППАРАТНАЯ РЕАЛИЗАЦИЯ ФУНКЦИИ SCRYPT НА FPGA

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

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

Функция Scrypt [1] предназначена для формирования секретного ключа на основе секретной строки (пароля). Характерной особенностью алгоритма функции является необходимость использования значительного объема памяти и последовательный характер большей части вычислений, что усложняет оборудование для криптоанализа путем перебора возможных значений паролей или ключей (brute-force attack). Данная функция используется, в частности, при доказательстве выполненной работы (proof of works) в криптовалюте Litecoin и в системе хранения резервных копий Tarsnap.

Укрупненно алгоритм функции Scrypt применительно к криптовалюте Litecoin заключается в последовательном выполнении следующих функций: PBKDF2 (P = 80 байт, S = 80 байт, c = 1, $dkLen$ = 128) [2], ScryptROMix (r = 1, B = 128 байт, N = 1024)

и второй функции PBKDF2 (P = 80 байт, S = 128 байт, c = 1, $dkLen$ = 32 байта). Внутри функции ScryptROMix используется функция ScryptBlockMix [1]. Первое 1024-кратное выполнение функции ScryptBlockMix используется для заполнения блока памяти из 1024 128-разрядных ячеек. При втором 1024-кратном выполнении функции ScryptBlockMix содержимое этих ячеек, выбранных в псевдослучайном порядке, используется для операции xor с результатом функции ScryptBlockMix. При практической реализации алгоритма можно было обойтись без памяти, вычисляя требуемое значение переменной, соответствующее некоторой ячейке памяти, прямо внутри второй группы циклов ScryptBlockMix, однако это потребует значительного времени из-за последовательного характера вычисления значений формируемого массива (следующий элемент вычисляется на основе значения предыдущего). Внутри функции ScryptBlockMix для получения псевдослучайных чисел используется хэш-функция Salsa20/8 [3].

Исходя из анализа вычислительного процесса указанных функций выбраны следующие архитектуры для их аппаратной реализации: функция Salsa20/8 реализуется параллельно-итеративной архитектурой, ScryptBlockMix и ScryptROMix реализуются итеративной архитектурой, PBKDF2 реализуется итеративно-конвейерной архитектурой. На верхнем уровне реализации функции Script используется конвейерная архитектура. Была выполнена реализация данной системы на базе отладочной платы VC707, использующей базовый кристалл FPGA XC7VX485T-2FFG1761. Аппаратные затраты после процедуры синтеза средствами ISE 14.7: 14211 Slice Registers, 16246 Slice LUTs, 32 BRAM. Тактовая частота – 179 МГц. Выполнение PBKDF2_1 занимает 1685 тактов, ScryptROMix – 46079 тактов, PBKDF2_2 – 281 такт.

Предложенная система может использоваться в качестве ядра майнера криптовалюты Litecoin.

Список литературы

1. RFC7914. The scrypt Password-Based Key Derivation Function [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc7914. – Дата доступа: 28.04.2023.

2. RFC2898. PKCS #5: Password-Based Cryptography Specification. Version 2.0 [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc2898. – Дата доступа: 28.04.2023.

3. Daniel J. Bernstein. Salsa20 specification [Электронный ресурс]. – Режим доступа: http://cr.yp.to/snuffle/spec.pdf. – Дата доступа: 28.04.2023.

ШИРОКОПОЛОСНЫЕ ПОГЛОЩАЮЩИЕ ЭКРАНЫ НА ОСНОВЕ ГРАДИЕНТНОЙ СТРУКТУРЫ ИЗ УГЛЕРОДНОГО ВОЙЛОКА

И.А. Кашко, В.В. Филиппов, Н.А. Певнева, В.А. Лабунов

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

В настоящее время актуальны работы в области создания и совершенствования высокоэффективных широкополосных радиопоглощающих материалов. Специфика взаимодействия углеродного войлока с электромагнитным излучением (эффект аномально большого поглощения и рассеяния СВЧ-излучения очень тонкими проводящими волокнами) обуславливает его использование в конструкциях экранов электромагнитного излучения [1].

Для слабоотражающего широкополосного поглотителя электромагнитного излучения оптимальной конструкцией является поглотитель градиентного типа.

В поглотителе градиентного типа используется постепенное изменение от проводимости близкой к нолю (проводимость свободного пространства) на поверхности падения поглотителя до более высокой проводимости на его задней (тыльной) стороне. Это постепенное изменение может быть достигнуто как изменением проводимости углеродных волокон войлока, так и изменением его плотности.

В качестве основы материала для ослабления электромагнитного излучения использовался углеграфитовый войлок «Карбопон В-10М и Карбопон В-22М» на основе карбонизированного вискозного (натурального) волокна, промышленно выпускаемый белорусским предприятием ОАО «Светлогорскхимволокно». Основной особенностью войлока данных марок является температура повторного отжига, при которой достигается волновое сопротивление близкое к волновому сопротивлению воздуха. Данная особенность позволяет электромагнитному излучению с минимальным отражением проходить границу воздушная среда/углеродный войлок. Технологический процесс предприятия позволяет получать войлок толщиной 2мм. Модифицируя каждый слой войлока и сшивая их вместе, удается изготовить широкополосный экран градиентного типа с малым отражением.

Изменение сопротивления углеродного войлока осуществлялось нами с помощью двух методов. Для уменьшения сопротивления использовался высокотемпературный отжиг в среде аргона или азота. При этом, чем выше была температура и длительность отжига, тем сильнее оказывалось воздействие на углеродный материал. Для увеличения сопротивления углеродного войлока использовалось электрохимическое окисление на аноде в водном растворе медного купороса и серной кислоты (H_2O – 1 кг, $CuSO_4$ – 100 г, H_2SO_4 – 50 г) при плотности тока 10 А/дм^2.

Изготовленные из углеродного войлока градиентные экраны толщиной в 6 мм при измерении коэффициента отражения в ближней зоне электромагнитного поля со стальной отражающей пластиной позади исследуемого образца показывали значения в –5,0 дБ в диапазоне 1,0–2,0 ГГц, –10,0 дБ в диапазоне 2,0–4,0 ГГц, –15,0 дБ в диапазоне 4,0–8,0 ГГц, –20,0 дБ в диапазоне 8,0–12,0 ГГц и –15,0 дБ в диапазоне 12,0–18,0 ГГц.

Список литературы

1. Kuzmichev V.M., Kokodiy N.G., Safronov B.V. [et al.]. Factor of absorption efficiency of a thin metal cylinder in the microwave range // J. Commun. Technol. Electron. 2003. Vol. 48, no. 11. P. 1349–1351.

ПОКРЫТИЕ НА ОСНОВЕ 2D ЧАСТИЦ Ti_3C_2 ДЛЯ ИСПОЛЬЗОВАНИЯ В ЭЛЕКТРОМАГНИТНЫХ ЭКРАНАХ СВЧ ДИАПАЗОНА

И.А. Кашко[1], В.В. Филиппов[1], Н.А. Певнева[1], В.А. Лабунов[1], Е.А. Оводок[2], И.А. Авдейчик[2], С.К. Позняк[2], Т.В. Гаевская[2]

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

[2]*Учреждение БГУ «Научно-исследовательский институт физико-химических проблем», Минск, Беларусь*

Разработка систем защиты от широкополосного электромагнитного излучения включает в себя использование не только специальных элементов конструкций, но и подбор подходящих материалов и покрытий [1].

В качестве защитных СВЧ поглощающих экранов широко используются покрытия из различных модификаций углеродных материалов. Однако они, как правило, имеют довольно высокий уровень отраженного излучения. Различные возможности для защиты от СВЧ излучения возникают при использовании сравнительно нового материала – максенов (MXenes). В работе исследовано подавление СВЧ как прошедшего, так и отраженного излучения защитными покрытиями на основе тонких (0,3–0,8 мкм) слоев, составленных из максеновых 2D частиц в виде чешуек.

MXene получали обработкой MAX фазы (Ti_3AlC_2) в растворе LiF + HCl. При этом происходило удаление атомов Al из структуры MAX фазы и формирование 2D MXene частиц. Полученные 2D MXene частицы имели латеральный размер 1,0–3,0 мкм. На основе синтезированных частиц MXene изготавливали устойчивый водный коллоидный раствор с концентрацией частиц 5 г/л. Формирование тонкого (менее 1,0 мкм) покрытия, осуществлялось методом распыления коллоидного раствора MXene на подложку из стеклопластика с последующей сушкой образцов при 60 ºС. Поверхностное сопротивление серии изготовленных образцов находилось в диапазоне 100,0–1000,0 Ом/кв.

Измерение коэффициента отражения и ослабления электромагнитного излучения образцов, в диапазоне частот 8–12 ГГц, выполнялось волноводным методом с использованием векторного анализатора цепей Anritsu MS4644B и волноводно-коаксиальных переходов ВКП-23х10. Характеристики отражения и пропускания образцов были измерены в ближней зоне электромагнитного поля волноводно-коаксиального перехода. При измерении коэффициента отражения использовался стальной отражающий экран позади исследуемого образца.

Лучший результат (наименьший коэффициент отражения) продемонстрировали образцы с поверхностным сопротивлением пленки 830,0–990,0 Ом/кв. Он составил менее –5,0 дБ с минимумом от –22,0 до –24,0 дБ в районе 10,4 ГГц. По мере роста толщины пленок и уменьшения их сопротивления отражение электромагнитного излучения от границы воздух–покрытие на основе максенов возрастало. Пропускание же этих образцов, наоборот, оказалось наибольшим. Наименьшее пропускание –5,0 дБ и менее имел образец с наименьшим сопротивлением 105,0 Ом/кв. Таким образом, изменяя толщину покрытия и его сопротивление, можно регулировать отражение / пропускание, добиваясь его оптимального соотношения для тех или иных задач.

Список литературы

1. Аполлонский С.М., Горский А.Н. Расчеты электромагнитных полей. М.: Маршрут. 2006. 992 с.

ПРИМЕНЕНИЕ ДВУХУРОВНЕВЫХ ТЕСТОВ ДЛЯ ОЦЕНКИ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ В ДИАПАЗОНЕ РАБОЧИХ ТЕМПЕРАТУР

Н.Г. Киевец

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

Для различных приложений широко применяются электронные пластиковые карты (ЭПК) со встроенными физическими генераторами случайных чисел (ГСЧ), вырабатывающими случайные последовательности (СП). Поскольку СП используются для создания криптографических ключей и от их статистических свойств зависит безопасность передаваемых данных, актуальной является задача оценки качества работы ГСЧ ЭПК.

В связи с тем, что ЭПК эксплуатируются при различных температурах, представляет интерес проверка качества работы ГСЧ ЭПК во всем диапазоне рабочих температур от 0º до 50º в соответствии со стандартом [1].

Была поставлена задача выполнить оценку качества работы ГСЧ пяти ЭПК с микроконтроллерами К5004 ВЕ2 при температурах 0º, 21º и 50º с использованием методики двухуровневого тестирования СП [2].

Для решения поставленной задачи от ГСЧ каждой ЭПК получено 12 тыс. СП длиной 256 бит – по 4 тыс. СП при каждой из трех температур. Далее выполнено двухуровневое тестирование СП каждого массива из 4 тыс. СП. В эксперименте использовались частотный тест, тест на подпоследовательности одинаковых бит, тест на самые длинные подпоследовательности единиц в блоках, тест аппроксимированной энтропии и тест кумулятивных сумм.

Полученные результаты тестирования показали высокое качество работы ГСЧ ЭПК во всем диапазоне рабочих температур и пригодность ГСЧ ЭПК для генерации криптографических ключей длиной 256 бит.

Список литературы

1. Карточки идентификационные. Карточки с интегральными схемами контактные. Ч. 1: СТБ 1211.1-2000 (ИСО/МЭК 7816-1:1998). Введ. 01.07.2000. Минск: Госстандарт, 2000. 4 с.

2. Киевец Н.Г., Корзун А.И. Двухуровневое тестирование случайных последовательностей длиной 128 и 256 бит // Доклады БГУИР. 2017. № 3 (105). С. 78–83.

ПЛОЩАДЬ ПОД КРИВОЙ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ОШИБКИ ПРИ НАБЛЮДЕНИИ ВЕКТОРОВ ПЕРЕХОДОВ

И.П. Кобяк

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

Рассмотрен метод наблюдения лебеговской меры векторов переходов в случайном процессе с точки зрения значений вероятности ошибки при формировании точечных оценок. На основе алгоритма конечных разностей для комбинаторных моментов, входящих в состав производящей функции (ПФ) получено соотношение, характеризующее площадь под интегральной кривой данного распределения. С учетом указанного результата сформированы ряды для каждого *i*-го члена функции, определяющие значение соответствующего слагаемого через алгебраическую сумму приращений $(i-k)$-х моментов. Общее суммирование всех членов ПФ позволило получить результаты в форме нестандартных рядов, вычисление которых было выполнено для конечного, однако достаточно большого числа слагаемых то есть при длине выборки $n>>1$. Это позволило упростить вычисления рядов с использованием формул арифметической прогрессии. Причем расчет функции для конкретного значения $p=3/16$, то есть для максимального значения вероятности наблюдения векторов переходов заданного вида, в любых *r*-разрядных последовательностях, дало результат: $P_{err}=99/128$. Соответственно, для параметра p^2 суммирование рядов привело к дроби: 297/2048. Однако, использование результатов современной теории вероятностей показало, что простое суммирование полученных значений невозможно, в связи с полиномиальным представлением параметра *p*. Так, в работе [1] получено соотношение, определяющее удельный вес вероятности *p* и вероятности p^2 в соответствующем вероятностном полиноме. В связи с этим

для полученных сумм были рассчитаны требуемые коэффициенты, а общий результат или площадь под интегральной кривой функции распределения была определена соотношением $P_{ifc} = Mo + (0{,}65561)\deg(N >> n),\ N \to \infty,$ где Mo-мода распределения.

Список литературы

1. Кобяк И.П. Асимптотика для вероятности пропуска ошибки при наблюдении векторов переходов // BIG DATA and advanced analytics 2021: сб. материалов 7-й междунар. науч.-практ. конф., Минск, 19–20 мая 2021 г. С. 328–335.

ПРОБЛЕМНЫЕ ВОПРОСЫ ИНТЕГРАЦИИ PSIM-СИСТЕМ

А.Н. Коваленко
Учреждение образования «Военная академия Республики Беларусь», Минск, Республика Беларусь

PSIM – Physical Security Information Management (управление информацией о физической безопасности) – интеллектуальная программная платформа для сбора данных из разнородных источников, управления с помощью одного комплексного интерфейса пользователя с целью повышения безопасности и эффективности рабочих процессов. PSIM является комплексной системой безопасности, которая является отдельной системой и выступает надстройкой над системами безопасности. Она собирает и обрабатывает информацию из разрозненных устройств обеспечения безопасности и информационных систем, после чего представляет ее в едином виде.

PSIM-система является ключевым элементом в обеспечении безопасности объектов различного уровня, начиная от крупных предприятий и заканчивая небольшими объектами.

Одной из основных проблем при внедрении PSIM является сложность интеграции с существующими системами безопасности и другими устройствами. Как правило, разные поставщики поставляют разные системы, которые работают на разных протоколах и с разными API (Application Programming Interface). Это может усложнить интеграцию, так как требуется использование дополнительных программных модулей и процедур для связи различных систем и устройств. Несмотря на то, что PSIM-система является стандартом для управления физической безопасностью, не существует унифицированных стандартов для ее реализации. Это приводит к проблемам совместимости, когда различные компании используют разные стандарты для своих систем, также это затрудняет интеграцию систем и усложняет обмен информацией между ними.

Внедрение PSIM-системы требует дополнительного обучения для персонала, ответственного за управление системой. Некоторые операции, такие как мониторинг и анализ данных, требуют специальных навыков и знаний. Отсутствие необходимых навыков и знаний приводит к некорректной настройке и использованию системы, что в свою очередь снижает эффективность системы.

Внедрение PSIM-системы является сложным и ответственным процессом, который требует внимательного и тщательного подхода. Если система правильно настроена и интегрирована с другими системами безопасности, она значительно повышает безопасность объектов различного уровня. Необходимо учитывать многие проблемные вопросы и решать их, чтобы получить максимальную эффективность от применения PSIM-системы.

Список литературы

1. PSIM – игра по правилам и без. [Электронный журнал]. – Режим доступа: https://ru-bezh.ru/journal-24-25/23416-psim-igra-po-pravilam-i-bez. – Дата доступа: 18.04.2023
2. Возможности современных систем управления информацией о физической безопасности (PSIM) [Электронный ресурс]. – Режим доступа: http://lib.secuteck.ru /articles2/ ip-security / vozmozhnosti - sovremennyh - sistem - upravleniya - informatsiey – o - fizicheskoy - bezopasnosti - psim. – Дата доступа: 18.04.2023.

ВЛИЯНИЕ АДГЕЗИИ ПРОЗРАЧНОГО ПРОВОДЯЩЕГО КОНТАКТА ИЗ ОДНОСТЕННЫХ УГЛЕРОДНЫХ НАНОТРУБОК НА ВОЛЬТ-АМПЕРНЫЕ ХАРАКТЕРИСТИКИ ФОТОЧУВСТВИТЕЛЬНОГО ЭЛЕМЕНТА НА ОСНОВЕ КРЕМНИЯ

Н.Г. Ковальчук, Е.А. Дронина

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

Одностенные углеродные нанотрубки (ОСУНТ) представляют большой интерес для применений в качестве прозрачного проводящего контакта в фотодетекторах, обусловленный как их уникальными физическими и химическими свойствами, так и возможностью относительно просто и технологично получить их на кремнии. При этом эффективность работы такого фотодетектора во многом зависит от качества контакта между ОСУНТ и материалом подложки. В данной работе представлено исследование влияния обработки поверхности одностенных углеродных нанотрубок этанолом на вольт-амперные характеристики (ВАХ) сформированного гетероперехода. ОСУНТ синтезировались методом химического парофазного осаждения (ХПО) на кремнии из раствора ферроцена/этанола [1]. Спектры комбинационного рассеяния света ОСУНТ содержат G-пики в G-полосе и пики радиально дыхательной моды (RBM). Это подтверждает одностенную природу полученных углеродных нанотрубок. Обработка в этаноле смещает положительную ветвь ВАХ сформированного гетероперехода в область больших токов. Такое изменение может быть объяснено значительным улучшением адгезии между ОСУНТ и кремнием, что, в свою очередь, влияет на эффективность работы устройства и приводит к улучшению параметров фоточувствительного элемента. Используя модифицированный метод Ченгов [2], который учитывает естественный оксид на границе ОСУНТ и кремний, получаем следующие параметры гетероперехода: фактор идеальности гетероперехода, $\eta \sim 4$, и высота барьера, $\varphi_B \sim 0{,}31$ эВ. Полученные параметры находятся в хорошем соответствии с данными, сообщаемыми в литературе.

Список литературы

1. Komissarov I. [et al.] Structural and magnetic investigation of single wall carbon nanotube films with iron based nanoparticles inclusions synthesized by CVD technique from ferrocene/ethanol solution // Physica Status Solidi. 2013. C 10.7-8. P. 1176–1179.
2. An Y. [et al.] Forward-bias diode parameters, electronic noise, and photoresponse of graphene/silicon Schottky junctions with an interfacial native oxide layer // Journal of Applied Physics. 2015. Vol. 118. 114307.

ИСПОЛЬЗОВАНИЕ FORTINAC ДЛЯ КОНТРОЛЯ УСТРОЙСТВ IOT В КОРПОРАТИВНОЙ СЕТИ

О.А. Кондрашук, Е.В. Константинова

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

Число типов и моделей устройств IoT (Internet of Things) стремительно расширяется с развитием рынка «интернета вещей». Если ранее необходимо было контролировать подключения компьютеров и мобильных устройств, то на сегодняшний день ассортимент оборудования, которое необходимо обнаружить и идентифицировать, существенно расширился. Неконтролируемое подключение устройств IoT в сети организации, увеличивают вероятность возникновения инцидентов безопасности. Поэтому необходимо вести учет и контроль каждого устройства в корпоративной сети.

Поскольку модернизация технологий затрагивает практически все отрасли человеческой деятельности, различные предприятия и организации, которые ранее не уделяли большого внимания информационной безопасности, сейчас вынуждены решать проблемы, возникающие в этой сфере. С этой целью была разработана система контроля доступа к сети FortiNAC (Network Access Control). Данная система обеспечивает обнаружение и профилирование всех устройств, подключающихся к корпоративной инфраструктуре, конфигурацию политик безопасности, а также реагирование на различные события и инциденты безопасности.

NAC-система компании Fortinet имеет трехуровневую архитектуру безопасности. На первом уровне происходит идентификация и профилирование всех подключившихся к сети устройств, в том числе IoT-устройств, идентификация установленного на них программного обеспечения. Информация, полученная на данном этапе используется для присвоения подключенному устройству прав доступа в соответствии с политикой безопасности, которая разработана для разных типов устройств с учетом таких параметров, как местонахождение, тип подключения, тип установленного программного обеспечения. Последний уровень архитектуры безопасности FortiNAC предусматривает использование средств, обеспечивающих реагирование на потенциально опасные изменения состояния подключенных устройств. В случае несоответствия параметров устройства установленным правилам, система контроля доступа к сети определяет возможные угрозы и автоматически снижает уровень доступа вплоть до полной блокировки. Такие же действия предпринимаются в случае использования VPN-соединения для доступа в сеть.

Таким образом решение FortiNAC минимизирует риски возникновения угроз безопасности в корпоративных сетях, связанные с незащищенными устройствами, которые осуществляют доступ к сети, обеспечивая полную видимость различных пользователей, устройств и приложений. Кроме того, система контроля доступа к сети FortiNAC является легко масштабируемой, позволяет расширять защиту большого количества устройств и устраняет необходимость ее развертывания на каждом объекте крупных предприятий.

Список литературы

1. Система контроля доступа к сети FortiNAC [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/reviews/FortiNAC#part2. – Дата доступа: 27.04.2023.

2. FortiNAC: управление доступом к сети [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Продукт:FortiNAC. – Дата доступа: 27.04.2023.

ОРГАНИЗАЦИЯ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ИЗ ОПТИЧЕСКОГО ВОЛОКНА С ИСПОЛЬЗОВАНИЕМ КОМПЕНСАЦИОННОГО СПОСОБА

О.В. Кочергина[1], В.И. Курмашев[2], Т.А. Матковская[3], Ю.В. Тимошков[4]

[1]*Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь*

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

В настоящее время для передачи информации широко применяются оптические волокна. Считается, что они имеют хорошую информационную безопасность [1–3]. Поскольку информационный сигнал, распространяется внутри оптического волокна, то доступ к нему без разрыва волокна затруднен. Несмотря на это в настоящее время известны различные способы формирования каналов утечки информации из оптического волокна без его разрыва [4]. Одним из наиболее скрытных и эффективных среди этих способов является компенсационный [4]. Сущность этого способа заключается в выводе части мощности информационного сигнала за пределы оптического волокна, а затем обратного ввода такой же мощности в волокно, таким образом, чтобы пользователь не обнаружил несанкционированного подключения. Вывести часть мощности сигнала за пределы оптического волокна можно с помощью изгиба, сформированного ответвителем-прищепкой. Целью исследования является реализация компенсационного съема передаваемой информации при помощи ответвителей-прищепок для различных типов оптических волокон и длин волн оптического излучения.

В качестве объектов исследований использовались одномодовые оптические волокна G.652, G.655 и G.657, так как они наиболее часто применяются в современных системах связи. Собрана экспериментальная установка, состоящая из участка оптического волокна, к обоим концам которого подключены измерители мощности. Для вывода и ввода оптического излучения с боковой поверхности оптического волокна использовались серийно выпускаемые ответвители-прищепки FOD 5503 [5]. Ввод мощности обратно в волокно осуществляется также посредством ответвителя-прищепки. Таким образом, для реализации компенсационного способа необходимо определить долю мощности, ответвляемую из оптического волокна, потери мощности на ответвителе-прищепке и коэффициент ввода излучения в оптическое волокно в сторону источника оптического излучения и в сторону его получателя для длин волн оптического излучения 1310, 1490, 1550 и 1625 нм.

Получено, что увеличение длины волны приводило к росту потери мощности оптического излучения для всех исследуемых оптических волокон от –5,04 до –1,89 дБ для G652, от –0,47 до –0,04 дБ для G655 и от –6,22 до –2,08 дБ для G657. Наибольшее значение потери мощности соответствовало длине волны 1625 нм и волокну G655, а наименьшее – длине волны 1310 нм и волокну G657. Также увеличение длины волны приводило к росту значения доли ответвляемой мощности оптического излучения с боковой поверхности оптического волокна для всех исследуемых волокон. Максимальная величина ответвляемой мощности была получена для длины волны 1625 нм и волокна G655 и составила –10,65 дБ, а минимальная – для длины волны 1310 нм и волокна G657 и составила –20,71 дБ. Таким образом, для уменьшения потерь мощности оптического излучения, вносимых ответвителем-прищепкой, и снижения ответвляемой ею мощности необходимо использовать для передачи информационного сигнала длину волны 1310 нм и оптическое волокно G657.

Установлено, что увеличение длины волны приводило к росту коэффициентов ввода оптического излучения, как в сторону источника оптического излучения, так

и в сторону его получателя. Мощность, вводимая в оптическое волокно, распространяется не одинаково в сторону источника и в сторону получателя для всех исследуемых длин волн. Коэффициент ввода в сторону источника принимает меньшие значение, чем коэффициент ввода в сторону получателя. При этом, если поменять местами вход и выход ответвителя-прищепки, то ситуация изменяется на противоположную. Такое распределение мощности связано с расположением макроизгиба, созданного ответвителем-прищепкой. Чем большее расстояние проходит сигнал, тем большие потери он испытывает.

Таким образом, установлено, что реализация компенсационного метода съема информации возможна, но с учетом расположения точки ввода оптического излучения в макроизгиб. На основании проведенных исследований предложена методика оценки применимости компенсационного съема информации из оптического волокна при помощи ответвителей-прищепок.

Список литературы

1. Govind P. Agrawal Fiber-Optic Communication Systems. New York: Wiley-Interscience; 2002. 530 p.

2. Дмитриев С.А., Слепов Н.Н. Волоконно-оптическая техника: современное состояние и новые перспективы. М.: Техносфера, 2010. 576 с.

3. Убайдуллаев Р.Р. Волоконно-оптические сети. М.: Эко-Трендз, 2001. 263 с.

4. Зеневич А.О. Обнаружители утечки информации из оптического волокна. – Минск: Белорусская государственная академия связи, 2017. 143 с.

5. Бараночников М.Л. Приемники инфракрасного излучения. Национальный университет Львовская политехника, 1985. 94 с.

ПРОБЛЕМЫ И ТРЕБОВАНИЯ К ОБУЧЕНИЮ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Е.Ю. Кухарчик

Учреждение образования «Академия управления при Президенте Республики Беларусь», Минск, Беларусь

Современный мир становится все более информационным, и при этом количество защищенной информации значительно возрастает. По этой причине, создается все больше возможностей для кибератак и киберпреступлений, что в свою очередь увеличивает спрос на специалистов в области защиты информации. Подготовка компетентных специалистов является одной из главных задач в этой области.

Специалисты по защите информации должны обладать определенными компетенциями, включающими знания и навыки в области криптографии, сетевых протоколов, программного обеспечения для защиты информации, методов анализа и оценки уязвимостей систем, а также знания правовых и организационных аспектов защиты информации. Кроме того, специалист по защите информации должен уметь анализировать и оценивать риски безопасности, создавать и реализовывать политику безопасности, а также уметь разрабатывать и внедрять системы защиты информации. Знания в этих областях могут помочь специалистам по защите информации разрабатывать и внедрять наиболее эффективные системы защиты информации, а также эффективно реагировать на возможные угрозы безопасности.

Подготовка компетентных специалистов является одной из главных задач в этой области. Однако, существует ряд проблем и недостатков в обучении студентов в этой

сфере. Одна из основных проблем заключается в том, что существующие учебные программы в высших учебных заведениях недостаточно освещают важность защиты информации и не дают должного количества знаний для успешной карьеры в этой области. Учебные проекты и задания могут быть не связаны с реальной жизнью и практически не помогают приобрести необходимые реальные навыки. Кроме того, отсутствие доступа к новейшим технологиям в области защиты информации для учебных заведений может быть еще одной причиной, по которой студенты остаются в устаревшей информационной среде. Это может заставить их оставаться пассивными в этой сфере и не дает им соревноваться в рынке труда. Также одной из причин недостаточной подготовки специалистов по защите информации может быть и отсутствие мотивации у студентов. И если этот курс является не обязательным, они могут не обращать на него должного внимания. Однако необходимо заметить, что успешное обучение специалистов в этой области также зависит от его содержания и методов преподавания. При использовании новейших методов информационных технологий, обучение может стать более интересным и привлекательным. Кроме того, когда студенты имеют доступ к новейшим технологиям, практически проводимые лабораторные работы могут дать им ценный опыт и помочь приобрести новые и востребованные навыки.

В целом, подготовка специалистов в области защиты информации является сложным и многогранным процессом. Студенты должны иметь доступ к новейшим технологиям, проходить интересные и полезные курсы, которые не только научат их теоретическим знаниям, но и предоставят практические навыки для успешного устройства на работу. Только в таких условиях студенты смогут готовиться к сложным задачам защиты информации в реальном мире, и зайти на это поле боя со всеми положительными эмоциями и знаниями.

Список литературы

1. Малюк А.А., Погожин Н.С., Толстой А.И. Обучение вопросам компьютерной безопасности специалистов-профессионалов и персонала, связанного с противодействием компьютерным атакам // Известия Южного федерального университета. 2003. № 33 (4).

2. Мовчан И.Н. Проблемы подготовки специалистов в области информационной безопасности // Открытое образование. 2013. № 5.

3. Астахова Л.В., Сафонова И.А. Развитие цифровых компетенций будущих специалистов по защите информации в вузе // Вестник Южно-Уральского государственного университета. 2020. №12 (1).

ВЛИЯНИЕ СПИН-ОРБИТАЛЬНОГО РАССЕЯНИЯ НА КРИТИЧЕСКОЕ СОСТОЯНИЕ НАНОСТРУКТУР СВЕРХПРОВОДНИК – ФЕРРОМАГНЕТИК

В.Н. Кушнир, С.Л. Прищепа

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

Слоистые наноструктуры сверхпроводник (S) – ферромагнетик (F) являются естественной элементной базой сверхпроводниковой спинтроники; ее первой основной задачей является управление сверхпроводящим состоянием каждого из S-F элементов путем задания его магнитного состояния [1]. Одна из проблем, сопряженная с решением основной задачи – учет влияния процессов спин-орбитального и парамагнитного рассеяния электронов на характеристики сверхпроводимости S-F структур и, в частности, на их критическое состояние. Данная проблема решалась в настоящей работе в рамках микроскопической теории в формализме

линеаризованных уравнений диффузионного предела матричным методом [2]. Процессы спин-орбитального и парамагнитного рассеяния оказываются учтенными данным методом эффективными «углами», выраженными через частоты рассеяния. Для численного расчета эффектов использовались параметры S-F структур семейства Nb/PdNi. Были рассчитаны собственные температуры критических состояний сверхпроводимости в зависимости от эффективных параметров рассеяния при различных толщинах и количестве F-S бислоев. Достаточно пассивная роль парамагнитного рассеяния отражается монотонным убыванием критических температур при увеличении его интенсивности (в этом отношении задача управления параметрами спинтронных элементов становится тривиальной). Между тем зависимости собственных критических температур от частоты спин-орбитального рассеяния в F-слое оказываются, на первый взгляд, достаточно странными. А именно, увеличение интенсивности спин-орбитального рассеяния сопровождается не уменьшением, а увеличением критической температуры. Кроме того, происходит смещение точки 0 – пи-кроссовера в сторону больших значений толщин F-слоя. Данный факт обязан, как на это указывает расчет, частичному нивелированию ферромагнитного порядка в F-слое. Вместе с тем, полученное решение можно рассматривать как постановку экспериментальной задачи.

Список литературы

1. Kushnir V.N., Sidorenko A., Tagirov L.R. [et al.]. Basic superconducting spin valves. In: Functional nanostructures and metamaterials for superconducting spintronics. Springer Int. Pub. AG, part of Springer Nature. 2018. P. 1–29.

2. Кушнир В.Н. Сверхпроводимость слоистых структур. Минск, БНТУ, 2010.

ПРЕОБРАЗОВАТЕЛИ ЭНЕРГИИ РАДИОВОЛН В ЭЛЕКТРОЭНЕРГИЮ

В.И. Лебедев, Ю. Витали, Г.В. Давыдов, В.Е. Галузо

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

В работе приводятся результаты анализа возможных областей применения преобразователей энергии радиоволн в электроэнергию в том числе и в области защиты информации. Рассматривается возможность передачи солнечной энергии с космических станций, преобразовав ее в радиоволны и передав их на Землю. Такие преобразователи наиболее часто используются для преобразования энергии радиоволн в электроэнергию постоянного тока. Эти устройства называются выпрямительными антеннами (ректеннами) и используются в электропитании датчиков, микромашин, медицинских имплантантов, телескопов пространственного базирования, генераторов радиочастотных меток.

Возможная область применения ректеннов - передача энергии от солнечных электростанций, расположенных на геостационарной орбите Земли [1]. Электроэнергия, вырабатываемая фотоэлектрическими батареями, расположенными на космических объектах, преобразуется СВЧ генераторами в электромагнитные колебания. СВЧ генераторы подключены к антенным решеткам для передачи сфокусированной энергии ректеннам, расположенным на Земле. СВЧ генераторы и соответствующие ректенны работают в сантиметровом диапазоне волн из-за их значительно более слабого поглощения в ионосфере и тропосфере Земли по сравнению с поглощением оптического излучения от Солнца.

Список литературы

1. Ванке В.А. СВЧ – электроника – перспективы в космической энергетике // Электроника: наука, технология, бизнес. 2007. № 5. С. 98–102.

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ПРИМЕНЕНИЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

В.М. Логин

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

Образовательным стандартом высшего образования I ступени по специальности 1-39 03 01 «Электронные системы безопасности» предусмотрена подготовка специалиста по квалификации инженер-проектировщик, обладающего практическими навыками в области применения и проектирования систем видеонаблюдения [1]. Будущим специалистам в данной области предлагается в ходе учебного процесса и курса специальных дисциплин освоить методику проектирования видеосистем.

Шаги проектирования видеосистемы в деталях заключаются в следующем.

Сперва необходимо выбрать (1) соответствующий для каждого предусмотренного места монтажа тип камеры, который в каждом случае оптимально подходит для конкретной постановки задачи.

Определить заданные величины (2), идет ли речь о (а) – внутренней ориентации или (б) – наружной ориентации, которые определены при выборе необходимой комплектации камер. Этот пункт должен быть рассмотрен также индивидуально для каждой камеры, т.к. во многих вариантах конфигурации оборудования, как для внутренних, так и для наружных камер он существует. Ниже на соответствующих шагах, в частности в 2а или 2б, необходимо осуществить расчет принятой комплектации.

Следующее решение (А) – жесткий монтаж или (В) – монтаж на головке с изменяемой пространственной ориентацией служит критерием для (3) применяемых монтажных приспособлений, (4) типа применяемого объектива и (5) при известных условиях дополнительно необходимых монтажных приспособлений.

Вне зависимости, имеется ли наружная или внутренняя ориентация, жесткий монтаж или монтаж на головке с изменяемой пространственной ориентацией, (6) нужно выбрать подходящую систему передачи видео.

Для камер, которые должны работать на головках с изменяемой пространственной ориентацией (ИПО), (7) нужно выбрать оптимально подходящую систему дистанционного управления. Уже со сложившимся представлением о выборе коммутационного оборудования и центрального блока следует приступить к поиску интегральных системных решений. Если для решения предлагаются, например, системный видеокоммутатор, маленький матричный коммутатор видеосистемы или комплексный матричный коммутатор для видеомодулей, то необходимо определить подходящее комплексное решение [2].

Далее осуществляется выбор таких (8) устройств, как квадраторы, мультиплексоры, сенсоры и т. д.

На заключительном этапе необходимо правильно выбрать (9) видеомонитор, а также место для его установки или расположения.

Список литературы

1. ОСВО 1-39 03 01. Электронные системы безопасности. Минск: Министерство образования Респ. Беларусь.

2. Логин В.М., Будник А.В. Технические системы безопасности: лаб. практикум по курсу «Физические и аппаратные средства защиты информации и их проектирование» для студ. спец. I-38 02 03 «Техническое обеспечение безопасности» всех форм обуч. – Минск: БГУИР, 2007. 64 с.

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

В.М. Логин

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

Электронные системы контроля доступа (СКД) начали широко применяться в технических системах безопасности с 80-х годов XX века и прошли длительный эволюционный путь от простейших кодовых устройств, управляющих дверным замком, до сложных компьютерных систем, охватывающих целые комплексы зданий. В настоящее время на отечественном рынке технических средств охраны предлагается широкий ассортимент оборудования для СКД различной степени сложности.

Система контроля и управления доступом (СКУД) является третьим рубежом защиты после систем охранно-пожарной сигнализации и видеонаблюдения, но не заменяет бдительных сотрудников службы безопасности и требует предусматривать человеческий фактор – дисциплинированность, профессионализм, ответственность службы безопасности и сотрудников организации.

СКУД – это совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также задача оперативного контроля за персоналом и временем его нахождения на территории объекта. Существуют «три кита» из которых состоит СКУД: управляющие контроллеры; устройства идентификации личности; оборудование ограничения доступа [1]. СКУД позволяет: контролировать доступ людей в служебные помещения; контролировать доступ автомобильного транспорта на территорию объекта; организовать базы данных на каждого работника или посетителя; отслеживать процесс прохождения сотрудниками точек контроля; организовать учет рабочего времени персонала.

Всем сотрудникам компании, в которой установлена СКУД, выдаются специальные электронные пропуска, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в СКУД, которая на основании анализа данных о владельце идентификатора, принимает решение о разрешении допуска или запрете прохода того или иного сотрудника на охраняемую территорию. База данных позволяет оперативно разыскать сотрудника на территории по последней точке прохода, где он предъявлял идентификатор. В каждой точке прохода может быть несколько тайм зон (временных ограничений на доступ). В качестве исполнительных устройств СКУД могут использоваться электромеханические или электромагнитные замки различных типов, турникеты, автоматические двери, шлагбаумы, автоматические привода ворот и т.п.

Основными характеристиками СКУД являются: контроль и регистрация прохода сотрудников в разрешенное время или в соответствии с допуском в охраняемые помещения; ведение архива проходов; отображение состояния системы в режиме реального времени; автоматический учет рабочего времени; сравнение фотографии сотрудника, хранящейся в базе данных, с реальным изображением с видеокамеры зоны прохода; составления отчетов по параметрам (вход/выход, тревоги, дежурств, рабочего времени).

Список литературы

1. Логин В.М., Будник А.В. Технические системы безопасности: лаб. практикум по курсу «Физические и аппаратные средства защиты информации и их проектирование» для студ. спец. I-38 02 03 «Техническое обеспечение безопасности» всех форм обуч. – Минск: БГУИР, 2007. 64 с.

РОЛЬ ДИСЦИПЛИНЫ «АППАРАТНО-ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ И СЕТЕЙ» В ИЗУЧЕНИИ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Ломако

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

Текущий период истории человечества характеризуется бурным научно-техническим прогрессом в области информационно-коммуникационных технологий (ИКТ). Осуществляется массовый переход к распределенному сбору, хранению, обработке информации и, как следствие, к распределенному (удаленному) доступу к ней разных категорий пользователей. При этом проблемы защиты информации от несанкционированного использования, разрушения и искажений не только не исчезают, но и становятся еще острее, переходя на качественно новый уровень сложности. Решением указанных проблем должны заниматься подготовленные специалисты с высшим техническим образованием по широкому спектру специальностей.

Учебные планы специальности «Автоматизированные системы обработки информации» (АСОИ) и некоторых других, по которым ведется обучение в Белорусском государственном университете информатики и радиоэлектроники, содержат ряд дисциплин, имеющих отношение к техническим средствам защиты информации, причем наиболее всесторонне и комплексно соответствующие вопросы рассматриваются в дисциплине «Аппаратно-программное обеспечение ЭВМ и сетей» (АПОЭВМиС). Дело в том, что указанная дисциплина позволяет понять принципы и особенности реализации современных ИКТ, как на структурно-логическом, так и на аппаратно-физическом уровне. При этом естественным образом выявляются «узкие места» ИКТ в смысле недостаточной защиты информации, что позволяет целенаправленно акцентировать внимание на методах и средствах обеспечения информационной безопасности в конкретных местах автоматизированных систем.

В частности, дисциплина АПОЭВМиС дает понимание влияния на защиту информации следующих факторов: топология, архитектурные особенности и технологии построения сетей; физическая среда передачи данных; методы и протоколы доступа к физической среде передачи данных; протоколы приемопередачи данных, используемые на разных уровнях эталонной модели RM OSI ISO [1]; способы кодирования и сжатия данных для передачи в сетях; сетевое оборудование и реализуемые в нем методы обработки данных, например, средства, методы и алгоритмы маршрутизации; сетевая организация и управление работой сети;

системное сетевое программное обеспечение (ПО), включая, операционные системы, драйверы, сетевые утилиты, специальное ПО; программная антивирусная и антихакерская защита.

Изучение перечисленных и ряда других смежных вопросов требует существенных затрат времени. Именно поэтому объем учебной нагрузки по данной дисциплине для специальности АСОИ согласно новому образовательному стандарту заметно вырос: лекции – с 36 до 48 часов, лабораторные работы – с 16 до 32 часов, Изложенное выше подтверждает важную роль дисциплины АПОЭВМиС в деле подготовки квалифицированных специалистов, способных противостоять вызовам и угрозам информационной безопасности в современных сложных системах.

Список литературы

1. Ломако А.В. О важности изучения сетевых протоколов стека TCP/IP как инструментов обеспечения защиты информации в современных автоматизированных системах // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. С. 67–68.

АДАПТАЦИЯ МЕТОДОВ КРИПТОГРАФИИ К ПРИМЕНЕНИЮ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО РЕЕСТРА В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ

А.М. Макаров, Б.М. Гаджимурадов, Е.А. Писаренко, А.С. Ермаков

ФГБОУ ВО «Пятигорский государственный университет», Пятигорск, Россия

Появление сведений о внедрении технологии блокчейн в финансовую сферу деятельности и последовавшее практическое применение трансакций криптовалют вызвало бурную реакцию в научном и технологическом сообществе. Появилось множество публикаций по майнингу и транзакциям криповалют. Применение криптографии (асимметричного шифрования, двухключевой системы с открытым ключом), криптостойкого хэширования и цифровой электронной подписи на основе двухключевой схемы привело к пониманию сложности технологии блокчейн [1].

Обеспечение безопасности данных в сети блокчейн, наличие всей текущей базы данных и транзакций каждого абонента у каждого участника сети привело к возникновению эффекта доверительных отношений в цифровой среде. Однако, реализация доверительности автоматической обработки информации в системе «цифровая вычислительная система – цифровая вычислительная система» достигается за счет применения дорогостоящих технологий современных криптографических методов и средств. Поэтому весьма актуальной является задача адаптации теории и приложений криптографии для ее использования на объектах социально-экономической сферы.

В данной работе сделана попытка решения задачи адаптации двухключевой системы шифрования к объектам таких социально-значимых сфер, как жилищно-коммунальное хозяйство, фармацевтика, ведение и хранение медицинских карт, работа следственных органов. Как показал анализ поставленной задачи, основную трудность представляет адаптация технологий обмена ключами между участниками сети, назначение майнера и его роль в функционировании системы с распределенным реестром. Важным является и тот факт, что подавляющее большинство участников блокчейн-сети не только не являются профессиональными криптографами, но и ничего не знают о методах шифрования. То есть, большая часть пользователей сервисных услуг на основе криптографических методов подвергается цифровыми трансформациями своего привычного уклада деятельности в сфере получения услуг.

Список литературы

1. Materials the 3rd International Conference on Blockchain Technology and Information Security (ICBCTIS 2022), Xi'an, May 26–28, 2023.

ВАРИАНТ ОПТИМИЗАЦИИ ПРОЦЕССА THREAT INTELLIGENCE В ЦЕНТРЕ МОНИТОРИНГА КИБЕРБЕЗОПАСНОСТИ

А.В. Макатерчик, В.В. Маликов

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

Кибербразведка или Threat Intelligence является частью комплексного подхода по мониторингу и реагированию на современные киберугрозы. При этом организация кибербразведки в рамках современного центра мониторинга кибербезопасности сталкивается с целым рядом проблем, из которых для данного исследования выделены следующие:

Современная политическая обстановка не гарантируют стабильность доступа к источникам информации об угрозах.

Использование нескольких источников приводит к росту объемов информации требующей корреляции, обработки и фильтрации ложных данных. Что приводит к росту нагрузки на средства защиты информации и персонал.

Большое время реакции при ручной обработке инцидентов связанных с обнаружением индексов компрометации в потоках событий.

Сложность, а зачастую невозможность реализации превентивной блокировки источников угроз на средствах защиты информации, из-за существующих у них ограничений по производительности, емкости баз данных, количествуACL списков и т. п.

Решение данных проблем возможно при организации комплексного подхода, заключающегося в:

1. Организации сбора информации из нескольких источников: собственные инструменты кибербразведки, фиды и платформы от нескольких поставщиков из разных стран и сообществ.
2. Обработка их с использованием нескольких средств. Например, встроенный сервис SIEM (SOAR) и ПО Kaspersky CyberTrace.
3. Превентивную блокировку средствами защиты информации только источников угроз с высоким риском.
4. Анализ потоков событий на предмет наличия в них индексов компрометации с использованием как специально выделенных аппаратно-программных средств, например, Kaspersky CyberTrace, так и средствами, интегрированными в SIEM, SOAR и т.п.
5. При обнаружении в потоке событий индексов компрометации выполнять автоматическую блокировку источников угроз средствами защиты информации на ограниченный период времени.

Данный подход обеспечивает оптимизацию использования ресурсов средств защиты информации, уменьшение нагрузки на аналитиков безопасности, снижает количество ложно-позитивных событий.

Список литературы

1. Threat Intelligence сейчас модный тренд. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/phdays/articles/499145.php. – Дата доступа: 27.04.2023.

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПРОЦЕССЕ РАЗРАБОТКИ И ЭКСПЛУАТАЦИИ

А.Ф. Марко

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

При разработке и эксплуатации программного обеспечения (ПО) для систем перемещений важной задачей является обеспечение их целостности, которая позволяет предотвратить использование ПО с незапланированные изменениями. Контроль за целостностью в предложенном ПО обеспечивается на этапе разработки с помощью внедрения соответствия версий в интегрированную среду разработки Visual Studio (VS), на этапе эксплуатации – с помощью формирования и сравнения контрольных сумм.

Алгоритмы соответствия версий обновляют версии файлов с расширениями dll и exe при изменении их исходного кода. Алгоритмы обновления версий реализованы в виде расширения для среды VS, которая может взаимодействовать как с централизованной системой управления версиями Team Foundation Server (TFS), так и с децентрализованной системой Git. Пользовательский интерфейс расширения встроен в интерфейс среды VS, что позволяет контролировать соответствие версий и разрабатывать ПО в одном окружении [1]. Алгоритмы расширения определяют модифицированные компоненты ПО, формируют новые версии, присваивают их компонентам и сохраняют изменения в систему TFS или Git [2].

Алгоритмы формирования и сравнения контрольных сумм в процессе эксплуатации реализованы в виде отдельного модуля ПО системы управления. ПО для системы управления состоит из множества различных объектов: исполняемые файлы, файлы данных, объекты баз данных. Формирование контрольных сумм выполняется для каждого типа по-разному. Также учитывается тот факт, что некоторые объекты, например, SQL-таблица базы данных, содержащая реквизиты для входа пользователей системы, постоянно изменяется в процессе эксплуатации, следовательно, отслеживать изменения в ней не требуется и контрольные суммы формировать не нужно [2]. Для формирования контрольных сумм объектов используется алгоритм SHA-2, который создает контрольные суммы от 224 до 512 бит, что обеспечивает высокую степень надежности и защиты от подделки или изменения файла [3]. Кроме того, SHA-2 является стандартом безопасности для многих приложений и операционных систем.

Таким образом разработанные алгоритмы позволяют автоматически верифицировать целостность ПО в процессе его разработки и эксплуатации и тем самым предотвращают его использование вместе с незапланированными изменениями.

Список литературы

1. Шарп Дж. Microsoft Visual C#. Подробное руководство. СПб.: Питер; 2017. 848 с.

2. Марко, А.Ф. Методы соответствия версий и контроля целостности программного обеспечения для систем перемещений в режиме реального времени // Информационные технологии и системы 2022 (ИТС 2022): материалы междунар. науч. конф., Минск, 23 ноября 2022 г. С. 63–64.

3. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Диалектика, 2004. 432 с.

ЗАЩИТА ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КООРДИНАТНОГО ПРЕОБРАЗОВАНИЯ

А.И. Митюхин

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

Предлагается метод защиты информации посредством маскирования с использованием координатного преобразования. Базовым векторным пространством преобразования служат собственные векторы ковариационной матрицы cov(**C**) произвольного 2D снимка изображения C [1]. Информационные данные кодируются псевдослучайными последовательностями (ПСП) низкоскоростного помехоустойчивого кода. В основе метода лежит операция гаммирования значений коэффициентов координатного преобразования и поточного шифра (кода) в виде ПСП. Коэффициенты преобразования следует воспринимать как аддитивный помеховый источник, затрудняющий правильное декодирование кода в канале с подслушиванием. Маска в виде сильно коррелированного изображения после преобразования в базисе собственных функций представляется в виде последовательности некоррелированных коэффициентов [2]. Такое свойство позволяет определять коэффициенты как дискретные случайные величины, распределение которых определяется по всему блоку изображения. Это важно для повышения надежности передачи информации по основному каналу и, соответственно, уменьшения до заданного минимального значения пропускной способности канала утечки. Гаммирование кода и коэффициентов преобразования, представленных в двоичной форме после выполнения операции квантования, осуществляется в поле Галуа с характеристикой 2 ($GF(2)$). В качестве кода использовалась конструкция, полученная комбинированием m-последовательностей. В этом случае возможность восстановления структуры неприводимого примитивного над полем $GF(2)$ полинома кода по правильно принятой последовательности $2k$ информационных символов исключается. Не зная закон кодирования (модуляции) и конкретной маски в виде преобразованного изображения, используемой на определенном временном интервале передачи данных, применить в канале подслушивания оптимальные методы (согласованную или корреляционную фильтрацию) становится проблематичным. Экспериментальные исследования в среде МАТЛАБ показали возможность применения метода на практике.

Список литературы

1. Mitsiukhin A. Proceedings 59th IWK. TU Ilmenau, Band 59, 2017, Heft 2.2.02, 6 Seiten.

2. Jahne B. Digital Image Processing. Concepts. Algorithms, and Scientific Applications. E-BOK, 2013.

МОДЕЛИРОВАНИЕ ИЗ ПЕРВЫХ ПРИНЦИПОВ СВОЙСТВ ГРАФЕНА МОДИФИЦИРОВАННОГО АТОМАМИ ФТОРА

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 свойств графена модифицированного атомами фтора. Разработка новых полупроводниковых приборов требует исследования свойств новых материалов и графен является одним из таких материалов, которые

привлекают интерес исследователей. Графен с добавление атомов – фтора, водорода и других химических элементов позволяет создавать его химические модификации. Используя этот подход, можно разрабатывать полупроводниковые приборы и устройства с более совершенными выходными характеристиками. Было выполнено моделирование из первых принципов параметров и характеристик фторированного графена с применением программного комплекса Quantum Espresso. В рамках теории функционала электронной плотности, используя обменно-корреляционные функционалы вида PBE (Perdew-Burke-Ernzerhof), были получены основные характеристики модификации графена с использованием атомов фтора – зонная диаграмма, зависимости плотности состояния (параметр DOS) электронов и дырок от величины энергии. Путем итерационного решения транспортного уравнения Больцмана определены зависимости подвижности носителей заряда от величины температуры. Полученные зависимости и параметры фторированного графена могут служить основой для создания новых гетероструктурных приборов, содержащих слои модифицированного графена и других полупроводниковых материалов. Формирование гетероструктурных приборов с использованием графена и его модификаций позволит реализовать новые устройства, которые найдут широкое применение в системах передачи и обработки сигналов СВЧ и КВЧ диапазонов.

СТАТИСТИЧЕСКИЙ АНАЛИЗ КОНЕЧНЫХ ПОЛУГРУПП И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

В.А. Молчанов, В.Н. Кутин

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

В современной криптографии при построении криптографических примитивов, криптосистем и протоколов особое внимание уделяется применению методов универсальной алгебры [1]. Важность этих исследований обосновывается, в частности, тем, что алгебраическая криптография является одной из альтернатив решения проблемы постквантовой криптографии [2].

Настоящая работа посвящена применению в криптографии методов теории полугрупп [3], которые не только позволяют естественно обобщать известные криптосистемы, но и разрабатывать принципиально новые криптосистемы на основе неразрешимых и трудноразрешимых алгоритмических проблем теории полугрупп [4]. Например, одной из таких проблем теории полугрупп является известная проблема равенства слов [3].

Данная работа является продолжением исследований [5]. В рамках настоящей работы был проведен статистический анализ генерируемых симметрических полугрупп преобразований множеств небольшой мощности, а также эмпирических множеств преобразований мощности 100, 500, 1000, 5000, 10000, 50000, 100000, 500000, 800000, полученных путем случайной выборки элементов из симметрической полугруппы для дальнейшего проецирования результатов анализа на симметрические полугруппы преобразований множеств большой мощности. В частности, были получены: математическое ожидание, дисперсия, среднее квадратическое отклонение и распределения порядков элементов (преобразований) таких полугрупп. На основе вычисленных статистических характеристик были построены графики ядерных оценок плотности, полученные кривые, оказались близки по построению к нормальной кривой Гаусса. Полученные распределения прошли тест Д'Агостино-Пирсона на нормальность. Также было замечено, что с увеличением мощности генерируемой симметрической полугруппы, растет и значение математического ожидания количеств порядков

элементов, при этом значение математического ожидания количеств порядков элементов случайно выбранных множеств преобразований практически не меняется с ростом мощности множества.

Список литературы

1. Романьков В.А. Алгебраическая криптография. Омск: изд-во Ом. гос ун-та, 2013.

2. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM journal on computing. 1997. Vol. 26. 1484.

3. Lallement G. Semigroups and combinatorial applications. Pure and Applied Mathematics Series, Wiley, New York, 1979.

4. Maze G., Monico C., Rosenthal J. Public Key Cryptography based on Semigroup Actions. Advances in Mathematics of Communications 1.4. 2007. P. 489–507.

5. Молчанов В.А., Кутин В.Н. О применении методов теории полугрупп в криптографии // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. С. 73–74.

ПОПУЛЯРИЗАЦИЯ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СТРАНАХ СНГ

В.А. Мурыгин

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

Понятие защиты информации в наше время становится все более актуальным, особенно в свете растущей зависимости от цифровых технологий и увеличения объема цифровых данных.

Защита информации является важной составляющей в различных сферах жизни, включая бизнес, государственные организации, здравоохранение, образование и другие. Несмотря на это, в странах СНГ вопросы защиты информации не всегда получают должное внимание.

Для того чтобы повысить осведомленность о важности защиты информации, необходимо проводить регулярные кампании по ее популяризации. Одной из таких кампаний может быть проведение мероприятий, на которых будут представлены современные методы защиты информации, а также последствия, которые могут возникнуть в случае утечки конфиденциальной информации.

Кроме того, необходимо повышать осведомленность населения о методах защиты информации в повседневной жизни. Для этого можно проводить обучающие курсы и семинары, которые помогут людям научиться правильно использовать пароли и другие методы защиты своей личной информации, а также научат отличать безопасные и небезопасные действия в Интернете.

Важно также проводить информационные кампании о рисках, связанных с нарушением конфиденциальности информации, и об опасности взлома и кражи личных данных. Это поможет людям осознать серьезность проблемы и заинтересоваться методами защиты своих данных.

Кроме того, страны СНГ могут активно сотрудничать с международными организациями по защите информации, такими как CERT (Computer Emergency Response Team), которые специализируются на предотвращении кибератак и угроз безопасности информации. В таком сотрудничестве может быть обмен информацией, анализ уязвимостей и общие практики по защите информации.

В заключении, популяризация понятия защиты информации в странах СНГ является критически важным шагом в направлении повышения кибербезопасности и защиты конфиденциальности в информационной эпохе. Чтобы достичь этой цели,

необходимо проводить образовательную работу среди населения и бизнес-сообщества, поддерживать и развивать местную инфраструктуру информационной безопасности и сотрудничать с международными организациями [1–4].

Список литературы

1. ScienceDirect [Электронный ресурс]. – Режим доступа: https://www.sciencedirect.com/. – Дата доступа: 01.05.2023.

2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html. – Дата доступа: 01.05.2023.

3. Перспективы использования зарубежного опыта и стран СНГ для совершенствования законодательства о защите детей от информации, причиняющей вред их здоровью и развитию [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-zarubezhnogo-opyta-i-stran-sng-dlya-sovershenstvovaniya-zakonodatelstva-o-zaschite-detey-ot-informatsii. – Дата доступа: 01.05.2023.

4. Концепция информационной безопасности Республики Беларусь – взгляд в будущее [Электронный ресурс]. – Режим доступа: https://beldumka.belta.by/isfiles/000167_921517.pdf. – Дата доступа: 01.05.2023.

МАГНЕТИЗМ НАНОЧАСТИЦ КОБАЛЬТА НА ПОВЕРХНОСТИ МЕДИ

Е.С. Назаренко, А.Л. Данилюк, С.Л. Прищепа

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

Исследованы магнитные свойства наночастиц кобальта со структурой «ядро-оболочка» (CoO/Co) на поверхности меди, полученных электрохимическим осаждением. Для анализа магнитных измерений и их интерпретации использована модель случайной анизотропии (RAM) и интегральный вариант закона приближения к намагниченности насыщения (LAS), справедливый для 2D систем [1]. LAS для 2D систем соответствует интегральному преобразованию Мейера (K-transform). С его помощью возможно определить корреляционные функции осей случайной магнитной анизотропии, а также поля обмена и случайной анизотропии. Из экспериментальных данных по измерению намагниченности получена функция-образ для массива CoO/Co на меди при температуре 4 К. Полученная функция-образ характеризуется немонотонной зависимостью от напряженности магнитного поля. Проведенное фитирование показало, что экспериментальные данные хорошо укладываются на аналитические зависимости степенного вида. В этом случае, согласно интегральному преобразованию Мейера, корреляционная функция определяется функцией Бесселя первого рода. Проведенные расчеты показали, что корреляционная функция является колебательной, а ее амплитуда определяется значением показателя m, зависящего от величины поля обмена. При $m < 0{,}5$ амплитуда уменьшается с расстояниям z, при $m = 0{,}5$ не меняется, а при $m > 0{,}5$ растет. Рост амплитуды корреляционной функции говорит об усилении корреляций осей анизотропии. Такое усиление в наночастицах CoO/Co мы связываем с влиянием магнитной анизотропии CoO, составляющей порядка $(2{,}5–2{,}7)10^7$ Дж/м^3 [2], а также наличием поля обменного смещения, способствующего закреплению намагниченности Co. Эти факторы в наночастицах CoO/Co приводят, на наш взгляд, не только к усилению корреляций осей анизотропии Co, но и способствуют проявлению эффекта когерентной анизотропии по аналогии с массивом углеродных нанотрубок, содержащих

наночастицы железа и цементита [3]. Для оценки полей обмена и анизотропии, а также параметров корреляционной функции применялась прямая процедура расчета LAS путем подстановки корреляционной функции в интегральное преобразование Мейера для двумерной магнитной системы с учетом вклада когерентной анизотропии. В результате получено, что поле случайной анизотропии составляет 4,6–4,7 кЭ, обменное поле 0,8–1,25 кЭ, поле когерентной анизотропии 1,0–1,2 кЭ. Величина поля случайной анизотропии согласуется с оценками ее величины по RAM. Магнитная анизотропия, которую мы оцениваем из LAS, относится только к «ядру», состоящему из наночастиц Co. Таким образом, проведенная обработка экспериментальных данных и расчеты показали, что оболочка CoO на наночастицах Co ведет не только к появлению обменного смещения, но и возникновению когерентной анизотропии в массиве наночастиц CoO/Co на поверхности меди.

Список литературы

1. Danilyuk A.L. [et. al.] Europhysics Letters. 2017. 117. 27007.
2. Nogués J. [et al.] Phys. Rev. Lett. 2006. Vol. 97. 157203.
3. Danilyuk A.L. [et. al.] New J. Phys. 2015. Vol. 17. 023073.

МАГНИТНЫЕ СВОЙСТВА МАССИВА УГЛЕРОДНЫХ НАНОТРУБОК С НАНОЧАСТИЦАМИ ЖЕЛЕЗА И ЦЕМЕНТИТА

Е.С. Назаренко, М.В. Шарейко

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

Перспективы использования массивов углеродных нанотрубок (УНТ) в спинтронных приборах обработки информации определяются их магнитными свойствами. Образцы были получены методом каталитического CVD с использованием ферроцена [1]. Анализ экспериментальных данных показал, что область приближения к намагниченности насыщения (LAS) характеризуется обратной квадратичной зависимостью от напряженности внешнего магнитного поля для образца, синтезированного с низкой концентрацией ферроцена 0,5 мас.%. Когда концентрация ферроцена больше 1 мас.% полученная LAS пропорциональна обратной зависимости от напряженности магнитного поля в степени 1/2. Установлено, что в массивах магнитофункционализированных углеродных нанотрубок, синтезированных при концентрации ферроцена 0,5–0,8 объемных процентов, с ростом температуры от 2 до 300 К происходит постепенное изменение закона приближения к намагниченности насыщения от обратной квадратичной зависимости от напряженности внешнего магнитного поля до обратной зависимости квадратного корня.

С помощью модели случайной анизотропии получены оценки поля обменного взаимодействия и поля магнитной анизотропией для различных концентраций наночастиц железа в ориентированных массивах углеродных нанотрубок. Полученные оценки этих полей показали, что их величины соответствуют области приближения к намагниченности насыщения. Этот результат влечет за собой определение корреляционных функций, обусловливающих вклад случайной анизотропии, а также уточнение оценок полей обмена и анизотропии. С помощью интегральной модели приближения к намагниченности насыщения [2] установлено, что при концентрации ферроцена 0,5 мас.% корреляционная функция имеет ступенчатый характер (ширина ступеньки составляет около 400 нм) и описывается функцией схожей с функцией Ферми-Дирака. В этом случае обменное взаимодействие между магнитными

наночастицами слабо и основной вклад в энергию дает случайная и когерентная анизотропия. Этот эффект обусловлен тем, что ориентация УНТ вместе с локализацией ферромагнитных наночастиц во внутренних каналах УНТ способствует возникновению ориентационной упорядоченности в образце. С ростом концентрации ферроцена и с повышением температуры корреляционная функция качественно меняет вид и описывается осциллирующей функцией.

Таким образом, в результате проведенных исследований магнитных свойств нанокомпозитов на основе массивов УНТ, содержащих наночастицы железа и цементита, выявлены механизмы обменного взаимодействия и магнитной анизотропии, оценены основные магнитные параметры с использованием модели случайно анизотропии и модифицированной модели для закона приближения к намагниченности насыщения. Показано, что в случае, когда значение обменного поля находится в области приближения к намагниченности насыщения, для оценок магнитных свойств необходимо определять корреляционные функции методом обратного интегрального преобразования Лапласа.

Список литературы

1. Danilyuk A.L. [et al.] New J. Phys. 2015. Vol.17 (2). P. 023073.
2. Chudnovsky E.M. J. Magn. Magn. Mater. 1989. Vol. 79, iss. 1. P. 127–130.

ЗАЩИТА ДАННЫХ В ЭПОХУ КВАНТОВЫХ КОМПЬЮТЕРОВ: ВАЖНОСТЬ ПЕРЕХОДА НА ПОСТКВАНТОВУЮ КРИПТОГРАФИЮ

М.А. Наумов

Государственное предприятие «НИИ ТЗИ», г. Минск, Республика Беларусь

В настоящее время сложно представить передачу конфиденциальной информации между информационными системами без применения средств криптографической защиты информации. Совместное использование симметричных и асимметричных криптографических алгоритмов позволяет обеспечивать защиту передаваемых данных с заданным уровнем стойкости. Однако не все принимают во внимание возрастающую угрозу применения квантовых компьютеров для атак на уязвимые криптографические алгоритмы асимметричного шифрования, выработки и проверки электронной цифровой подписи.

Современная криптография подразумевает использование «дорогих» асимметричных алгоритмов только для проверки подлинности сертификата и выработки общего сеансового ключа, который используется при шифровании основного объема данных с помощью симметричной криптосистемы.

Несмотря на то, что симметричные алгоритмы не являются уязвимыми для атак с применением квантовых компьютеров сами по себе, существует возможность раскрытия сеансовых ключей, с помощью атак на уязвимые асимметричные алгоритмы. Поэтому целесообразно инициировать постепенный переход на использование постквантовых алгоритмов.

Наиболее важно начинать внедрение постквантовых алгоритмов в тех областях, где информация сохраняет актуальность долгое время. Это любые пользователи и операторы конфиденциальной информации с длительным жизненным циклом:

– государственная и иная охраняемая законом тайна;
– коммерческая тайна;
– персональные данные;
– медицинские данные;

– промышленные ноу-хау.

Для других областей этот класс атак менее критичен, так как через условные десять лет информация потеряет свою актуальность. Но, скорее всего, в течение ближайших пяти–восьми лет мы увидим переход на квантово-устойчивые решения по всему миру для защиты от новых угроз. Множество систем, использующих классические асимметричные алгоритмы, могут стать уязвимыми уже в ближайшие несколько лет.

В настоящее время в США с июля 2022 года по итогам NIST (National institute of standards and tecnology) были отобраны несколько постквантовых алгоритмов с открытым ключом, а с ноября 2022 года был инициирован переход на постквантовую криптографию для всех внутренних агенств в течении 2023 года.

Список литературы

1. NIST [Электронный ресурс]. – 2023. – Режим доступа: https://csrs.nist.gov/projects/post-quantum-cryptography – Дата доступа: 05.04.2023.

2. Migrating to Post-Quantum Cryptography [Электронный ресурс]. – November 18, 2022. – Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf – Дата доступа: 8.04.2023

ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ ОТПЕЧАТКА ПАЛЬЦА

А.В. Никитин

ЗАО «Диджитал Дизайн», Санкт-Петербург, Российская Федерация

Электронная подпись появилась в связи с развитием электронного способа оборота документов. Так как фальсификация подписи на основе обычного изображения не составляет труда, требовалось создать метод, позволяющий реализовать безопасную идентификацию субъекта, выполнившего подпись документа. Основным методом, который позволяет это сделать, является электронная цифровая подпись, которая основана на генерации открытого и закрытых ключей шифрования посредством использования определенной хэш-функции в зависимости от требуемого уровня защищенности подписи. С помощью закрытого ключа осуществляется подписание документа и, поэтому, данный ключ доступен исключительно субъекту, подписавшему документ. Открытый же ключ является общедоступным и используется субъектом, которому требуется проверить, что документ подписан нужной подписью.

В работе рассмотрены виды и алгоритмы электронной подписи, проведен анализ работы данных алгоритмов и исследованы особенности работы с ним. Также проведен анализ существующих методов биометрической идентификации и изучены способы применения биометрических данных для формирования на их основе электронной подписи.

Метод сканирования отпечатков пальцев прост в использовании и обеспечивает надежность. Основным преимуществом данного метода является стоимость реализации и небольшие размеры сканирующего устройства. Биометрическая система распознавания реализуется в аппаратной и программной части. В аппаратную часть входят сканеры, которые считывают биометрические особенности с физического объекта (папиллярные линии) и создают их цифровую модель. Программная часть использует полученную цифровую модель и сверяет ее с базой данных для распознавания субъекта. Основными параметрами оценки точности работы являются коэффициент ложного пропуска (FAR) и коэффициент ложного отказа (FRR). Таким

образом, имея уникальные модели физического признака субъекта можно реализовать генерацию уникальной подписи на ее основе.

В работе реализовано приложение, позволяющее подписывать документы формата PDF посредством использования электронной подписи на основе биометрических данных. Приложение реализовано с использованием библиотеки Bouncy Castle, содержащей провайдер для JCE и JCA (архитектура криптографии в Java и расширение криптографии соответственно). В использованной библиотеке также поддерживается сертификат X.509 и стандарт OpenPGP (протокол шифрования электронной почты).

В перспективе, имея единую базу данных с сохраненными в ней электронными моделями физических признаков субъектов, будет упрощен процесс подписания документов.

СОКРЫТИЕ ИНФОРМАЦИИ В ФАЙЛАХ ФОРМАТА SVG

А.Н. Николайчук

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

Информация, передаваемая по открытым каналам связи, подвергается угрозам раскрытия, изменения и уничтожения. Одним из возможных решений проблемы угрозы раскрытия является использование стеганографических методов. Существующие стеганографические алгоритмы лишь частично удовлетворяют требованиям, которые предъявляются к системам скрытой передачи данных. Актуальной является задача поиска новых алгоритмов и каналов стеганографического встраивания информации. В процессе изучения данной проблемы была выявлена резко возросшая популярность векторных форматов изображений, которые сейчас активно внедряются на web-ресурсах и могут представлять собой достаточно эффективный стеганографический канал [1].

Файл SVG формата представляет собой XML-документ, который может содержать информацию разных видов: текст, растровые изображения, векторные объекты. Такое разнообразие типов данных, которыми оперирует данный формат, позволяет применять стеганографические методы, используя в качестве контейнера любой из типов элементов, перечисленных выше [2].

Стеганография векторных изображений обычно использует внедрение сообщения непосредственно в сами фигуры. Отображаются фигуры в SVG с помощью координат, по которым они описываются, в соответствии с рабочей областью, которая ограничивается с помощью значений атрибутов *width* и *height* тега <*path*>. Уникальность описания фигур в векторных изображениях позволяет формировать объекты вне рабочей области, и использовать данное свойство для внедрения скрытых данных. Такой способ стеганографического осаждения информации в контейнер позволяет размеру сообщения быть независимым от размера самого контейнера или его содержимого, а также предотвратить модификацию внедренной информации при использовании операции сдвига, которая может рассматриваться как тип несанкционированной модификации стеганоконтейнера [3].

Список литературы

1. Николайчук А.Н., Урбанович П.П. Анализ стеганографических методов на основе контейнеров SVG-формата // Информационные технологии: матер. 86-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января – 12 февраля 2022 г. С. 49–51.

2. Николайчук А.Н., Урбанович П.П. Стеганография в векторных изображениях // 73-я науч.-техн. конф. учащихся, студентов и магистрантов: сборник научных работ, Минск, 18–23 апреля 2022 г. С. 947–949.

2. Николайчук А.Н., Урбанович П.П. Стеганографический метод на основе использования особенностей отображения элементов в формате SVG // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2023. № 1 (266). С. 64–70.

ТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ НА СЛУЖБЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ВЕБ-ПРОСТРАНСТВА

А.А. Новиков, К.А. Радкевич

ОАО «Гипросвязь», Минск, Беларусь

Анализ практического опыта применения многочисленных алгоритмов тематического моделирования, убеждает, что тематические модели обладают огромным «запасом решений», в том числе при разработке проектных решений в области обеспечения безопасного веб-пространства.

Благодаря глобальному распространению сети Интернет большинство пользователей получили возможность в невиданных ранее объемах получать и генерировать информацию. Это стало не только благом, но и породило ряд проблем, связанных с генерацией негативного контента, носящего деструктивный характер, как в отношении конкретных людей, так и сообществ, корпораций и государств в целом. Очевидно, что «красноармейца со штыком» к каждому защищаемому объекту (субъекту) не представишь, нужны новые подходы и технологии.

Все ранее используемые аналитические методы, столкнувшиеся с феноменом «больших данных» указывают на потребность в новых методах обработки и анализа, способных извлекать из этих, как правило, неструктурированных данных полезное «зерно», знание. Совокупность таких методов обозначается термином «интеллектуальный анализ данных» (data mining).

Из этой совокупности выделяется подмножество, специализирующееся на анализе текстовых данных – «интеллектуальный анализ текстовых данных» (text mining). Кроме того, выделяется группа методов, которые выполняют задачу тематического моделирования – построения статистических моделей, определяющих тематическую принадлежность каждого документа из корпуса [1].

Тематическое моделирование – это одна из современных технологий обработки естественного языка (англ. Natural language processing, NLP), активно развивающаяся с конца 90-х годов. Тематическая модель коллекции текстовых документов определяет, к каким темам относится каждый документ, и какие слова образуют каждую тему. Тематическое моделирование не претендует на полноценное понимание естественного языка (англ. natural language understanding, NLU), однако выявление тематики можно считать определенным шагом в этом направлении [2].

В сентябре 2022 года в Государственном комитете по науке и технологиям Республики Беларусь успешно прошел государственную экспертизу международный научно-технических проект «Система мониторинга и интеллектуального анализа веб-пространства “Безопасное веб-пространство”». Проект рассчитан на два года, стартует в мае 2023 года. В проекте участвуют представители научного коллектива Центра перспективных исследований в сфере цифрового развития ОАО «Гипросвязь» и ученые Центрального университета Раджастхана и Индийского института информационных технологий Коты, Республика Индия.

В рамках данного проекта предполагается на основе тематических моделей разработать алгоритмы автоматизированного мониторинга и интеллектуального

анализа контента веб-пространства в заданных пределах (областях, доменах) по разработанным правилам (частным политикам), для последующей передачи и использования результатов системой поддержки принятия решений. Также запланировано исследование возможности переноса некоторых разработанных алгоритмов на язык программирования Python.

Список литературы

1. Воронцов К.В. Вероятностное тематическое моделирование: теория, модели, алгоритмы и проект BigARTM, 2020.

2. Deerwester S., Dumais S.T., Furnas G.W. [et al.] Indexing by Latent Semantic Analysis // JASIS. 1990. Vol. 41. P. 391–407.

АЛГОРИТМ ОБНАРУЖЕНИЯ DDOS-АТАК НА ОСНОВЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТРАФИКА

Д.Н. Одинец, В.В. Носков

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

Алгоритм анализирует информацию о характеристиках заголовка трафика [1], чтобы обнаружить вредоносное ПО DDoS-атаки с подменой IP. Его этапами являются извлечение, анализ и обнаружение аномальных пакетов. На первом этапе на основе анализа пакетов коммутатора уровня 3 создается таблица T1 путем извлечения информации о функциях, включая IP-адрес и MAC-адрес заголовков Ethernet, текущее время, временной интервал.

На втором этапе вычисляются статистические характеристики (частоты встречаемости). для обнаружения вредоносных программ DDoS-атак с подменой IP. На третьем этапе извлеченные IP-адреса и MAC-адреса из заголовков Ethernet трафика в режиме реального времени сравниваются с атрибутивной информацией, представленной в таблице T1, чтобы определить, произошло ли заражение DDoS-атак с подменой IP-адресов вредоносным ПО. Если есть совпадение между IP-адресами и MAC-адресами трафика в реальном времени со значениями свойств в T1, делается вывод о вероятном заражении DDoS-атаки с подменой IP-адресов вредоносными программами. В результате исследований получены графические зависимости времени обнаружения DDoS-атаки с подменой IP от входных параметров.

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2006. 957 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЗАКРЫТЫХ ИНФОРМАЦИОННЫХ СЕТЯХ

А.Л. Панин, А.А. Белоус

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

Закрытые информационные сети (ЗИС) широко применяются в различных сферах человеческой деятельности. Их основной функцией является обеспечение оперативной и достоверной информацией пользователей. Одной из их особенностей является ограниченная пропускная способность, ввиду использования каналозакрывающей аппаратуры. В условиях повседневной деятельности этого, как правило, достаточно.

Однако, при выходе из строя нескольких основных узлов сети увеличивается объем служебного трафика ввиду необходимости построения новой схемы маршрутизации сети, которая может длиться от нескольких минут до нескольких часов. Перегрузка каналов может привести к отсутствию или неприемлемому запаздыванию одного или нескольких видов информации, то есть нарушению целостности, доступности, а также увеличению объема служебной информации.

Для решения задачи обеспечения целостности и доступности сетевого оборудования и уменьшения объема служебной информации при деструктивном воздействии необходимо использовать эффективную адаптивную схему маршрутизации. Разработка подобного решения является сложной оптимизационной задачей, поскольку сеть функционирует в условиях воздействия неопределенных факторов нестохастической природы (требуется учитывать топологию сети, параметры каналов связи, различие в обработке разных типов трафика и др.). Проведение натурных исследований для повышения качества передачи информации на введенных в эксплуатацию сетях сопряжено с огромными техническими, административными и финансовыми трудностями. В виду этого, альтернативой является построение моделей, обеспечивающих возможность исследования процессов обмена информации в сетях. Построение моделей технических систем с учетом воздействия на них факторов нестохастической природы является крайне сложной задачей в виду отсутствия общей теории и сложности формализации процессов, протекающих в указанных системах. В настоящее время для преодоления трудностей, вызванных обработкой неопределенных знаний, широко используется математический аппарат нечеткой логики.

Для оценки эффективности применения существующих и новых методов маршрутизации разработана комплексная математическая модель ЗИС, включающая в себя модели оценки целостности и доступности информации в условиях внешних деструктивных воздействиях. В основу модели положена нечеткая нейронная сеть, реализующая работу системы прямого нечеткого вывода типа Тагаки-Сугено [1]. Входными данными системы нечеткого вывода являются представленные в формализованном виде показатели целостности информации и объема сетевых ресурсов, требующихся для передачи информации, а также лингвистическая переменная – деструктивное воздействие, в результате которого выходит из строя сетевое оборудование. Результатом работы машины прямого нечеткого вывода является оптимальный маршрут по критерию максимума вероятности целостности информации и минимальный объем сетевого ресурса, требующегося для ее передачи. Программная реализация машины прямого нечеткого вывода выполнена с использованием программного расширения Fuzzy Logic для системы моделирования MATLAB. Таким образом, разработанная комплексная математическая модель ЗИС позволяет анализировать эффективность применения существующих и разработанных методов маршрутизации, а также определять оптимальные маршруты передачи информации по критерию максимума вероятности целостности и доступности в условиях деструктивного воздействия на сеть.

Список литературы

1. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая линия – Телеком, 2007. 384 с.

КРИПТОГРАФИЧЕСКАЯ СХЕМА ОБУЧЕНИЯ С ОШИБКАМИ НА РЕШЕТКАХ С ДОПОЛНИТЕЛЬНЫМ КОДИРОВАНИЕМ ПОЛЯРНЫМ КОДОМ

В.В. Панькова, С.Б. Саломатин

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

Гомоморфное шифрование обеспечивает безопасную обработку данных непосредственно над шифротекстом, результаты вычислений которого также шифруются. Известны схемы асимметричного шифрования для побитового шифрования потока данных. Схемы обучения с ошибками (RLWE), полностью гомоморфны и имеют два подпроцесса: один связан с целочисленными векторами, принятия решений, а другой связан с целочисленными полиномами [1].

Существует компромисс в схемах шифрования с открытым ключом (PKE), основанных на кольцевом обучении с ошибками (RLWE), а именно: требование более широкого распределения ошибок для повышения безопасности.

Прямым решением этой проблемы является код исправления ошибок [2]. Однако применение корректирующих кодов к криптографическим схемам имеет свои особенности. Во-первых, остаточный компонент ошибки, полученный при расшифровании, имеет коррелированные коэффициенты. Наиболее распространенные коды с исправлением ошибок предполагают, что шум канала является независимым и не имеет памяти. Это объясняет, почему в существующих схемах PKE на основе RLWE используются только простые методы исправления ошибок. Во-вторых, компонент остаточной ошибки имеет коррелированные коэффициенты, что затрудняет точную оценку частоты отказов расшифрования. В-третьих, большинство кодов, исправляющих ошибки, плохо спроектированы с точки зрения безопасности, например, декодирование синдрома носит непостоянный характер во времени.

Одним из путей решения задачи является применение схемы полярного кодирования [3] систем PKE на основе RLWE. Биноминальное распределение весов и предположение о «независимости» используется для получения некоррелированного остатка шумовой компоненты, а стратегия беспроводной связи, отказ, применяется для построения полярных кодов.

Моделирование схемы показало, что предлагаемая структура повышает запас по частоте отказов расшифрования. Полярное кодирование и декодирование имеют квазилинейный характер сложности и обладает внутренней поддержкой реализаций с постоянным временем.

Список литературы

1. Гаража А.А., Герасимов И.Ю., Николаев М.В. Об использовании библиотек полностью гомоморфного шифрования // International Journal of Open Information Technologies. 2021. Vol. 9, no. 3. С. 11–20.

2. Fritzmann T., Poppelmann T., Sepulveda J. Analysis of error correcting codes for lattice-based key exchange // International Conference on Selected Areas in Cryptography. 2018. P. 369–390.

3. Гладких А.А., Климов Р.В., Чилихин Н.Ю. Методы эффективного декодирования избыточных кодов и их современные приложения. Ульяновск : УлГТУ, 2016. 258 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОГО РЕПОЗИТОРИЯ DOCKER

С.Н. Петров[1], В.Н. Ганисевский[2], А.Д. Алам Яр[2]

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

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

Создание защищенного локального репозитория Docker может быть полезным для организаций, которые хотят иметь контроль над использованием образов Docker в своей среде. Защищенный репозиторий Docker призван обеспечить безопасность и целостность образов Docker, предотвратить использование поддельных образов.

После установки Docker и создания локального репозитория необходимо настроить механизмы аутентификации и авторизации пользователей для доступа к репозиторию. Первым делом создается файл конфигурации для авторизации Docker, для чего этого можно использовать достаточно популярную утилиту htpasswd, которая создает файл с именами пользователей и хэшами паролей. Результатом работы утилиты станет файл «docker-auth» с пользователем «user» и запросом пароля. Созданный файл конфигурации указывается в качестве источника аутентификации. Необходимо настроить клиентский доступ к репозиторию, используя учетные данные авторизации, для чего создается файл конфигурации Docker в домашней директории пользователя.

Доступ к репозиторию осуществляется по протоколу HTTPS.

Содержимое репозитория, Docker-образы, также должны быть защищено. Одним из механизмов защиты является цифровая подпись, которая позволяет обеспечить целостность образов Docker при их распространении и использовании. Это достигается путем создания уникального идентификатора образа (хэш-суммы) и его подписи цифровым сертификатом, который удостоверяет авторство создателя. Чтобы создать цифровую подпись образа Docker, сначала необходимо создать закрытый ключ (private key) и соответствующий ему открытый ключ (public key), используя криптографические алгоритмы. Затем создается подпись образа, используя закрытый ключ. Подпись включает хэш образа и другие метаданные. Когда образ Docker загружается на другой сервер или устройство, проверка цифровой подписи образа позволяет убедиться в его целостности и подлинности. Если образ был изменен, подпись становится недействительной, что предотвращает использование поддельных образов и защищает от возможных атак.

Для создания и использования цифровых подписей образов Docker существует множество инструментов и сервисов, таких как Notary, Docker Content Trust, Sigstore и других. Эти инструменты позволяют создавать и управлять цифровыми подписями, а также упрощают процесс проверки подписей при загрузке и использовании образов.

ВОПРОСЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В КУРСАХ ПЕРЕПОДГОТОВКИ СЛУШАТЕЛЕЙ

В.А. Полубок, А.А. Косак

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

Не секрет, что стремление защитить свои интересы было присуще человеку с давних пор. Еще в древности он использовал различные варианты кодирования информации, изобретал устройства, которые бы способствовали созданию более стойких шифров, и при этом обеспечивал легкость шифрования.

Существует множество протоколов программного шифрования, которые защищены от взлома в различной степени. Отличие криптографических алгоритмов защиты информации от всех других методов защиты основано на свойствах самой информации с исключением свойств материальных носителей. Самыми распространенными среди средств криптографической защиты являются следующие типы протоколов: симметричные, в которых для шифрования и расшифровки используется один и тот же ключ: DES, AES, ГОСТ 28147-89, Camellia, Blowfish, RC4 и т.д. [1].

Анализ обучения слушателей переподготовки по специальностям, связанным с информационными технологиями, свидетельствует о недостаточной подготовке в области обеспечения информационной безопасности. Результаты анализа показывают, что в информационные курсы необходимо вводить темы, связанные с криптографической защитой информации. Для этих целей была модернизирована лабораторная работа в рамках курса «Основы алгоритмизации и программирования на языках высокого уровня», которая знакомит слушателей с основными принципами криптографической защиты данных. Знания, полученные в рамках данной работы, повысят уровень теоретической и практической подготовки слушателей, и в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Лебедев А.Н. Криптография с открытым ключом и возможности ее практического применения. Тем. сб. «Защита информации». 1992. Вып. 2.

ДОБАВЛЕНИЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ВИДЕОФАЙЛ ЧЕРЕЗ ИЗМЕНЕНИЕ МЕТАДАННЫХ

Н.В. Попеня

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

Добавление цифрового водяного знака в видеофайл через изменение метаданных является одним из способов внедрения информации в видеофайл с помощью стеганографии. Этот метод основан на изменении метаданных видеофайла. Метаданные видеофайла – это информация, связанная с видеофайлом, которая содержит дополнительную информацию о видео, не относящуюся к самому видео, но необходимую для его управления и организации. Метаданные могут содержать информацию о длительности видео, разрешении, формате, частоте кадров, звуковых дорожках, а также информацию о дате создания, настройках камеры и другие данные, которые могут быть изменены без влияния на содержимое видеофайла [1].

Метаданные могут быть внесены в видеофайл во время его создания, например, с помощью программного обеспечения для обработки видео или камеры, которая записывает видео, а также могут быть добавлены после создания видеофайла с помощью специальных программных инструментов.

Алгоритм метода внедрения информации в метаданные видеофайла может включать следующие этапы:

1. Выбор метаданных видеофайла, которые могут быть изменены. Обычно это атрибуты, связанные с авторством, датой создания, идентификатором камеры и т.д.

2. Кодирование информации: информация, которую необходимо внедрить, должна быть закодирована в форму, которую можно вставить в метаданные.

3. Изменение метаданных видеофайла. Информация в метаданных может быть изменена с помощью программного обеспечения, которое позволяет редактировать

метаданные видеофайла. Для этого нужно указать тип метаданных и вставить закодированную информацию.

4. Проверка целостности после внедрения информации в метаданные. Это можно сделать, используя программное обеспечение, которое позволяет проверять контрольную сумму видеофайла или сравнивать файлы до и после внедрения информации.

5. Проверка и подтверждение информации. После проверки целостности необходимо убедиться, что информация была успешно внедрена в метаданные и может быть извлечена из видеофайла. Это можно сделать с помощью программного обеспечения, которое позволяет просматривать метаданные видеофайла или извлекать информацию из них.

Этот метод имеет свои преимущества и недостатки. Среди преимуществ можно выделить то, что изменение метаданных не влияет на содержимое видеофайла и не приводит к потере информации. Кроме того, этот метод может быть легко реализован с помощью специальных программных инструментов. Однако недостатком является то, что этот метод может быть относительно легко обнаружен и удален с помощью различных инструментов для анализа метаданных видеофайла. Кроме того, некоторые форматы видеофайлов могут не поддерживать изменение метаданных.

Список литературы

1. Ганжур М.А., Дзюба Я.В., Панченко В.А. Особенности цифровой стеганографии как метода обеспечения сокрытия данных // Проблемы современного педагогического образования. 2018. № 59-4.

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЬ

Н.В. Попеня

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

Цифровой водяной знак на видео позволяет скрыть некоторую информацию (например, авторские права) в видеофайле таким образом, чтобы она была невидима для человеческого глаза, но могла быть извлечена специальным программным обеспечением. Цифровой водяной знак может содержать информацию о владельце контента, дате и месте создания, а также служить как индикатор подлинности видео. Частотный и пространственный методы внедрения цифрового водяного знака – это два различных подхода к добавлению цифрового водяного знака кадры видеопоследовательности с помощью компьютерной стеганографии [1].

Частотный метод нанесения цифрового водяного знака заключается во внедрении цифрового водяного знака в частотном диапазоне видеофайла. Для применения этого метода применяется преобразование Фурье, которое позволяет разложить кадры видеопоследовательности на его частотные компоненты. В результате этого преобразования, кадры представляется в виде набора коэффициентов, которые характеризуют амплитуду и фазу различных частотных компонент. Далее, водяной знак внедряется в некоторые из этих коэффициентов. Наиболее эффективным является использование низкоамплитудных компонент, чтобы изменения, внесенные в них, были незаметны для человеческого глаза. После внедрения водяного знака происходит обратное преобразование Фурье, чтобы получить кадры с внедренным водяным знаком.

Частотный метод нанесения цифрового водяного знака может быть эффективен, если кадры видеопоследовательности являются визуально сложными и содержат

большое количество деталей. Однако, этот метод может привести к потере качества изображения или видеофайла, если коэффициенты будут слишком сильно изменены.

Пространственный метод нанесения цифрового водяного знака заключается во внедрении цифрового водяного знака в пространственном диапазоне кадра видеопоследовательности. Для применения этого метода, водяной знак внедряется в сами кадры видеопоследовательности, путем изменения некоторых пикселей. Эти изменения должны быть достаточно малозаметны для человеческого глаза, чтобы не ухудшить качество видеопоследовательности.

Пространственный метод является более простым и менее трудоемким по сравнению с частотным методом, но менее эффективным в защите от копирования и изменения. Также, этот метод может быть более уязвимым для атак, так как злоумышленник может попытаться удалить или изменить водяной знак путем изменения или удаления измененных пикселей. Однако, пространственный метод может быть эффективным для некоторых кадров видеопоследовательностей, особенно если они содержат мало деталей или не предполагают сильных изменений.

Выбор между частотным и пространственным методом зависит от конкретных требований и условий применения. Частотный метод может быть более эффективен в случаях, когда визуальная целостность кадров видеопоследовательности является приоритетом, а пространственный метод может быть более подходящим в случаях, когда важнее защитить видео от несанкционированного использования.

Список литературы

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-ПРЕСС, 2009. 272 с.

РЕДАКТИРОВАНИЕ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АНОНИМИЗАЦИИ ИЗОБРАЖЕНИЙ И ВИДЕО В ИНТЕРНЕТЕ

Т.А. Пулко, А.А. Винокуров

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

Учреждение образования «Национальный детский технопарк», Минск, Беларусь

С ужесточением правил во всем мире, таких как GDPR ЕС, CCPA в США, PIPL в Китае и APPI в Японии, компании, государственные организации и частные лица обязаны защищать личную информацию, которая включает биометрические данные на изображениях и видео. Правила конфиденциальности в разных регионах устанавливают разные правовые основы для сбора и обработки данных, у них есть одна общая черта: согласие. В случае общедоступных видеоданных часто бывает невозможно запросить согласие у каждого субъекта данных. Позаботиться о конфиденциальности данных можно легко, используя автоматическую анонимизацию видео и изображений. В настоящий момент, для этого не требуется высокотехнологичное оборудование или специальный специалист. Технологии искусственного интеллекта чрезвычайно эффективны при обнаружении объектов и, таким образом, могут использоваться для автоматизации редактирования изображений и видео быстрым и безопасным способом без участия человека. Это можно сделать и вручную, однако для больших наборов данных или многочисленных PII в одном кадре, ручная работа утомительна, медленна и связана с высокими затратами. Автоматизированные решения, намного быстрее, и самый

простой способ защиты данных с камер - это программное обеспечение для деидентификации, основанное на искусственном интеллекте.

В Brighter Redact оптимизированы методы редактирования лиц и номерных знаков, при этом позволяют защитить личную информацию в изображениях и видеоданных. Рассмотрено размытие лица для изображений и видеоданных, как полностью автоматизированное решение для анонимизации, гарантирующее высочайшую точность и стандарты качества.

Это уникальное решение, в котором лица и номерные знаки заменяются синтетическими данными изображения с помощью генеративного искусственного интеллекта, совместимо с разработкой алгоритмов машинного обучения и аналитики [1].

Список литературы

1. Brighter AI's image & video anonymization solution [Электронный ресурс]. – Режим доступа: https://brighter.ai/product/. – Дата доступа: 16.04.2023.

МОДЕЛИРОВАНИЕ МЕТОДОМ PM6 СТРУКТУРНЫХ И ОПТИЧЕСКИХ СВОЙСТВ ДВУХ SiV ЦЕНТРОВ В НАНОАЛМАЗЕ КАК ВОЗМОЖНОГО ЭЛЕМЕНТА КВАНТОВОЙ АНТЕННЫ

В.А. Пушкарчук[1], А.П. Низовцев[2], Д.С. Могилевцев[2], С.Я. Килин[2], А.Л. Пушкарчук[3], С.А. Кутень[4], А.А. Хрущинский[4]

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

[2]*Институт физики им. Б.И. Степанова НАН Беларуси, Минск, Беларусь*

[3]*Институт физико-органической химии НАН Беларуси, Минск, Беларусь*

[4]*Институт ядерных проблем Белорусского государственного университета, Минск, Беларусь*

Квантовые антенны, как устройства, формирующие свет на уровне одиночных квантов, уже стали ключевыми элементами нанооптики и наноэлектроники. Квантовые антенны активно изучаются на предмет возможного применения в квантовых коммуникациях, квантовой визуализации и зондировании, а также в сборе энергии. Однако конструкция и оптимизация этих излучающих/приемных устройств еще недостаточно разработаны по сравнению с известными способами для обычных радиочастотных антенн [1]. Нами была предложена общая концепция квантовой антенны, как устройства, использующего такое свойство, как дискретность энергетических уровней излучателя. В качестве эмиттерной модели рассматриваются «кремниево-вакансионные» центры (SiV^-) в наноалмазе. В данной модели квантовый излучатель, состоящий из двух двухуровневых эмиттеров, может быть реализован с помощью пары центров окраски в алмазе, в частности – отрицательно заряженных центров «кремний-вакансия» SiV^-. В связи с этим, нами выполнено прямое компьютерное моделирования методами квантовой химии системы двух SiV центров, расположенных недалеко друг от друга в кластере алмаза. В работе квантово–химическим методом PM6 изучен пассивированный водородом кластер $C_{313}[2SiV^{-2}]H^{172}$, моделирующий наноалмаз, содержащий два заряженных отрицательно центра SiV^{-1} Для оценки оптической активности электронов, локализованных в области SiV^- центров, были проведены расчеты с использованием метода TD-SCF PM6. Для кластера $C_{313}[2SiV^{-2}]H_{172}$ был рассчитан спектр поглощения. Показано что, в запрещенной зоне двухцентровых кластеров формируются дублетные состояния,

соответствующие симметричным и антисимметричным состояниям пары Дикке взаимодействующих излучателей и, следовательно, возможно создание квантового излучателя, состоящего из пары эмиттеров, которыми являются два SiV^- центра.

Список литературы

1. Slepyan G.Y., Vlasenko S., Mogilevtsev D. Quantum Antennas // Adv. Quantum Technol. 2020. Vol. 3. P. 1900120.

ИСПОЛЬЗОВАНИЕ ХАРАКТЕРИСТИК РАСТРИРОВАНИЯ WEB-ДОКУМЕНТОВ ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ЭЛЕКТРОННЫЙ КОНТЕНТ

М.Г. Савельева, П.П. Урбанович

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

Одним из вариантов защиты от несанкционированного доступа и изменений электронного документа, являющегося контейнером, может стеганография [1]. При этом документ может быть создан на основе растровой или векторной графики, а оригинальный контент может быть преобразован из одного формата графики в другой. Если использовать растровую графику для текстовых документов-контейнеров, то при конвертации возникает проблема расплывания контуров букв и постепенного изменения цвета. Однако эту проблему можно использовать в своих целях, внедрив в защищаемый контент тайную информацию, например, цифровой водяной знак (ЦВЗ). Чтобы увеличить скорость передачи тайной информации, можно использовать наиболее часто встречающиеся оттенки среди переходных полутоновых оттенков растрированных символов.

Нами было проанализировано 50 страниц стандартизированного оформления текстовых документов в формате PNG (преобразованных из PDF). Анализ показал, что при конвертации PDF-документов в формат PNG наиболее часто встречаются оттенки из градации серого. Простые текстовые документы имеют наименьший разброс значений частоты появления оттенков (с кодом от 0 до 255). Пиковые значения (0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255) во всех распределениях (R, G, B) соответствуют цвету от черного (0) до белого (255) для 16 различных оттенков: 0 0 0; 17 17 17; …; 255 255 255). Так как белый цвет – это фон, то оставшиеся распределенных 15 оттенка соответствуют отображениям элементов буквенных символов [2]. Градация от черного к белому через 16 означает, что цветовой диапазон от чистого черного (0,0,0) до чистого белого (255,255,255) разбивается на 16 равных отрезков. То есть каждый отрезок представляет собой интервал значений для каждого из цветовых каналов: красного (R), зеленого (G) и синего (B). Каждый отрезок представлен определенным значением для каждого цветового канала, так что в каждом отрезке все три цветовых канала имеют одинаковое значение. Такой подход используется для создания равномерного и легко читаемого цветового пространства, которое может быть использовано для различных целей, включая создание цифровых изображений и видео, а также в стеганографических методах защиты авторских прав на электронный контент.

Эта информация может быть использована в качестве важной отправной точки при разработке методов стеганографической защиты электронного контента, таких как защита авторского права. Выбор подходящего цветового оттенка для внедрения тайной информации (например, цифрового водяного знака) позволяет увеличить пропускную способность метода и снизить эффективность некоторых атак на стеганоконтейнер.

Список литературы

1. Шутько Н.П., Листопад Н.И., Урбанович П. П. Моделирование стеганографической системы в задачах по охране авторских прав // Информационные технологии в промышленности (ITI`2015): тез. докл. Восьмой Междунар. науч.-техн. конф., Минск, 2015. С. 30–31.

2. Савельева М.Г., Урбанович П.П. Растрирование web-документов и использование его характеристик для стеганографической защиты авторских прав на электронный контент // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2023. № 1 (266). С. 54–63

ПРИМЕНЕНИЕ ПОЛУТОНОВЫХ ОТТЕНКОВ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ЭЛЕКТРОННЫЙ КОНТЕНТ

М.Г. Савельева, П.П. Урбанович

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

Создание точных копий электронных документов становится проще благодаря доступности цифрового контента в компьютерных сетях и электронных хранилищах [1]. Один из методов защиты электронного контента от несанкционированного использования или изменения – это стеганография, при которой тайная информация внедряется в защищаемый контейнер, который может быть создан из растровой или векторной графики, или преобразован из одного формата в другой. Однако при конвертации текстовых документов-контейнеров может возникнуть проблема растрирования текста. Тем не менее, эту проблему можно использовать для внедрения тайной информации в защищаемый контент.

В [2] приведена классификация букв в зависимости от формы штрихов (строчные и прописные графемы могут относиться к разным группам):

− буквы первой группы, состоящие только из вертикальных и горизонтальных штрихов (здесь и далее даются заглавные начертания знаков) – «Г», «Е», «Н» и др.;

− буквы второй группы, состоящие только из вертикальных, горизонтальных и наклонных линий – «А», «Ж», «И» и др.;

− буквы третьей группы, в которых прямые штрихи соединяются с округлыми – «Б», «В», «Ч» и др.;

− буквы четвертой группы (круглые буквы) – «З», «О», «С» и др.

При конвертировании из одного формата в другой буквы могут растрироваться (из векторной графики перейти в растровую). В таком случае для того, чтобы в электронном виде обработать графемы и внедрить в них тайное сообщение, разбиение на группы, описанное в [2], не подходит. Это связано с тем, что при растрировании букв с округлыми или наклонными элементами невозможно создать штрихи правильного виды (в частности, наклонные и округлые) с помощью квадратных пикселей.

Для выделения новых групп следует провести анализ преобладающих переходных полутоновых оттенков, возникающих при растрировании, для каждой буквы русского алфавита, что позволит разбить графемы на группы в зависимости от их особенностей отображения при растрировании.

Список литературы

1. Шутько, Н. П. Защита авторских прав на электронные текстовые документы методами стеганографии // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2013. № 6 (162). С. 131–134.

2. Тоотс Виллу. Современный шрифт. М.: Книга, 1966. 272 с.

СОЗДАНИЕ ВИДЕОКОНТЕНТА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

И.М. Салей, А.Ю. Богачёва

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

Фейковый видеоконтент, использующий аватары известных персон, до недавнего времени рассматривался почти исключительно с позиции нарушения требований информационной безопасности. В то же время, в 2021 году Минпросвещения России был утвержден паспорт стратегии «Цифровая трансформация образования», которая включает проект «Цифровая трансформация отрасли «Образование (общее)», реализация которого рассчитана на 2021–2030 годы и потребует создания, кроме прочего, подготовку современных учебных материалов, практикумов и видеолекций [1].

В работе рассматривается задача создания фейкового образовательного контента с использованием нейронных сетей. Целью работы было создание (генерация) видеолекций для более понятного и удобного обучения в университете. Для этого была проведена аналитика различных методов генерации текста и видео. Были выявлены преимущества и недостатки каждого метода в контексте создания фейкового контента.

Для генерации текста мы использовали нейросеть ChatGPT [2]. С ее помощью мы получили возможность создавать качественные фейковые тексты на любые темы, различной длины, которые звучат естественно и уместно. Тексты генерировались на основе заданных тематик лекций и были дополнительно отредактированы для повышения качества.

Для создания говорящих аватаров был использован онлайн сервис D-ID [3], позволяющий создать генеративные аватары, которые читают заданный текст выбранным вами голосом. Созданные аватары были интегрированы в видео лекции с помощью монтажа. Бесплатная версия данного сервиса позволяет выполнять преобразование изображений и текста в видео, синтезировать голос на более чем 100 языках, использовать встроенные аватары или загружать свои собственные. Сервис D-ID достаточно удобен в случае, если автор видеолекции испытывает некие сложности технического или психологического характера при съемке на камеру. Его использование весьма существенно упрощает создание видео с участием людей.

Использование аватаров в видеолекциях позволит студентам лучше усваивать материал, так как виртуальный преподаватель способен лучше визуализировать информацию и делать ее более доступной. Разработанный подход к созданию видео лекций может быть использован в образовательных учреждениях для обучения студентов различных научных направлений.

Список литературы

1. Паспорт стратегии Цифровая трансформация образования [Электронный ресурс]. - Режим доступа: https://docs.edu.gov.ru/document/ 267a55edc9394c4fd7db31026f68f2dd/ ?ysclid= lh2ga3b2ga632121553. – Дата доступа: 29.04.2023.

2. Introducing ChatGPT [Электронный ресурс]. – Режим доступа: https://openai.com/blog/chatgpt. – Дата доступа: 29.04.2023.

3. Digital People, Text-to-Video [Электронный ресурс]. – Режим доступа: https://d-id.com. – Дата доступа: 29.04.2023.

ЗАЩИТА КРИПТОГРАФИЧЕСКИХ УСТРОЙСТВ АЛГЕБРАИЧЕСКИМИ КОДАМИ ОБНАРУЖЕНИЯ МАНИПУЛЯЦИЙ

С.Б. Саломатин

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

Рассматривается проблема обнаружения алгебраических манипуляций (AMD) [1] по каналу связи, который частично передает информацию противнику. Модель предполагает, что злоумышленник вычислительно неограничен, и между отправителем и получателем нет общего ключа или коррелированной случайности.

Криптографические методы внедрения ошибок. Усовершенствованная модель злоумышленника, в которой злоумышленник знает каждую деталь криптографического устройства, включая код обнаружения ошибок, используемый для защиты устройства. Злоумышленник может выбрать определенные входы для устройства во время атак с внедрением ошибок. Более того, злоумышленник также может внедрить любой конкретный шаблон ошибки на выходе устройства. В этом случае злоумышленник имеет полный контроль не только над ненулевой ошибкой, но также над безошибочным выходом y и ошибочным [2].

Определим архитектуру, которая по-прежнему может обеспечить гарантированную вероятность обнаружения ошибок в рамках приведенной выше модели злоумышленника, строго защищенной криптографической архитектурой.

Конструкции АМД-кодов, основанные на введении случайности в информационные биты кода. В кодовой архитектуре избыточные биты кода определяются не только выходом y исходного устройства, но и случайными данными x, сгенерированными генератором истинных случайных чисел, который по умолчанию встроен в большинство криптографических устройств для инициализации ключа [3]. В основе кодовых структур лежат обобщенные коды Рида–Маллера и Рида-Соломона. Криптографические устройства, защищенные кодами AMD, имеют высокую вероятность обнаружения ошибки (сбоя).

Список литературы

1. Cramer R., Dodis Y., Fehr S. [et al.] Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors // Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, ser. EUROCRYPT’08. 2008. P. 471–488.

2. Bar-El, H., Choukri H., Naccache D. [et al.] The sorcerer’s apprentice guide to fault attacks // Proceedings of the IEEE. 2006. Vol. 94, no. 2. P. 370–382.

3. Sunar B., Martin W.J., Stinson D.R. A provably secure true random number generator with built-in tolerance to active attacks // IEEE Trans. Comput. 2007. Vol. 56, no. 1. P. 109–119.

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ БЕЛОРУССКОЙ АЭС

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

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

В БГУИР в 2023 году будет проводиться первый набор на новую специальность «Информационные и управляющие системы физических установок», которая относится к специальному высшему образованию и направлена на подготовку специалистов с присвоением квалификации «Инженер» и степени «Магистр» и сроком обучения 5,5 лет.

Основное место работы будущих выпускников – Белорусская АЭС. Атомная станция – высокотехнологичный ядерный объект, с повышенными требованиями к безопасному функционированию на протяжении длительного периода времени, который для Белорусской АЭС составляет 60 лет. Повышенные требования предъявляются и к обслуживающему персоналу, подготовка которого должна осуществляться на качественно новом и высоком уровне с учетом интенсивно развивающихся и совершенствующихся технологий, в том числе и информационных.

Современная система управления АЭС – это совокупность программно-технических средств (рабочих станций и серверов с установленным системным программным обеспечением, коммутаторов, устройств синхронизации времени и так далее), объединенных в локальную вычислительную сеть волоконно-оптическими линиями связи, а безопасность и защита информации – главные приоритеты при работе таких систем [1]. Выпускники, призванные для работы на АЭС должны обладать знаниями, умениями и навыками по нескольким смежным профилям обучения и такая тенденция со временем будет только усиливаться.

В рамках специальности «Информационные и управляющие системы физических установок» подготовка специалистов будет осуществляться на стыке интенсивно развивающихся направлений, таких как ядерная энергетика и физические установки, системы управления и IT-направление. В последнее время наметилась тенденция по внедрению информационных технологий в атомную, достаточно консервативную отрасль. В частности, «Росэнергоатом» проводит в настоящее время работы по созданию цифрового шаблона опыта эксплуатаций АЭС и планирует переход на модель управления в рамках интеллектуальной энергетической системы страны, что позволит управлять рисками кибербезопасности на имеющихся АЭС. Эти работы основаны на системополагающих рекомендациях МАГАТЭ [2]. Еще одной особенностью управления рисками кибербезопасности на АЭС является решение о изоляции системы управления от внешнего вмешательства, построение прочной системы внешней защиты.

Построение эффективной системы кибербезопасности АЭС является сложной, важной и ответственной задачей, для решения которой нужны специалисты, обладающие глубокими знаниями не только IT-направления, но и знаниями, связанными с принципами функционирования АЭС и ее системы управления. Подготовка таких специалистов и будет осуществляться в рамках специальности «Информационные и управляющие системы физических установок».

Список литературы

1. На площадке Балаковской АЭС ИТ-специалисты атомной отрасли обсудили цифровые решения. [Электронный ресурс]. – Режим доступа: https://rosatom.ru/

journalist/news/na-ploshchadke-balakovskoy-aes-it-spetsialisty-atomnoy-otrasli-obsudili-tsifrovye-resheniya/?sphrase_id=3973845. – Дата доступа: 28.04.2023.

2. Основные принципы безопасности атомных электростанций 75-INSAG-3 Rev.1. Доклад международной консультативной группы по ядерной безопасности. Вена: МАГАТЭ.

ОБЗОР ПУТЕЙ ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ ОПТИКО-ЭЛЕКТРОННЫХ СИСТЕМ ОБНАРУЖЕНИЯ

А.В. Сергеенко, А.Ю. Липлянин

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

На сегодняшний день одним из основных способов защиты и фиксирования факта несанкционированного проникновения на охраняемые объекты является использование оптико-электронных систем обнаружения. Как и всем оптико-электронным системам им свойственен ряд недостатков: чувствительность к погодным условиям, средствам маскировки, естественным преградам и т.п. Особенно эти недостатки негативно влияют на качество работы систем применяемых для охраны одиночных объектов, находящихся вне городской черты.

Существует несколько путей повышения эффективности работы оптико-электронных систем обнаружения:

1) аппаратные [1]:

– использование нескольких оптических каналов (мультиспектральные оптические системы);

– использование различий в поляризации светового потока, отраженного от объектов искусственного и естественного происхождения;

– разложение отраженного светового потока на спектральные составляющие (гиперспектральная съемка);

2) программные:

– разработка новых алгоритмов обнаружения объектов на изображениях, повышения качества и восстановления изображений;

3) Организационные:

– удаление предметов, мешающих обзору из зон видимости оптико-электронных систем;

– освещение участков обзора в темное время и при плохих погодных условиях и др.;

4) Комбинирование нескольких методов.

Список литературы

1. Беляев Б.И., Катовский Л.В. Оптическое дистанционное зондирование. Минск: БГУ, 2006. 455 с.

МЕТОДИКА ПРЕПОДАВАНИЯ ТЕМЫ «ГИДРОАКУСТИЧЕСКИЕ ДАТЧИКИ»

А.И. Серый

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

В учебных программах дисциплины «Технические средства и методы защиты информации» [1], изучение которой предусмотрено учебными планами отдельных физико-математических специальностей (в частности, «Компьютерная физика») возможно наличие темы «Гидроакустические датчики». Важное место в этой теме занимают вопросы, связанные с общими и индивидуальными характеристиками

отдельных устройств и классов устройств. Несмотря на быстрое развитие технических средств и методов защиты информации, следствием чего является постепенная утрата актуальности сведений о некоторых конкретных технических устройствах, общие принципы работы гидроакустических датчиков, решаемых ими задач, а также выбора мер борьбы с ними (при необходимости) можно считать относительно устойчивыми.

Каждый отдельно взятый гидроакустический датчик можно охарактеризовать по следующим пунктам. 1.1. Частотный диапазон. 1.2. Порог чувствительности и уровень устойчивости к помехам. 1.3. Происхождение сигналов (сигналы непосредственно от исследуемых объектов в случае пассивной разведки либо сигналы, отраженные от объектов, в случае активной разведки). 1.4. Принципы работы устройства съема и обработки информации с последующей передачей. 2.1. Места установки (системы водоснабжения, канализации, водяного отопления в помещениях; водоемы); трудности (с точки зрения, как злоумышленника, так и правоохранительных органов), возникающие при необходимости скрытой установки датчиков. 2.2. Назначение – перехват акустической (речевой или неречевой) информации, измерение глубины водоема, слежение за подводными лодками, дайверами, косяками рыб, крупными затонувшими объектами, подводным мусором и др. 2.3. Характер назначения – мирный, военный, промышленный и др.

Из приведенных пунктов можно делать вывод, что иногда (но не всегда) могут понадобиться перечисленные далее меры по борьбе с принятием акустических сигналов, во многом сходные с аналогичными общими мерами для каналов утечки информации в целом, перечисленными в [2]. 3.1. Меры по недопущению съема информации датчиком, связанные: а) с понижением уровня исходного сигнала (в том числе путем звукоизоляции); б) с зашумлением сигнала. 3.2. Меры по поиску датчиков. 3.3. Меры противодействия работе датчиков после их обнаружения: а) отключение; б) блокировка канала дальнейшей передачи информации; в) вывод датчика из строя. Приоритеты при выборе конкретных мер противодействия по сути не отличаются от перечисленных в [2] для технических каналов утечки информации в целом.

Список литературы

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Голубятников И.В., Солдатов А.А., Скрыль С.В. Технические средства и методы защиты информации. М.: Горячая линия–Телеком, 2012. 616 с.

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

СХОДСТВО КЛАССИФИКАЦИОННЫХ ПРИЗНАКОВ РАЗЛИЧНЫХ ТИПОВ УСТРОЙСТВ, ИЗУЧАЕМЫХ В РАМКАХ ДИСЦИПЛИНЫ «ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

А.И. Серый

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

В учебных программах дисциплины «Технические средства и методы защиты информации» [1], изучаемой студентами некоторых физико-математических специальностей (в том числе студентами специальности «Компьютерная физика») предусмотрено знакомство с разными типами устройств и систем. В качестве примеров можно назвать микрофоны (направленные, радио-, лазерные), тепловизионные приборы, приборы ночного видения, скрытые камеры, диктофоны, стетоскопы,

гидроакустические датчики, СВЧ- и инфракрасные передатчики, индикаторы поля, сканирующие компьютерные радиоприемники, радиопеленгаторы, анализаторы спектра, радиочастотомеры, фильтры сигналов, металлодетекторы, нелинейные локаторы и др.

Несмотря на принципиальное различие между различными типами устройств и довольно частое существенное различие между различными моделями устройств одного и того же типа, при составлении плана характеристики конкретной модели устройств заданного типа (либо всего типа устройств в целом) можно выделить вопросы, имеющие схожую словесную формулировку (за которой иногда может стоять и более-менее похожее содержание).

Ниже приведены примеры вопросов. Вопросы могут быть отнесены как ко всему типу устройств в целом, так и к определенным моделям (в этом случае сведения становятся более конкретными, определенными). Для разных типов устройств один и тот же вопрос может характеризоваться существенно различной степенью важности.

1. Типы сигналов (акустические, электромагнитные и др.). 2. Рабочий частотный диапазон. 3. Порог чувствительности и его зависимость от частоты. 4. Пределы габаритных размеров. 5. Диапазон масс. 6. Дальность действия. 7. Рабочие температурные пределы. 8. Физические законы, лежащие в основе функционирования. 9. Время непрерывной работы. 10. Средний срок службы. 11. Стоимость. 12. Производители. 13. Специфические классификационные признаки, характерные для заданного типа либо заданной модели. Вопросы могут быть использованы студентами при подготовке к контролю знаний.

Публикация является дополнением к [2].

Литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Голубятников И.В., Солдатов А.А., Скрыль С.В. Технические средства и методы защиты информации. М.: Горячая линия–Телеком, 2012. 616 с.

2. Серый, А.И. К вопросу о методике преподавания дисциплины «Технические средства и методы защиты информации» // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 86–87.

ЛОГИСТИЧЕСКАЯ МОДЕЛЬ «ДОСТОВЕРНОСТИ» ТЕХНОЛОГИИ БЛОКЧЕЙН

А.В. Сидоренко, М.Г. Волосач

Белорусский государственный университет, Минск, Беларусь

Одной из основных проблем применения технологии блокчейн является достоверность данных, что определяет необходимость применения эффективных алгоритмов шифрования. Они должны гарантировать достаточную криптографическую стойкость для информации в сети, а также обеспечить реализацию цифровой подписи при необходимости.

В работе для шифрования рассматривается алгоритм ассимметричного щифрования RSA. Алгоритм использует два ключа: открытый и секретный, которые вместе образуют пару ключей. Если сообщение было зашифровано открытым ключом, то расшифровать его можно ключом, известным только получателю переданной информации. При попытке взломать секретный ключ придется перебрать достаточно много комбинаций Например, при длине ключа в 256 бит и скорости подбора паролей 1024 в секунду потребуется перебрать 1,23+67 лет.

Нами предложен функционал программного продукта, предназначенного для обработки и анализа информации. Реализация программы проведена на языке C++.

Приводится пример работы компьютерной программы. Разработанный программный продукт обладает достаточно низкими системными требованиями. Особенностью данного программного продукта является возможность работы с мобильным телефоном.

Широкое распространение технологии «Интернет вещей» в различных сферах человеческой деятельности вызывает необходимость в обеспечении ключевых факторов: секретности, конфиденциальности, аутентификации передаваемой информации. Для сохранения связи между датчиками распределенных на большой территории пользователей и обеспечения достоверной передачи данных к облачным технологиям в настоящее время получают распространение системы на основе блокчейна и краевые вычисления [1]. Такие характеристики блокчейна, как: децентрализация, механизм консенсуса, шифрование данных и смартконтракты позволяют сохранить в базе данных и обеспечить конфиденциальность и аутентификацию передаваемой информации.

Нами предложен функционал программного продукта, предназначенного для получения, обработки и анализа информации с датчиков, совместимых с платой Arduino. Разработанный программный продукт обладает достаточно низкими системными требованиями и может быть запущен с использованием пакета Java, в частности, версии Java Runtime Envirioment. Особенностью данной системы является возможность работы с мобильным телефоном. При этом информация может быть передана на телефон и получена в виде сообщения электронной почты на компьютере.

Список литературы

1. Сидоренко А.В. Робототехника и блокчейн // Развитие информатизации государственной системы научно-технической информации: матер. XVII Междунар. конф., Минск, 20 сентября 2018 г. С. 111–114.

ЗАЩИТА ИНФОРМАЦИ В СИСТЕМАХ СВЯЗИ «ИНТЕРНЕТ ВЕЩЕЙ»

А.В. Сидоренко, М.К. Савченко

Белорусский государственный университет, Минск, Беларусь

Широкое распространение технологии «Интернет вещей» в различных сферах человеческой деятельности вызывает необходимость в обеспечении ключевых факторов: секретности, конфиденциальности, аутентификации передаваемой информации. Для сохранения связи между датчиками распределенных на большой территории пользователей и обеспечения достоверной передачи данных к облачным технологиям в настоящее время получают распространение системы на основе блокчейна и краевые вычисления [1]. Такие характеристики блокчейна, как: децентрализация, механизм консенсуса, шифрование данных и смартконтракты позволяют сохранить в базе данных и обеспечить конфиденциальность и аутентификацию передаваемой информации.

Нами предложен функционал программного продукта, предназначенного для получения, обработки и анализа информации с датчиков, совместимых с платой Arduino. Разработанный программный продукт обладает достаточно низкими системными требованиями и может быть запущен с использованием пакета Java, в частности, версии Java Runtime Envirioment. Особенностью данной системы является возможность работы с мобильным телефоном. При этом информация может быть передана на телефон и получена в виде сообщения электронной почты на компьютере.

Список литературы

1. Сидоренко А.В. Робототехника и блокчейн // Развитие информатизации государственной системы научно-технической информации: матер. XVII Междунар. конф., Минск, 20 сентября 2018 г. С. 111–114.

ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Р.С. Симанович

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

Криптографическая защита данных в облачных вычислениях является актуальной темой, так как облачные вычисления становятся все более распространенными и важными для бизнеса. Вместе с тем, сохранение конфиденциальности, целостности и доступности данных остается важным вопросом при использовании облачных вычислений.

Облачные вычисления создают новые угрозы для безопасности данных, такие как возможность несанкционированного доступа, утечки данных и атаки с целью их изменения. Криптографические методы являются важным инструментом для защиты данных в облачных вычислениях, однако существует необходимость в разработке новых методов и алгоритмов, которые учитывают специфические условия облачных вычислений.

При выборе метода криптографической защиты данных в облачных вычислениях необходимо учитывать различные факторы, такие как тип хранимых данных, уровень конфиденциальности, требования к скорости и доступности данных. Одним из главных вызовов при использовании криптографии в облачных вычислениях является баланс между уровнем безопасности и производительностью системы.

В современных облачных вычислениях все большее значение приобретает гомоморфное шифрование, которое позволяет выполнять вычисления с зашифрованными данными без необходимости их расшифровки.

Одним из ключевых требований к использованию криптографии в облачных вычислениях является соблюдение нормативных требований и стандартов безопасности данных, таких как GDPR, HIPAA, PCI DSS и другие.

В заключении, использование криптографии для защиты данных в облачных вычислениях является важным и сложным вопросом, который требует учета многих факторов, таких как требования безопасности данных и особенности архитектуры облачных систем. Правильный выбор метода криптографической защиты данных может обеспечить высокий уровень защиты данных и снизить риски утечки информации [1–7].

Список литературы

1. Криптография в цифровых технологиях [Электронный ресурс]. – Режим доступа: https://ecpexpert.ru/kriptografiya-v-tsifrovykh-tekhnologiyakh/. – Дата доступа: 01.05.2023.
2. «Облачные» вычисления и проблемы их безопасности [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/oblachnye-vychisleniya-i-problemy-ih-bezopasnosti. – Дата доступа: 01.05.2023.
3. Облачная криптография [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/oblachnaya-kriptografiya. – Дата доступа: 01.05.2023.

4. Интегральная модель оценки эффективности и рисков облачных ИТ-сервисов для внедрения на предприятие [Электронный ресурс]. – Режим доступа: https://fundamental-research.ru/ru/article/view?id=38350. – Дата доступа: 01.05.2023.

5. Ковалевский В., Максимов В. Криптографические методы // КомпьютерПресс. 1993. № 5.С. 31–34.

6. Варновский Н., Шокуров А. Гомоморфное шифрование // Труды Института системного программирования РАН. 2007. Т. 12. С. 27–36.

7. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993. 216 с.

СПИН-ЗАВИСИМЫЙ ТРАНСПОРТ В НАНОСТРУКТУРАХ ФЕРРОМАГНЕТИК/ОКСИДНЫЙ ДИЭЛЕКТРИК/ФЕРРОМАГНЕТИК

Т.Н. Сидорова, А.А. Назаренко, Д.А. Подрябинкин

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

Разработка элементов резистивной памяти (RRAM) в настоящее время весьма актуальна [1]. Спин-зависимый токоперенос в элементах RRAM позволяет адаптировать такие элементы для применения в спинтронике [2]. Однако остаются еще нерешенные проблемы, связанные с пониманием особенностей спин-зависимого транспорта в наноструктурах ферромагнетик/оксидный диэлектрик/ферромагнетик. В настоящей работе представлены результаты исследования закономерностей спин-зависимого транспорта в наноструктурах ферромагнетик/оксидный диэлектрик/ ферромагнетик.

Установлена взаимосвязь степени спиновой поляризации электронов в оксидном диэлектрике на его ловушечных и интерфейсных состояниях от степени их начальной спиновой поляризации, создаваемой ферромагнитным электродом, а также от напряженности внешнего электрического поля в оксидном диэлектрике. Данная взаимосвязь была рассмотрена для потенциальных рельефов, представляющих одиночный потенциальный барьер и два потенциальных барьера, разделенных потенциальной ямой. В первом случае с ростом начальной поляризации и увеличением внешнего потенциала степень спиновой поляризации возрастает почти линейно до 10 %. Во втором случае для относительно узкой ямы зависимость степени поляризации электронов от приложенного потенциала имеет сверхлинейный характер, а ее величина достигает 20 %. Однако для широкой потенциальной ямы меняется характер зависимостей и возникает область насыщения. При этом величина степени спиновой поляризации не превышает 7,5 %. Такое поведение объясняется селективностью резонансного прохождения спин-зависимых электронов через дискретные уровни в квантовой яме и интерференцией электронных волн, отраженных от второго барьера. Установленные взаимосвязи позволяют конструировать спинтронные элементы резистивной памяти на основе гетероструктур ферромагнетик/оксидный диэлектрик/ферромагнетик с управляемой спиновой поляризацией для получения максимальной эффективности элементов резистивной памяти.

Список литературы

1. Slesazeck S., Mikolajick T. Nanotechnology. 2019. Vol. 30, no. 35. P. 352003.

2. Ito D. [et al.] ECS Transations. 2015. Vol. 69, no. 3. P. 111–115.

МОДЕЛЬ ТОКОПЕРЕНОСА В СПИНОВОЙ ЯЧЕЙКЕ ПАМЯТИ

Т.Н. Сидорова, Д.А. Подрябинкин

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

Среди элементов систем обработки информации, перспективных для мега- и гигагерцового диапазона частот, спиновые транзисторы и ячейки памяти представляют наибольший практический интерес. Среди возможных конструкций этих элементов особенно привлекательными являются те, в которых нет необходимости применять внешнее магнитное поле, а расщепление энергетических электронных состояний по спину и управление потоком спин-поляризованных электронов достигается за счет использования спин-орбитального взаимодействия и связанной с ним передачей спина. В этой связи разработка спинтронных элементов памяти в настоящее время весьма актуальна [1]. Но остаются еще нерешенные проблемы, связанные с пониманием особенностей спин-зависимого транспорта в наноструктурах.

В данной работе представлена разработанная модель токопереноса в спиновой ячейке памяти на основе кремниевой наноструктуры ферромагнетик/туннельный диэлектрик/кремний/туннельный диэлектрик/ферромагнетик. Модель учитывает туннелирование электронов из ферромагнитного электрода (CoFeB) через диэлектрик в кремний, их диффузионно-дрейфовый токоперенос в кремниевом канале с учетом времени спиновой релаксации порядка 10 нс, а также туннелирование в ферромагнитный коллектор (CoFe) также через диэлектрик толщиной 1–2 нм. Для расчета коэффициента туннельной прозрачности диэлектриков толщиной 1–2 нм использовался метод фазовых функций, позволяющий учитывать параметры барьера, потенциал сил изображения, включать сложный потенциальный рельеф границ раздела и в объеме диэлектрика. Модель позволяет определить величину тока для каждой спиновой компоненты – спин-вверх и спин-вниз и рассчитать величину магнитосопротивления. Показано, что в случае использования потенциалов достаточно сложного вида (негладких, или имеющих особенности) модель позволяет существенно упростить расчеты и интерпретацию получаемых результатов по сравнению с использованием уравнения Шредингера. Модель спин-зависимого токопереноса в кремнии включает диффузионно-дрейфовые составляющие для каждой спиновой компоненты с учетом длины спиновой диффузии, коэффициента диффузии и времени спиновой релаксации по механизмам Эллиота–Яфета и Дьяконова–Переля, а также с учетом таких механизмов рассеяния как рассеяние на ионизированных примесях и фононах.

Список литературы

1. Jafari A. [et al.] J. Low Power Electron. Appl. 2022. Vol. 12 (4). P. 63.

СИСТЕМА ЛИНГВИСТИЧЕСКОГО АНАЛИЗА ДАННЫХ

В.Б. Соколов

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

Предлагается разработать систему, позволяющую в обрабатываемых данных находить определенные закономерности, дающие возможность маркировать людей по группам интересов, а также выявлять скрытые закономерности о их намерениях.

Целью данной системы является оказание противодействия современным методам ведения информационной войны, а также нейтрализации ее последствий в первую очередь на высокотехнологичный сектор.

Задачей представляемой системы является выявление уникальных словарей групп, подвергшихся влиянию, а также, определение по нечеткому анализу степени внедрения этих словарей в социум для дальнейшей ретрансляции.

Реализация системы лингвистического анализа данных позволит выделить группы без семантического анализа, который без углубленной проработки группы, а также ее целей просто не возможен.

В случае явного подозрения на криминал можно использовать системы допроса, основанные на применении интерфейса мозг – компьютер, с демонстрацией ряда изображений с высокой частотой следования – так называемый визуальный анализатор человека на узнавание, срабатывающий быстрее, чем происходят процессы мышления. Ряд изображений составляется на основе словарей и предполагаемой семантики. Это позволит работать значительно эффективней.

Реализация системы лингвистического анализа базируется на использовании определенного и необходимого функционала, а именно - анализа контента социальных сетей, отрисовка карты распределения словарей по типу карт Кохонена, K-Means, K-Means++ и K-Medoids, Partitioning Around Medoids (PAM), а также буферных зон (частичное влияние).

Система лингвистического анализа данных представляет собой самообучающуюся систему, способную маркировать пользователей соцсетей в соответствии с их предпочтениями на основе анализа данных активности в соцсетях: текст (в т.ч. графические элементы – эмодзи), реакции (лайки, репосты и т. д.), производить оценку активности в социальных группах.

Сбор исходных данных для обработки системой лингвистического анализа осуществляется применением парсинга данных в соц. сетях

Для реализации системы лингвистического анализа используются различные интерфейсные системы, позволяющая работать с данными сторонним пользователям, различные веб интерфейсы, приложения.

Обучение системы лингвистического анализа данных предусматривает использование известных алгоритмов и систем, позволяющих взаимодействовать человеку и системе лингвистического анализа для обучения последней.

Подсистема хранения и обработки данных системы лингвистического анализа данных использует хорошо известные инфраструктурные решения для вычислений, хранения, сбора и обработки данных. Облачные и стационарные системы.

Методы реализации системы лингвистического анализа данных базируются на двухэтапном принципе. 1. Создание базы данных (Big Data). 2. Обработка текста VSM, LSA. Алгоритмическая реализациия системы лингвистического анализа данных представляет собой классическую последовательность действий, состоящих из следующих этапов. 1. Сбор экспериментальных данных. 2. Выполнение кластеризации обозначенными методами, определение подходящего значения k. 3. Анализ полученных результатов. 4. В случае если остаются неясности с группами – изменение параметров кластеризации, до момента, когда число несоответствий будет укладываться в допустимый диапазон. 5. Проработка целевых групп.

ОРГАНИЗАЦИЯ СИСТЕМЫ ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Д.В. Солодкий

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

В современном мире повсеместной цифровизации все большую значимость приобретает защита информационных ресурсов как юридических, так и физических лиц. По данным positive technologies общее количество успешных инцидентов, которые привели к негативным последствиям в 2022 году увеличилось на 20,8%. Связано это с возросшим напряжением в киберпространстве. Значительное влияние оказывает и рост рынка киберпреступности: злоумышленники расширяют теневой бизнес. Тем временем в связи с массовыми утечками данных появляется возможность проведения атак с использованием скомпрометированной информации о пользователях. В 2023 году эти же причины послужат еще большему росту числа атак. Базовой, а зачастую и основной защитой от злоумышленников является системы парольной аутентификации.

Анализ литературного материала показал, что несмотря на большое количество материалов по данной теме, проблема все еще актуальна, так как более 40 % успешных атак на организации связан с компрометацией учетных данных пользователей информационных систем.

Целью работы является изучение методов и средств получения доступа к учетным записям пользователей.

Для этого необходимо решить следующие задачи.

1. Определить способы компрометации учетных данных.
2. Освоить методы и средства получения доступа.
3. Провести пинтесты на типовых информационных системах.
4. Определить средства противодействия данным киберугрозам.

Практическое применение результатов исследования возможно в целях повышения уровня защищенности информационных систем.

Выводы.

1. Методы социальной инженерии являются действенным средством атак.
2. Противодействие уязвимостям нулевого дня (и прочим программным уязвимостям) требует высокой скорости реакции от служб ИБ.
3. Противодействие современным вызовам в сфере ИБ требует комплексного подхода к системам защиты.

Рекомендации: при проектировании информационной системы необходимо учитывать разные виды угроз и применять комбинированные методы и средства ЗИ. Современная система ЗИ обязательно должна включать в себя UTM, SIEM и DLP модули, настроенные и взаимосвязанные между собой.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс]. – 2023. – Режим доступа: https://www.ptsecurity.com. – Дата доступа: 04.04.2023.
2. Атаки на домен [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com. – Дата доступа: 06.04.2023.
3. Бесконтрольный привилегированный доступ: как снизить риски для бизнеса [Электронный ресурс]. – 2023. – Режим доступа: https://www.anti-malware.ru. – Дата доступа: 09.04.2023.

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ МОБИЛЬНОГО ДЕТЕКТОРА ЦВЕТНЫХ ИЗОБРАЖЕНИЙ

В.А. Столер, М.М. Клещенок

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

Разработано веб-приложение, предоставляющее пользователю мобильного устройства возможность загрузки графических изображений объектов различного назначения и дальнейшего анализа их цвета. По результатам этого анализа пользователю выводится текстовая характеристика выбранного фрагмента (пикселя) объекта, а также параллельно выводится звуковое описание его цвета.

В работе приведены особенности работы веб-приложения и возможный потенциал для дальнейшего развития и разработки. Составлен алгоритм работы приложения, состоящий из описанных ниже трех основных этапов.

На первом этапе, обработчиком события addEventListener распознается событие касания изображения. Само изображение располагается на встроенном в язык элементе canvas. Обращаясь к canvas можно получить двумерные координаты расположения пикселя, на котором произошло событие касания. Далее методом getImageData можно получить информацию об изображении, передать его в аргументы метода размер 1×1, узнать параметры конкретного пикселя, взяв его rgba-значение.

На втором этапе идет перевод цветовой характеристики из системы RGBA в цветовую систему HSL за счет созданной функции конвертации. Такой перевод необходим для анализа цвета именно в системе HSL, которая представляет собой комбинацию трех значений: тон, насыщенность и светлота. Для базовой работы приложения достаточно опираться только на значение тона, которое показывает угол по цветовому кругу и на значение светлоты, показывающее расстояние от центра круга.

На третьем этапе происходит анализ значения цвета блоком условия. Для оптимизации процесса анализа может быть написан цикл, состоящий из необходимого числа итераций по проверке подходящего цвета. И далее, когда условие проверки возвращает булево значение «true», аудиосистема устройства выводит название цвета в голосовой форме.

В результате был разработан мобильный цветовой детектор со встроенным веб-приложением, работа которого построена на обработке графического изображения, преобразующего численную характеристику цвета в его аудио-название.

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПОРОГОВЫХ УРОВНЕЙ РЕГИСТРАЦИИ ОПТИЧЕСКИХ ИЗЛУЧЕНИЙ В КАНАЛАХ ОДНОФОТОННОЙ КВАНТОВО-КРИПТОГРАФИЧЕСКОЙ СВЯЗИ

А.М. Тимофеев

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

При создании систем однофотонной квантово-криптографической связи одной из наиболее важных задач является обеспечение наименьших потерь передаваемой информации [1–3]. В этой связи целесообразно использовать высокочувствительные приемные модули, такие, как счетчики фотонов. Поскольку в известных литературных источниках отсутствует методика определения нижнего и верхнего пороговых уровней регистрации оптических излучений при передаче данных, обеспечивающих наименьшие потери передаваемой информации применительно к квантово-криптографическим каналам связи, это являлось целью данной работы. Разработана

методика выбора нижнего и верхнего пороговых уровней регистрации при передаче двоичных данных, которая учитывает статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов и позволяет достичь наименьших потерь информации в квантово-криптографических каналах связи с приемником на основе счетчика фотонов с мертвым временем продлевающегося типа.

Список литературы

1. Щеглов А.Ю. Анализ и проектирование защиты информационных систем. СПб., Профессиональная литература, 2017.

2. Тимофеев А.М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи // Вестник ТГТУ. 2019. Т. 25, № 1. С. 36–46.

3. Тимофеев А.М. Исследование вероятности стирания двоичных символов «0» при возникновении ошибочной регистрации данных в квантово-криптографическом канале связи с приемником на основе счетчика фотонов // Вестник связи. 2023. № 1. С. 46–52.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ МЕРТВОГО ВРЕМЕНИ СЧЕТЧИКА ФОТОНОВ НА ВЕРОЯТНОСТЬ ОШИБОЧНОЙ РЕГИСТРАЦИИ ДВОИЧНЫХ СИМВОЛОВ В КАНАЛЕ КВАНТОВО-КРИПТОГРАФИЧЕСКОЙ СВЯЗИ

А.М. Тимофеев, М.А. Наумов

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

Государственное предприятие «НИИ ТЗИ», г. Минск, Республика Беларусь

В настоящее время достаточно интенсивное развитие получают системы связи, построенные на базе квантово-криптографических каналов связи, т. к. они характеризуются абсолютной скрытностью и конфиденциальностью передаваемой информации [1, 2]. Добиться столь высокого уровня информационной безопасности становится возможным, в частности, при использовании приемного оборудования, обеспечивающего минимальную вероятность ошибочной регистрации данных для заданных технико-эксплуатационных показателей [1, 2]. Поскольку в известных литературных источниках оценка вероятности ошибочной регистрации данных квантово-криптографических каналов связи отсутствует, это являлось целью данной работы. Применительно к счетчикам фотонов с мертвым временем продлевающегося типа получено выражение для оценки вероятности ошибочной регистрации двоичных данных. Установлено, что рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средней скорости счета сигнальных импульсов, при которой достигается наименьшее значение вероятности ошибочной регистрации данных.

Список литературы

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. [и др.] Квантовая криптография: идеи и практика. Мн., Белорус.наука, 2007.

2. Тимофеев А.М. Оценка влияния вероятности стирания двоичных символов «0» на вероятность ошибочной регистрации данных в квантово-криптографическом канале связи // Системный анализ и прикладная информатика. 2022. № 2. С. 62–65.

ПОДГОТОВКА МАГИСТРАНТОВ СПЕЦИАЛЬНОСТИ «РАДИОСИСТЕМЫ И РАДИОТЕХНОЛОГИИ» В ОБЛАСТИ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ

Н.А. Титович, З.Н. Мурашкина

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

В вопросах обеспечения защиты информации важную роль играет проблема электромагнитной совместимости (ЭМС). Электрические, электромагнитные и программные каналы передачи информации являются основными в современных радиоэлектронных системах (РЭС). Следовательно, и утечки по этим каналам являются основными. Любое электронное средство всегда находится во взаимодействии с другой электроникой, при этом постоянно существует риск их взаимного негативного влияния. Известно большое количество решений, позволяющих защитить радиосредства от всевозможных электромагнитных помех (ЭМП) помех, сократить их помехоэмиссию до допустимых норм. Это как схемотехнические решения (выбор менее восприимчивой к воздействию ЭМП элементной базы, защитные каскады и фильтры) и конструктивные (использование экранированных кабелей и корпусов), так и системные методы обеспечения ЭМС. Все выше изложенное выдвигает более высокие требования к качеству подготовки специалистов в этой области. С этой целью был разработан электронный образовательный ресурс «Оптимизация радиосистем по критериям электромагнитной совместимости» для специальности 1-39 80 01 «Радиосистемы и радиотехнологии».

В основу преподавания данной дисциплины положен системный подход к обеспечению ЭМС. Он предполагает рассмотрение проблемы защиты от помех уже на этапе выбора элементной базы: полупроводниковых приборов (ПП) и интегральных микросхем (ИМС). В разделе «ЭМС радиотехнических элементов и цепей» рассмотрены вопросы влияния ВЧ и СВЧ помех на работоспособность ПП и ИМС, изложены критерии оценки восприимчивости элементов радиоаппаратуры к воздействию ЭМП, экспериментальные и расчетные методики оценки их восприимчивости. Рассмотрены также причины возникновения внутрисистемных помех и их влияние на тактико-технические характеристики РЭС. Большое внимание уделено рассмотрению методов обеспечения внутрисистемных ЭМС за счет эффективного экранирования, фильтрации, правильного выполнения заземления.

Подробно рассмотрены характеристики и параметры ЭМС радиотехнических устройств: радиопередающих и радиоприемных устройств, антенных систем. Дан пространственно-энергетический анализ мешающего взаимодействия РЭС: каналы мешающего взаимодействия, энергетические соотношения. Изложены основы статистической теории ЭМС РЭС, способы оптимизация РЭС по критериям ЭМС, описаны межсистемные методы улучшения ЭМС.

Много внимания уделено рассмотрению стандартов измерения параметров ЭМС. Изложены проблемы обеспечения электромагнитной экологии.

Разработан банк вопросов по оценке качества знаний студентов и магистрантов по данной дисциплине.

Список литературы

1. Титович Н.А., Мурашкина З.Н. Электронный образовательный ресурс «Оптимизация радиосистем по критериям электромагнитной совместимости» для специальности 1-39 80 01 «Радиосистемы и радиотехнологии» / Свидетельство № 017 от 30.11.2021.

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ОБОЗНАЧЕНИЯ СТАТУСА ДОКУМЕНТА ВНУТРИ ОРГАНИЗАЦИИ

И.А. Трегубов

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

1. Обзор существующих проблем с обозначением статуса документа внутри организации:

– низкая эффективность процессов управления документами, связанная с неясностью статуса документа;

– распространенные ошибки, связанные с неправильной интерпретацией статуса документа, например, его просроченности;

– примеры организаций, столкнувшихся с проблемами управления документами: Volkswagen [1]

2. Разработка программных средств для обозначения статуса документа внутри организации:

– определение набора статусов документа, таких как «в работе», «на согласовании», «утвержден»;

– реализация механизмов обновления статуса документа в соответствии с его жизненным циклом;

– примеры программных средств для обозначения статуса документа: SharePoint [2]

3. Применение программных средств для обозначения статуса документа внутри организации:

– улучшение процессов управления документами, связанных с ясностью статуса документа;

– обеспечение соответствия документов требованиям безопасности и конфиденциальности;

– примеры организаций, использующих программные средства для обозначения статуса документа: KPMG [3];

4. Рекомендации по использованию программных средств для обозначения статуса документа внутри организации:

– обучение сотрудников использованию программных средств для обозначения статуса документа;

– регулярное обновление статусов документов для улучшения процессов управления документами;

– интеграция программных средств для обозначения статуса документа с другими системами управления бизнес-процессами.

Список литературы

1. Volkswagen fined for security failures in car theft case [Электронный ресурс]. – Режим доступа: https://www.computerweekly.com/news/252488163/Volkswagen-fined-for-security-failures-in-car-theft-case. – Дата доступа: 01.05.2023.

2. Manage documents and content types [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/en-us/sharepoint/manage-documents-and-content-types. – Дата доступа: 01.05.2023.

3. [Электронный ресурс]. – Режим доступа: https://www.kpmg.com. – Дата доступа: 01.05.2023.

МЕХАНИЗМ ФОРМИРОВАНИЯ ДИОКСИДА ВАНАДИЯ МЕТОДОМ АНОДНОГО ОКИСЛЕНИЯ ТОНКИХ ПЛЕНОК ВАНАДИЯ ДЛЯ УСТРОЙСТВ БОЛОМЕТРИЧЕСКОГО ТИПА

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 датчиков различного назначения исследуются материалы с новыми функциональными возможностями, среди которых особый интерес представляет обратимый фазовый переход металл-изолятор в диоксиде ванадия VO_2. Переход происходит при температуре ~340 K и может быть инициирован не только нагревом/охлаждением, но и генерацией носителей заряда при создании сильного электрического поля, а также путем инжекции или фотогенерации носителей заряда [1].

Благодаря наличию фазового перехода металл-диэлектрик, пленки VO_2 привлекают внимание, в частности, при изготовлении устройств детектирования ИК излучения посредством регистрации изменения температуры активного чувствительного элемента [2]. В качестве такого элемента используется микроболометр, измеряющий интенсивность падающего ИК излучения путем отслеживания изменения сопротивления чувствительного слоя при нагреве или охлаждении. Для высокопроизводительного микроболометра требуется, чтобы чувствительный материал имел высокий температурный коэффициент сопротивления ТКС и низкое удельное сопротивление для минимизации тепловых шумов и джоулева нагрева. Этим требованиям отвечают пленки VO_2, однако, они имеют ограничения в качестве детектирующего материала для микроболометров из-за ряда факторов. Актуальным является исследование процессов осаждения пленок оксида ванадия с требуемыми свойствами.

В данной работе исследуется процесс анодного окисления ванадия для формирования тонких пленок диоксида ванадия. На основании проведенных исследований предложен состав электролита и режим формирования анодных пленок оксида ванадия на подложках Al/Al_2O_3, Ti/TiO_2: водный раствор 2,0М уксусной кислоты, 0,02М $Na_2B_4O_7$, напряжение анодирования 4,6–5.0 В. Основной электрохимический процесс проходит следующим образом:

$Na_2B_40_7 \cdot 10H_20 \rightarrow 2Na^+ + B_40_7^{-2} + 10H_20$ (катализатор CH_3COOH),

$12H_20 + 2B_4O_7^{-2} + V \rightarrow VO_2 + 4e^- + H_3BO_3$.

В результате диссоциации тетраборат натрия мигрирует к аноду и является источником кислорода для формирования оксида ванадия. Входящая в состав электролита уксусная кислота выполняет функцию контроля pH и катализатора.

Представлены результаты исследования состава и микроморфологии поверхности полученных пленок диоксида ванадия.

Список литературы

1. Пергамент А.Л., Кулдин Н.А., Стефанович Г.Б. [и др.] Диэлектрические свойства диоксида ванадия и перспективы использования сэндвич структур на основе VO_2 в сенсорной технике // Современные проблемы науки и образования. 2014. № 5.

2. Liu K., Lee S., Yang S. [et al.] Recent progresses on physics and applications of vanadium dioxide // Materials Today. 2018. Vol. 21, iss. 8. P. 875–896.

АКТУАЛЬНЫЕ УГРОЗЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

И.И. Фролов

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

С развитием искусственного интеллекта (ИИ) и машинного обучения (МО) появились новые угрозы, связанные с этой технологией. В этом обзоре рассмотрим некоторые из основных угроз и проблем, связанных с развитием ИИ и МО [1].

Атаки на модели МО. Злоумышленники могут использовать различные методы для атаки на модели МО. Например, они могут изменять или подменять входные данные, чтобы система приняла неправильные решения. Это может быть особенно опасно, если МО используется в критических областях, таких как медицина или автономные транспортные системы.

Вредоносные атаки с использованием ИИ. С развитием ИИ возрастает вероятность использования его для разработки и распространения вредоносного программного обеспечения. Злоумышленники могут создавать интеллектуальные атаки, которые способны обманывать системы обнаружения и проникать в защищенные сети.

Уязвимости в алгоритмах и моделях МО. Недостаточно защищенные алгоритмы и модели МО могут стать уязвимыми для атак. Например, злоумышленники могут настроить модель МО таким образом, чтобы она давала неправильные результаты или была подвержена взлому.

Неправильное использование данных [2]. Сбор и использование больших объемов данных для обучения моделей МО могут повлечь за собой проблемы конфиденциальности и нарушение приватности. Если некорректные или недостоверные данные используются при обучении модели, это может привести к искаженным результатам и неправильным выводам.

Этические и социальные вопросы. Развитие ИИ и МО влияет на широкий спектр этических и социальных вопросов. Например, проблема автономных систем, способных принимать решения о жизни и смерти, вызывает серьезные вопросы о нравственности и ответственности.

Генерация фальшивых данных. ИИ и МО могут быть использованы для генерации фальшивых данных, включая фальшивые изображения, тексты или видео. Это может привести к распространению дезинформации, манипуляции или созданию поддельных доказательств.

Атаки на инфраструктуру ИИ. Распределенные системы ИИ требуют значительных вычислительных ресурсов и специализированных инфраструктурных компонентов. Атаки на такую инфраструктуру могут привести к нарушению работы систем и серьезным последствиям для организаций, зависящих от ИИ.

Быть в курсе последних тенденций в области безопасности, внедрять надежные меры безопасности, проводить регулярные оценки рисков и повышать осведомленность пользователей – все это необходимо для эффективного снижения угроз информационной безопасности при использовании искусственного интеллекта и машинного обучения.

Список литературы

1. Режимы сбоя в машинном обучении [Электронный ресурс] – Режим доступа: https://learn.microsoft.com/ru-ru/security/engineering/failure-modes-in-machine-learning. – Дата доступа: 01.05.2023.

2. Атаки на искусственный интеллект [Электронный ресурс] – Режим доступа: https://media.kaspersky.com/ru/business-security/attacks-on-artificial-intelligence-whitepaper.pdf. – Дата доступа: 01.05.2023.

БАЗА ЗНАНИЙ MITRE ATT&CK ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.Ф. Чаган

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

В целях всестороннего построения системы защиты информации в информационных системах и ресурсах необходимо принимать во внимание все возможные угрозы как извне, так и внутри самой системы. Для этого часто прибегают к построению модели нарушителя информационной безопасности.

MITRE ATT&CK [1] является базой знаний, в которой способы описания и категоризация поведения злоумышленника основываются на анализе реальных APT-атак (Advanced Persistent Threat) индивидуальных или организованных преступных групп и написаны правила для автоматизации расследований. Проще говоря, это база знаний о поведении противника, представляющая единый язык для описания одного и того же поведения, который могут использовать различные команды и организации. Данная модель строится с позиции атакующего.

В указанной базе знаний известные поведения злоумышленников разделены на тактики, техники, процедуры и выражаются в виде таблиц (матриц) для различных ситуаций и типов. Тактика показывает, как злоумышленник действует на разных этапах атаки, какая цель или задача у него на каждом этапе. Техника – как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, утилиты, технологии, коды, эксплоиты. Процедура отражает какая техника выполняется и для чего. Поскольку данный список дает комплексное представление о поведении злоумышленника при взломе сетей, он крайне полезен для организации различных защитных мероприятий, мониторинга, обучения и т.д.

Общедоступная база знаний MITRE ATT&CK содержит раздел, посвященный организованным преступным группам, что дает возможность описать поведение злоумышленников в унифицированной форме. Злоумышленники отслеживаются по действиям, характерным именно для них, путем сопоставления с техниками и тактиками в ATT&CK.

Группа – это кластеры действий, которые отслеживаются под общим именем в сообществе безопасности (группы угроз, группы активности и субъекты угроз). В настоящее время (на апрель 2023 г.) база ATT&CK содержит подробную информацию о 135 группах с указанием используемых ими техник и инструментов.

Использование данной базы позволяет отслеживать активности после компрометации, фокусироваться на поведении злоумышленника, а не на единичных флагах, сигнализирующих о нарушениях, а также перейти от реактивных к проактивным действиям.

Список литературы

1. MITRE ATT&CK® [Электронный ресурс]. – Режим доступа: https://attack.mitre.org. – Дата доступа: 04.04.2023.

РАЗРАБОТКА ОБУЧАЮЩЕЙ ПРОГРАММЫ ПО ИЗУЧЕНИЮ ВООРУЖЕНИЯ СУХОПУТНЫХ ВОЙСК

Д.С. Шарак, А.П. Бовсун

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

В настоящее время при разработке сложных систем особенно актуальны и широко применяются методы и средства компьютерного моделирования, которые по сравнению с методами натурного и полунатурного физического моделирования обладают явными преимуществами по ресурсным и временным затратам на проектирование.

Использование компьютерных имитационных программ позволяет самостоятельно приобретать новые знания с помощью компьютерных учебников, справочно-консультационных, демонстрационных и имитационно-моделирующих подпрограмм, объективно оценивать получаемые знания и приобретать практические навыки.

Разработанный курсовой проект представляет собой приложение, позволяющее организовывать визуальное ознакомление с вооружением, специальной и военной техникой Вооруженных Сил Республики Беларусь (ВС РБ), изучение его характеристик.

В качестве языка программирования был выбран PHP, используемый на стороне WEB-сервера для динамической генерации HTML-страниц. Это один из немногих языков программирования, созданных специально для разработки веб-приложений.

В веб-страницах расположена информация об различных видах, характеристиках и предназначении образцов вооружения, находящихся на вооружении Сухопутных войск.

Разработанный программный модуль может служить наглядным пособием и оказывать помощь при изучении дисциплин по специальностям: «Управление мотострелковыми подразделениями», «Управление танковыми подразделениями», «Эксплуатация наземных систем вооружения» учреждения образования «Военная академия Республики Беларусь». Кроме того, данный программный комплекс может найти применение при обучении курсантов военных учебных заведений по другим специальностям, связанным с эксплуатацией вооружения, военной и специальной техники, а также при обучении офицеров и военнослужащих срочной службы.

Список литературы

1. Строгалев В.П., Толкачева И.О. Имитационное моделирование. М.: МГТУ им. Баумана, 2008.

РАЗРАБОТКА ИНФОРМАЦИОННО-СПРАВОЧНОЙ СИСТЕМЫ НАЧАЛЬНИКА КАФЕДРЫ С ИСПОЛЬЗОВАНИЕМ СЕРВЕРНЫХ ТЕХНОЛОГИЙ

Д.С. Шарак, А.О. Гирко

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

Управление подразделениями любого типа, связано с переработкой большого потока информации и принятием на ее основе оперативных и перспективных решений. Поэтому автоматизация управленческих работ является основным направлением. Применение современных средств вычислительной техники создает новые возможности для дальнейшего совершенствования управления.

Для разработки информационно-справочной системы начальника кафедры в качестве веб-сервера был выбран Open Server, который хорошо и удобно настраивается, поскольку имеет модульную структуру. Модули позволяют администраторам сервера включать или выключать дополнительную функциональность. У Open Server есть модули безопасности, кэширования, редактирования URL, аутентификации с использованием пароля и другие.

Язык программирования был выбран PHP, используемый на стороне WEB-сервера для динамической генерации HTML-страниц. Это один из немногих языков программирования, созданных специально для разработки веб-приложений [1]. Разработанный программный комплекс позволяет рационально распределять время, необходимое начальнику кафедры, для принятия решений, а также задач для профессорско-преподавательского состава. Это позволяет осуществлять планирование мероприятий по основным задачам функционирования циклов кафедры с экономией времени.

Представляемая в виде web-приложения информация имеет относительно небольшой размер, учитывая большое количество манипулирующей информации. Присутствие функций экспорта и импорта данных в другие приложения позволит существенно сократить время на создание и оформление отчетных и планирующих документов.

Список литературы

1. Веллинг Л., Томсон Л. Разработка веб-приложений с помощью PHP и MySQL. И.Д. Вильямс, 2016. 848 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УНИВЕРСИТЕТА

Е.И. Шаронова, С.И. Матюшкин

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

Университетские информационные системы являются ключевой составляющей инфраструктуры университетов, которые поддерживают учебный процесс, административные функции и другие виды деятельности. Поэтому обеспечение доступности университетских информационных систем является критически важным, чтобы обеспечить непрерывность работы университета. Соответственно, важнейшей задачей становится обеспечение доступности информационных сервисов университета.

Распространенными практиками по обеспечения доступности являются: резервное копирование; обнаружение сбоев; балансировка нагрузки; резервирование и зеркальных серверов.

DDoS является угрозой для бесперебойной работы информационных сервисов, последствия от которой бывают как технические, финансовые, так и репутационные. Для генерации трафика злоумышленники используют различные источники: обычные компьютеры и серверы; умные устройства Интернета-вещей; сетевые устройства; рекламные сервисы.

Машинное обучение является набирающим популярность направлением, применяется оно и для обнаружения DDoS-атак. Существует множество продуктов, включая облачные решения, которые используют машинное обучение для обнаружения DDoS-атак путем анализа сетевого трафика и выявления аномалий. Например, Radware DefensePro, F5 Silverline DDoS Protection, Arbor Networks Peakflow, Imperva Incapsula, Neustar SiteProtect и т.п. Эти решения использует алгоритмы машинного обучения.

Нейронные сети используются для обработки больших объемов данных и обучения моделей, которые могут определять характерные признаки ботнетов. Примерами таких проектов являются Deep Defense, Botwall, Botnet Detection Based on Deep Learning, BotMine. Эти модели анализирует трафик и идентифицирует характеристики ботнетов, такие как IP-адреса и сигнатуры вредоносных программ, скорость сетевого трафика и длительность соединения.

Соответственно, перспективным является внедрение решений на основе машинного обучения для обеспечения защиты интегрированной информационной системы Белорусского государственного университета информатики и радиоэлектроники с учетом состояния современного рынка средств защиты от DDoS атак.

АКТУАЛЬНОСТЬ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СРЕДНИМ СПЕЦИАЛЬНЫМ ОБРАЗОВАНИЕМ

В.В. Шаталова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», Минск, Беларусь

В настоящее время в Республике Беларусь подготовка по специальности «Информационная безопасность» ведется только по уровню высшего образования. Специалистов со средним специальным образованием по специальности 5-04-0611-02 «Техническое обеспечение информационной безопасности», включенной в Общегосударственный классификатор Республики Беларусь ОКРБ 011-2022 «Специальности и квалификации», в настоящее время не готовит ни одно учреждение образования. Вместе с тем, современные требования рынка труда, уровня организации и обеспечения функционирования систем информационной безопасности таковы, что не только инженерные работники должны знать и уметь применять приобретенные компетенции по данной специальности, но и технические специалисты среднего звена на высоком уровне должны владеть знаниями, умениями и навыками в области информационной безопасности. Специалист по информационной безопасности – одна из ключевых профессий, востребованных на рынке труда, так как почти каждая организация сегодня сталкивается с проблемой информационных угроз и, как следствие, задачей обеспечения безопасности данных. Совершенствуются технологии защиты данных, но уязвимость защиты не только не уменьшается, а постоянно растет. Поэтому очевидна актуальность проблем, связанных с защитой потоков данных и информационной безопасностью их сбора, хранения, обработки и передачи. Реализация указанных задач требует высокого уровня как теоретической, так и практической подготовки специалистов как с высшим образованием, так и со средним специальным.

Цифровая трансформация экономики предполагает организацию цифровой информационной среды путем формирования нормативной правовой базы и внедрения действенных инструментов управления процессами цифровизации экономики [1]. Одним из стратегических направлений отечественного промышленного производства является ускоренное развитие высокотехнологичных производств, что потребует освоения современных систем управления производством, внедрения ресурсосберегающего оборудования и технологических процессов, освоения систем умного производства, включая роботизацию, а также внедрения информационно-коммуникационных технологий и передовых производственных технологий, базирующихся на принципах концепции «Индустрия 4.0», включая вопросы обеспечения информационной безопасности. Планируется, что к 2025 году доля

специалистов, ответственных за вопросы информатизации в государственных органах и организациях, прошедших обучение в сфере цифрового развития, составит не менее 40 процентов.

Подпрограмма «Информационная безопасность и «цифровое доверие» предусматривает выполнение мероприятий не только по созданию современной ИК-инфраструктуры, внедрению цифровых инноваций в отраслях экономики и технологий «умных городов», но и обеспечению информационной безопасности этих решений, повышение уровня информационной безопасности данных и технологий ее обеспечения в рамках созданной цифровой информационной экосистемы [2]. Конкурентоспособность отечественных разработок и технологий информационной безопасности является важнейшим условием успешного цифрового развития государства. Концепция информационной безопасности Республики Беларусь подчеркивает необходимость обеспечения национальной безопасности страны, в том числе защищенности информационного пространства, информационной инфраструктуры, информационных систем и ресурсов, что позволит исключить риски, вызовы и угрозы, порождаемые трансформацией социума в информационное общество [3]. Новые подходы к защите персональных данных, продиктованные Законом Республики Беларусь «О защите персональных данных» также требуют реализации подготовки специалистов в области информационной безопасности [4].

С учетом выше сказанного актуальность открытия подготовки по специальности среднего специального образования 5-04-0611-02 «Техническое обеспечение информационной безопасности» обусловлена необходимостью подготовки высококвалифицированных и востребованных кадров для цифровой экономики, специалистов по внедрению информационных технологий и обеспечению информационной безопасности.

Список литературы

1. Об утверждении Программы социально-экономического развития Республики Беларусь на 2021–2025 годы: Указ Президента Республики Беларусь, 29.07.2021, № 292 // Национальный правовой Республики Беларусь [Электронный ресурс]. 2022. – Режим доступа: https://pravo.by/.

2. О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы: постановление Совета Министров Республики Беларусь, 02.02.2021, № 66 // Национальный правовой Республики Беларусь [Электронный ресурс]. – 2023. – Режим доступа : https://pravo.by/.

3. О Концепции информационной безопасности Республики Беларусь: постановление Совета Безопасности Республики Беларусь, 18.03.2019, № 1 // Национальный правовой Республики Беларусь [Электронный ресурс]. – 2023. – Режим доступа : https://pravo.by/.

4. Закон Республики Беларусь «О защите персональных данных», 07.05.2021, № 99-З // Национальный правовой Республики Беларусь [Электронный ресурс]. – 2023. – Режим доступа : https://pravo.by/.

АКТИВНЫЕ ЭЛЕМЕНТЫ МЭМС НА ОСНОВЕ ДВУХСЛОЙНЫХ МЕМБРАННЫХ СТРУКТУР

М.А. Шахвердиев, О.М. Чернаусик, С.А. Биран, А.В. Короткевич

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

Двухслойные мембранные структуры находят широкое применение в качестве активных элементов в исполнительных и сенсорных устройствах, применяемых в современных средствах защиты информации. Использование таких структур позволяет расширить динамический диапазон чувствительности изготавливаемых на их основе сенсорных устройств. Путем изменения толщины слоев можно получить необходимую чувствительность активного элемента [1]. На основе двухслойных структур можно изготавливать термоактюаторы для МЭМС устройств. В качестве материала для их изготовления перспективно использовать двухслойные консольные балки на основе анодированного алюминия. Разработана конструкция термоактюатора на основе двухслойных мембранных структур из анодного оксида алюминия.

Термоактюатор состоит из индикаторной площадки, консольных балок, удерживающих индикаторную площадку, и основания. Индикаторная площадка, имеющая высокую отражающую поверхность, может использоваться в качестве микрозеркала. Консольные балки выполнены из двухслойных структур на основе алюминия и его анодного оксида. Количество балок определяется требуемой чувствительностью устройства. Управление термоактюатором осуществляется путем нагрева резистивного материала, нанесенного на поверхность балок. При подаче тока резистивная плёнка нагревается, при этом за счёт различия температурных коэффициентов линейного расширения алюминия и оксида алюминия происходит изгиб балок и, соответственно, перемещение индикаторной площадки.

Термоактюаторы на основе двухслойных мембранных структур обеспечивают относительно большое линейное перемещение и могут создавать значительное усилие. Нагрев микробалок обеспечивает как вертикальное перемещение индикаторной площадки, так и ее поворот в различные стороны. Таким образом, использование для изготовления термоактюаторов двухслойных мембранных структур на основе анодированного алюминия обеспечивает получение недорогого функционального термоактюатора для МЭМС устройств.

Список литературы

1. Romanowicz B., Lerch Ph., Slimane C.K. Modelization and characterization of asymmetrical thermal microactuators // Journal of Micromech. Microeng. 1996. P. 134–137.

ПРИМЕНЕНИЕ МОДУЛЯ НЕЧЕТКОГО УПРАВЛЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ТИПОВ ВОЗДУШНЫХ ОБЪЕКТОВ В ЗАДАЧАХ УПРАВЛЕНИЯ ОГНЕМ ГРУППИРОВКИ ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ

И.Ф. Шелест, А.В. Хижняк

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

Задача о назначениях имеет множество интерпретаций и одна из них – это распределение воздушных целей между огневыми средствами.

Основной задачей целераспределения (ЦР), от которой зависит эффективность противовоздушного боя, является закрепление целей за огневыми средствами в соответствии с их тактическим предназначением. Автоматическое ЦР требуется при общем количестве целей, входящих в обобщенную зону поражения, сравнимых или

превышающих максимальное количество огневых каналов группировки средств ПВО. В условиях острого дефицита времени, решение задачи классификации типов воздушных объектов может быть достигнуто за счет введения в состав алгоритма ЦР дополнительного модуля автоматической классификации воздушных целей (ВЦ), подлежащих целераспределению. Это позволит выявлять наиболее опасные цели, учитывать тактическое предназначение огневых средств и, как следствие, оптимизировать решение задачи целераспределения.

В условиях ограниченности и низкой достоверности получаемой информации в отечественной и зарубежной литературе для решения задачи классификации декларируется преимущество математического аппарата теории нечетких множеств и, в частности, нечеткого вывода [1]. Суть процедуры нечеткого вывода состоит в выработке управляющего сигнала $\bar{y}$, соответствующего типу летательного аппарата, на основе измеряемых значений $\bar{x}$ (элементов вектора состояния ВЦ) [2].

Степени опасности цели определяется в соответствии с выражением: $\Theta_H = \frac{\Theta_i}{\Theta_{i\max}}$,

где Θ_i – степень опасности *i*-й цели.

Таким образом, применение математического аппарата теории нечетких множеств в целом и нечеткого вывода в частности позволяет решать задачу классификации воздушных целей на пунктах управления. Полученные результаты классификации в последующем могут быть использованы для первоочередного целераспределения наиболее опасных целей, а также для учета тактического предназначения огневых средств при закреплении за ним целей.

Список литературы

1. Поспелов, Д.А. Нечеткие множества в моделях управления и искусственного интеллекта. М.: Наука, 1986.

2. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая линия – Телеком, 2006. 452 с.

БЕЗОПАСНОСТЬ ЭКОСИСТЕМЫ УМНОГО ДОМА

Е.А. Шитик, П.И. Цыркунович

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

С развитием технологий Интернета вещей (IoT, Internet of Things) интеллектуальные устройства умного дома стали все более распространенными и доступными для использования. В свою очередь, это приводит к возрастанию интереса со стороны киберпреступников, которые ищут способы атаковать такие устройства. В результате этого, защита устройств умного дома стала важной задачей для разработчиков и производителей. Кроме этого, во всем мире растерт обеспокоенность безопасностью личных данных пользователей и обеспечением их защиты. В этом плане экосистема умного дома, которая зачастую строится на основе интеграции смарт-устройств различных производителей, конфигурируется и эксплуатируется пользователями без достаточной квалификации в области безопасности, является весьма уязвимой.

Для того, чтобы обеспечить должный уровень защиты, надо знать потенциальные слабые места и уязвимости проекта. Мы рассматриваем слабые звенья экосистемы умного дома в реализации информационных потоков проекта. Пусть общая схема системы умного дома такова: (Пользователь) – (Управляющая система) –

(Устройство автоматизации). Первый поток находится между пользователем и управляющей системой – в нем передаются команды пользователя программной платформе, на которой реализован умный дом. Второй - между управляющей системой и конечными устройствами автоматизации. К слабому звену можно так же отнести: открытость для внешнего доступа («торчание в интернет», передачу данных во внешние облачные хранилища), беспроводное общение между устройствами.

Чтобы обезопасить экосистему умного дома, необходимо в первую очередь повысить защищенность всех описанных выше слабых звеньев. К числу таких методов можно отнести: выбор безопасного протокола передачи данных – Zig-Bee, Z-Wave; реагирование на физическое вмешательство, которое может создать аномальное состояние; аутентификацию на стороне конечного устройства.

К особенностям нашего подхода к защите умного дома нужно отнести и использование специализированных устройств, называемых «защищенные шлюзы». Они обеспечивают контроль доступа, маршрутизацию трафика, аутентификацию пользователей, мониторинг и обнаружение взломов. Также защищенные шлюзы могут иметь функцию бэкапа и восстановления системы.

В заключение можно сказать, что защита устройств умного дома от киберугроз является важной задачей, которой необходимо уделить должное внимание. Пользователи должны соблюдать базовые меры по обеспечению безопасности, а производители должны уделять внимание безопасности на всех этапах разработки и выпуска смарт-устройств. По-нашему мнению, в сфере IoT, безопасность – основной сдерживающий фактор [1].

Список литературы

1. Kanev A.N., Nasteka A.V., Bessonova C.E. Automation Device Authentication at «Smart Home» // Vestnik policii. 2016. Vol. 7, iss. 1.

ПЕРЕДАЧА ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИЗМЕНЕНИЯ АПРОША С ИСПОЛЬЗОВАНИЕМ ОСОБЕННОСТЕЙ ФОРМАТА XML

Н.П. Шутько

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

Стеганография − это метод передачи информации с помощью скрытого текста, изображений или звука. Ранее автором был рассмотрен алгоритм встраивания секретной информации засчет модификации такого исходного пространственного параметра как апрош, т. е. изменения расстояния между соседними буквами или другими шрифтовыми знаками [1]. Апрош – это альтернативный способ записи слов, который может использоваться для создания скрытых сообщений в тексте. При таком методе стеганографии скрытые сообщения могут быть переданы тайно и незаметно для посторонних.

Как известно, формат *.docx представляет собой архив, содержащий файлы в формате *.xml. Дальнейший интерес представляет более детальное изучение тегов, которые формируют содержание данных файлов. В частности, содержимое файла document.xml, который описывает контент рассматриваемого документа, а также стили, которые к нему применяются.

При модификации апроша символа документа, созданного с помощью текстового процессора MS Word, соответствующее значение будет записано в указанный выше документ в теге <w:spacing/>. Так, например, разреженный интервал

со значением в 1 пт будет записан как <w:spacing w:val="-20"/>. Определение отклонений от исходного значения будет служить для осаждения или извлечения тайного сообщения.

Список литературы

1. Шутько Н.П., Урбанович П.П. Особенности использовании параметров апроша в методах текстовой стеганографии // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 103.

АЛГОРИТМ ГЕНЕРАЦИИ ШТРИХОВЫХ ЗАЩИТНЫХ ИЗОБРАЖЕНИЙ ПО ЗАДАННОМУ КЛЮЧУ

А.Н. Щербакова, Д.М. Романенко

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

При формировании изображений с защитой следует исходить из вида изображения и возможности его декодирования. Следует учитывать, что векторные изображения при их воспроизведении имеют определенные ограничения по типу линий, их цветности, передаваемой частоте. Однако с точки зрения кодирования в цифровом виде наложенные ограничения снимаются, что позволяет представить достаточно большое количество вариантов кодирования различных знаков.

Кодирование авторской информации в векторных изображениях может осуществляться в виде набора линий или простых геометрических фигур с разными параметрами (тип линии, толщина линии, цвет линии, расстояние между линиями).

Защита любых документов строится на внедрении защитного ключа. Каждому набору линий ставится в соответствие определенный символ. Также особенностью векторных изображений с внедренной защитой является их цветность.

Для генерации штрихового изображения по ключу первым шагом необходимо задать размеры изображения по горизонтали и вертикали и выбрать фоновый цвет. Далее ввести ключ. Каждый символ включает в себя свой набор параметров для кодирования. К этим параметрам относятся: количество линий, цвет линии, толщина линии, тип линии, схема штрихования линии. Тип линии может быть либо сплошной, либо штриховой. При выборе штрихового типа есть возможность настроить схему штрихования, задавая длину штриха и пробела. Если будет задано нечетное количество значений, то список значений будет повторяться. После необходимо ввести открытый текст, который и будет закодирован этим ключом.

Формат ключа:

[символ] [количество линий] [цвет линии] [толщина линии] [тип линии] [схема штрихования (необязательный параметр)]

Например, необходимо закодировать текст следующего содержания: «АБВ», ключ кодирования может выглядеть следующим образом:

А 2 #ff69b4 7 1 5,5

Б 1 #ff8c00 2 0

В 4 #00ff7f 7 1 2,3

Первый параметр – сам символ, далее количество линий, цвет в формате HEX, толщина линии, следующий параметр 1 или 0: 1 указывает на штриховую линию, 0 – на сплошную. При выборе штриховой линии вводятся параметры схемы штрихования.

В результате можно получить уникальное защитное изображение, которое будет содержать в себе авторский текст.

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XXI Белорусско-российской научно–технической конференции
(Минск, 6 июня 2023 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 24.05.2023. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 12,32. Уч.-изд. л. 8,6. Тираж 100 экз. Заказ 97.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/238 от 24.03.2014, № 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
ЛП № 02330/264 от 14.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск