Министерство образования Республики Беларусь
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
XIX Белорусско-российской научно-технической конференции
(Минск, 8 июня 2021 г.)

Минск БГУИР 2021

УДК 004.056.5
ББК 32.972.5
Т38

Технические средства защиты информации : тез. докл. XIX Белорусско-
Т38 российской науч.-техн. конф. (Республика Беларусь, Минск, 8 июня 2021 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2021. – 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

USING THE BASIC SPEECH SIGNALS TO CREATE SPEECH-LIKE NOISE

H. Amiry

Protection of speech information from leakage through technical channels is one of the main tasks when providing a set of measures for information security of a dedicated room [1, 2]. To solve it, both passive and active methods of protecting information are used. In the case of active methods of protecting speech information, vibration and acoustic masking noises are used, created by noise generators and various types of vibration emitters. Speech noise generated from speech signals is also an effective technique.

The paper considers an algorithm for the formation of speech-like noise using the synthesis of sound signals by random sampling of speech elements from the generated database. In this case, the task of separating the noise from the useful signal becomes more difficult compared to ordinary noise. Therefore, the use of speech-like noise makes it possible to increase the overall stability of the speech information protection system in a dedicated room. Studies have shown that the most effective interference type “speech chorus”.

The formation of speech-like noise took place in several stages. At the first stage, a speech array was created, including a set of Russian words and containing selected allophones. The input data for the synthesis and subsequent allophonic marking of the speech signal was an audio text array and a formed phonetic-acoustic database. After synthesis, the speech signal is used for segmentation and allophone marking of the natural speech signal. One of the stages was listening to the speech signal with the possible manual adjustment of the boundaries of the allophones. After compiling a database of allophones, software was used, which accepts an array of created files as input. Then the synthesis and reproduction of the input text took place using the recorded allophones. The “speech chorus” noise was formed similarly to the speech-like noise with the overlapping of the voices of several speakers at the same time.

References

1. Blintsov V., Nuzhniy S., Kasianov Y., Korytskyi V. Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels // Technology audit and production reserves. 2019. Vol. 5, no. 2 (49). P. 19–26.

2. Davydau H.V., Papou V.A., Potapovich A.V., Seitkulov Y.N., Li Ye, Fan Yanhong, Jiang Jingsai, Bi Xiaoyan. Method for protecting speech information // Doklady BGUIR. 2015. Vol. 8 (94). P. 107–110.

COMBINED ERASURE-AND-ERROR DECODING ALGORITHM FOR RS-CODES AND ITS APPLICATION FOR M-FSK MODULATION

B. Assanovich

For a long time, powerful algebraic BCH codes and its generalizations – Reed-Solomon codes – were used to suppress noise during data transmission. However, in 90-s random coding and decoding with the use of such code constructions as LDPC and turbo codes attracted particular attention of communication systems developers.

The use of iterative methods of information processing in these codes made it possible to approach the Shannon boundary when using soft decoding. However, in cases of data transmission (and not only), the time delay in the information processing is critical. Therefore, many engineering applications still use algebraic decoding techniques.

Error-correcting codes are used not only in communication systems, but also

in information security applications, where it is important to ensure access security with noisy input data. The structure of such systems was considered by us in [1]. It should be noted that in recent years, non-binary code constructions [2, 3] have attracted particular interest, which is explained by their flexibility of their structures and their high efficiency at a low signal-to-noise ratio.

In this paper, we consider the application of a modified combined erasure-and-error decoding method for RS codes using an iterative selection of the erasure vector based on an estimate of the noise level in the received signal. Unlike algebraic soft decoding of RS codes, our approach is closer to the stochastic method, described in [4].

The main difference of our work is that to find a suitable vector for decoding, we use an iterative search for the erasure vector by sorting the symbols of the code block in descending order of their reliability and waiting for a successful hard decoding based on the Berlekamp-Messi algorithm. It is important to note that the search for a suitable erasure vector is implemented using a symbol-by-symbol shift of the decoded codeword, which allows the entire decoder to be implemented in hardware. Simulation modeling of the proposed algorithm for data transmission with M-FSK modulation and (63, 13) RS-coding has been applied. The 2048-point DFT was used to get the reliability of the received symbols when searching for the erasure vector, giving the opportunity to obtain a coding gain of about 1 dB for BER = 1E-5 of data received.

The proposed algorithm is less efficient than Guruswami-Sudan and Kotter-Vardy soft decoding algorithms, however, it has a much simpler implementation and can be applied both in telecommunication and security systems

Literature

1. Assanovich B.A., Veretilo Yu.N. Biometric Database Based on HOG Structures and BCH Codes. Materials of the conference “ITS 2017”. Minsk, 2017. P. 286–287. (In Russ.)

2. Assanovich B.A., Veretilo Yu.N., Rudalesku V. Transition to Non-Binary Noise-Immune Codes in Biometric Systems. Abstracts of the XVI Belarusian-Russian Scientific and Technical Conference “Technical Means of Information Security”. Minsk, 2018. P. 15–16. (In Russ.)

3. Application of Turbo Codes for Data Transmission in UWB Using PSK Modulated Complex Wavelets. Signal Processing Workshop. Warsaw, 2020. P. 40–43.

4. Chang-Ming Lee and Y. Su. Stochastic Erasure-Only List Decoding Algorithms for Reed-Solomon Codes. IEEE Signal Processing Letters, 16. 2009. P. 691–694.

NFC TECHNOLOGY FOR ACCESS CONTROL SYSTEMS

I. Baryskievic, A. Tharwat

Widespread use of mobile phone payments makes Near-field communication (NFC) technology a promising research area [1]. NFC provides both security and unambiguous identification of the paying user as well as reliable, fast resistance to various types of attacks identification algorithm that allow to use it in the access control systems.

As a result of a comprehensive analysis of NFC technology, the physical component, the NFC technology protocol, as well as the basic algorithms and methods of user identification based on NFC technology were investigated. The simulation results of an access control system based on NFC technology showed that for BPSK modulation, the probability of successful packet transmission is 100 %, while this is about 95% for QPSK modulation. In the presence of traffic jam and SIC, BPSK still gives a 100 % probability of successful

packet transmission, while this figure drops to about 80 % for QPSK. In other locations, PSR is approximately 90 % for BPSK and 60–70 % for QPSK.

The probability of successful packet transmission, for different rooms with different noise levels, practically does not depend on the level of the mixing factor. The probability of successful packet transmission for different visits with different noise levels decreases with an increase in the mixing factor.

Based on the simulation results, it can be concluded that NFC technology for user identification has a number of key advantages, such as: speed of operation, protection against various types of attacks, and also low cost.

References

1. Coskun V., Ok K, Ozdenizci B. Near Field Communication (NFC): From Theory to Practice. John Wiley & Sons, 2011. 632 p.

ANALYSIS OF THE ACOUSTIC CHANNEL OF VOICE INFORMATION LEAKAGE IN A PROTECTED ROOM

A.N.S. Hasani

Protection of speech information in a dedicated room begins with the assessment of acoustic and vibration channels of speech information leakage [1, 2]. The research methodology based on creating acoustic signals in a dedicated room and then measuring the level of acoustic signals outside the room is rather complicated and time-consuming. Therefore, to assess the channels of speech information leakage, it is possible to use the results of the analysis of the acoustic channel of information leakage based on the physical model of the propagation of speech signals in the form of acoustic waves outside the allocated room.

In this work, for the mathematical description of the propagation of speech signals behind structural elements of premises, such as walls, over, ceiling, a rectangular plate was used for the corresponding selected element. The solution of the partial differential equation in the form of a numerical series for transverse vibrations of the enclosing plate is obtained. The equation used the approximation for a plate loosely fixed at the edges (for example, a hinged plate), for which there are no displacement and bending moments at the edges. The frequencies from the first to the tenth for the modes of natural vibrations of the wall made of gypsum blocks 0.09 m thick, 6 m long and 3.2 m high have been determined. The calculation results show that the frequencies of natural vibrations from the first to tenth in terms of wall height, length and their combinations are in the range from 70 to 5000Hz. It is shown that the spectrum of speech signals can be overlapped by a set of a number of natural resonant frequencies for the enclosing elements of the room. As a result, an acoustic wave with speech information is generated, which is excited by the back side of the enclosing structure.

Thus, acoustic vibrations are unevenly distributed throughout the building structure. There are certain areas with maximum values of natural vibrations. Such areas with maximum natural vibrations of structures must be localized by placing vibration sensors that generate an interference signal.

References

1. Horev A.A. Technical protection of information. Vol. 1. Techical channels of information leakage. M.: NPC Analitika, 2008. 436 p. (In Russian).

2. Davydau H.V., Papou V.A., Potapovich A.V., Seitkulov Y.N., Li Ye, Fan Yanhong, Jiang Jingsai, Bi Xiaoyan. Method for protecting speech information // Doklady BGUIR. 2015. Vol. 8 (94). P. 107–110.

DYNAMIC HOST CONFIGURATION PROTOCOL VULNERABILITIES

A.L. Smeer, A.S. Sunil Lal, E.S. Belousova

Dynamic Host Configuration Protocol (DHCP) is a network protocol which is used on UDP/IP networks. A DHCP Server dynamically assigns an IP-address and other network configuration parameters to each device in a network, so that they can communicate with other networks.

A pair of vulnerabilities in the DHCP client in Windows 10 and Windows Server 2019 allows attackers to execute code remotely, according to researchers at security firm Positive Technologies [1]. An attacker configures a DHCP server on their computer. Then the attacker waits for a vulnerable Windows 10 computer to ask for a renewal of IP address lease, which usually happens every few hours. By sending this invalid response, the attacker can obtain the rights of an anonymous user on the victim computer. It provides a useful entry point for continued escalation by pairing with other vulnerabilities. Nominally, attackers must be on the same network as the targeted system, though for organizations where DHCP Relay is used to use external DHCP servers, this limitation can be bypassed.

The aim of the work is to research DHCP vulnerability in Cisco Packet Tracer.

Based on simulation we can highlight the following features of DHCP vulnerability exploiting. Attacker introduces a new system (the laptop) in the network and then requests an IP-address, as the DHCP protocol will assign an IP-address automatically. Then attacker can see that an IP-address has been assigned to his device and he can change the MAC-address of this device, because the DHCP-server detects it as another device, i. e. a new device. So, it gets assigned a new IP address. In other words, attacker does MAC-spoofing attack. So, the DHCP pool of the server will be exhausted, the server will not respond to clients messages and it will simply drop clients replies. In this case, the attacker configures his device as DHCP-server. It receives the clients message and responds to it by giving IP-addresses, the IP-address of the DNS server and the default router. Replacing the default gateway attacker will cause all traffic to pass through his device, which will allow the attacker to get personal data of users. Spoofing a DNS server (DNS-spoofing) will result in users being given a nonreal IP-address of real web resources, which can be used for extortion.

In the continuation of our work, recommendations for protecting corporate networks from the vulnerability of the DHCP protocol will be compiled and tested.

Literature

1. Sanders, J. Windows 10 DHCP vulnerability allows for remote code execution [Electronic resource]. – 2021. – Access mode: https://www.techrepublic.com/article/windows-10-dhcp-vulnerability-allows-for-remote-code-execution/ – Date of access: 30.03.2021.

FAULT TOLERANCE AND SECURITY FOR COMMUNICATION NETWORKS

H.H. Sudani, M.B. Abrosimov

In general, it is assumed that a parallel program will execute on reliable hardware. A fault tolerant program and underlying infrastructure should be capable of surviving failures such as system crashes and network failures. At the highest level the application should be capable of automatically recovering from a set of faults without any change to the apparent behavior of the program. The process of check pointing may be used to allow a program to save its state to persistent storage. One should always anticipate that errors in communications will occur.

Routing in mobile networks generally involves multiple hops, whereas in distributed networks, it's a challenging task [1]. Distributed computing systems can provide several advantages, such as scalability, fault tolerance, and load balancing. Dealing with distributed systems and data storage together, introduces several challenges and difficulties [2], such as dynamic load balancing, unstable connections, communication failures, lack of flexibility in storing data, lack of auto-reconfigurations, limited radio range. A network's reliability has always been a major concern. Among different other factors such as software extensibility, maintainability, and usability, etc., Reliability have greater impact on software's life, because it can make the running application out of order [1, 2]. Reliability is a very broad term and any software application running in distributed environment can have various definitions. Reliability is associated with unexpected failures of products or services and understanding why these failures occur is key to improving reliability. A principle requirement for the creation of a fault-tolerant system is the ability to detect errors. Fault tolerance in relation to adhoc wirelessly interconnected mobile devices is a far more complex task than fault tolerance for high end clusters and parallel machines with fixed cabled infrastructure.

Literature

1. Bhuvana Suganthi D., Manjunath R., Anuradha V Rao. High Performance Mobile Computing Nodes in Distributed Networks // International Journal of Engineering Trends and Technology. 2014. Vol. 4, iss. 3.

2. Bobed C., Ilarri S., Mena E. Distributed Mobile Computing Development of Distributed Applications Using Mobile Agents. PDPTA. 2010.

ТЕСТИРОВАНИЕ ИСПОЛНЯЕМЫХ ФАЙЛОВ НА УЯЗВИМОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДА SYMBOLIC EXECUTION

А.М. Аблецов

Выявление уязвимостей какой-либо инфраструктуры является одним из ключевых способов для противодействия вредоносной активности, в том числе вредоносному программному обеспечению. Основными методами защиты от эксплуатации уязвимостей исполняемых файлов связанными с менеджментом памяти являются механизмы: предотвращение выполнения данных (DEP), рандомизация размещения адресного пространства (ASLR), позиционно-независимый код (PIC), механизм cannary, ограничение на изменение глобальной таблицы смещения (GOT), замена уязвимых функций на их безопасные аналоги. Так как исполняемые файлы являются одни из основных элементов любой инфраструктуры, то тестирование их на уязвимости ключевая задача для поддержания общего уровня безопасности защищаемой системы.

В настоящее время существует два подхода к тестированию исполняемых файлов на уязвимости: динамический и статический анализ. При динамическом анализе, исполняемый файл тестируется на уязвимости посредством подачи потенциально зловредных входных данных и детектировании аномального поведения программы. Статический анализ предполагает анализ заголовков файлов, инструкций ассемблера, строк данных без непосредственного исполнения тестируемого файла в системе. Одним из ответвлений статического анализа является метод Symbolic Execution. Суть метода Symbolic Execution заключается в том, что все условные переходы и вызовы функции тестируемой программы представляются в виде уравнений, относительно входных данных. И, следовательно, входные данные, приводящие к тому либо иному исходу исполнения программы, будут являться решением системы уравнений, что особенно актуально в программах, реализующих алгоритм выявления уязвимостей.

О КРИПТОАНАЛИЗЕ ШИФРОВ ПРОСТОЙ ЗАМЕНЫ С ИСПОЛЬЗОВАНИЕМ СЛОВАРЯ

М.Б. Абросимов, А.Д. Коннова, Д.А. Томилов

В работе рассматривается криптоанализ моноалфавитного шифра замены, то есть шифра, в котором каждой букве открытого текста сопоставляется единственная буква шифр-текста. Хорошо известным методом криптоанализа шифра простой замены является алгоритм [1] на основе частотного анализа, который состоит в итерационном процессе минимизации разницы частот. В зашифрованном сообщении вычисляются частоты символов и сравниваются с эталонными значениями. В таком случае можно сопоставить частоты символов шифроалфавита с исходными и восстановить исходный текст. Однако на практике одних лишь частот символов оказывается недостаточно. Текст может быть слишком короткий, чтобы в нем оказались эталонные или близкие к ним частоты. Как отмечает автор, для достаточно больших текстов количество ошибок может быть незначительным, и текст может быть прочитан, хотя и с некоторыми ошибками.

Предлагается добавить в алгоритм на основе частотного анализа дополнительный слой на основе словаря. Получив достаточное приближение к эталонным частотам, переходим к следующему этапу – проверке частично дешифрованных слов по словарю. При выборе определенного слова из словаря пробуем совершить замену ошибочной буквы и подсчитать коэффициент похожести слов. Коэффициент похожести слов – сумма минимальных ошибок в словах расшифрованной с помощью предположительной перестановки криптограммы со словами из словаря. Алгоритм заканчивает работу, когда не остается слов с ошибкой для исправления.

Была разработана программа, реализующая предлагаемый алгоритм. На вход подавались зашифрованные шифром простой замены тексты и анализировалось качество автоматической дешифровки. Если в работе [1] у автора были ошибки на тексте длиной 1000 символов, то описываемый метод полностью справился со всеми текстами длины более 800 символов.

Литература

1. Jakobsen T.P. A Fast Method for Cryptanalysis of Substitution Ciphers // Cryptologia. 1995. Vol. 19. P. 265–274.

РАСПРЕДЕЛЕНИЕ УРОВНЕЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СЕРВИСАХ

Р.Д. Авсеенко, Д.С. Кукла

Облачные вычисления изменили способ доставки и использования ИТ-решений конечными пользователями, так как они предоставляют такие услуги как хранилище данных, базы данных, облачные вычисления и многое другое. Большинство современных компаний используют облачные сервисы в своей деятельности ввиду их масштабируемости и удобства эксплуатации. Популяризация облачных технологий и сервисов поставила вопрос об обеспечении безопасности пользовательской информации. Поэтому улучшение безопасности является наиболее приоритетным направлением при построении различных информационных систем и сетей.

В рамках данного исследования было проанализирована возможность построения безопасной архитектуры на основе облачного сервиса Amazon Web Service (AWS). Фундаментальной практикой обеспечения безопасности AWS является

«defense-in-depth», которая реализуется с помощью набора сервисов, основываясь на базовых принципах:

1) контроль доступа – определение, соблюдение и аудит полномочий пользователей (сервис AWS Identity and Access Management и др.);

2) обнаружение угроз – выявление угроз и их устранение до появления последствий (сервис Amazon Guard Duty и др.);

3) защита инфраструктуры – обеспечение сетевой безопасности, фильтрация трафика (сервисы AWS Network Firewall, AWS Shield и др.);

4) защита данных – обеспечение конфиденциальности и целостности информации (сервис AWS Key Management System);

5) реагирование на угрозы безопасности – анализ потенциальных проблем (сервис Amazon Detective и др.).

Необходимо отметить, что облачный сервис Amazon AWS предоставляет множество функций, обеспечивающих управление доступом, контроль трафика, анализ уязвимостей. Так, например, Сервис AWS Identity and Access Management (IAM) предоставляет возможности безопасного управления доступом к сервисам и ресурсам AWS. Используя IAM, можно создавать пользователей и группы, управлять ими, а также использовать разрешения, чтобы предоставлять или запрещать доступ к различным ресурсам. В свою очередь AWS Network Firewall – это управляемая сервис, который упрощает развертывание основных средств защиты сети. Сервис AWS Key Management Service (KMS) обеспечивает централизованный управление криптографическими ключами, используемыми для защиты данных. Этот сервис использует для защиты ключей аппаратные модули безопасности (HSM).

Благодаря множеству предоставляемых сервисов AWS позволяет автоматизировать задачи обеспечения безопасности, решаемые вручную. Данные сервисы тесно интегрированы друг с другом и создают архитектуру построения безопасной, высокопроизводительной, гибкой и эффективной инфраструктуры приложений [1–3].

Литература

1. AWS Security Fundamentals [Электронный ресурс]. – Режим доступа: https://www.aws.training/Details/eLearning?id=34259 – Дата доступа: 02.05.2021.

2. AWS Cloud Security [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/products/security/?nc=sn&loc=2 – Дата доступа: 02.05.2021.

3. Информационная безопасность в AWS [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=7RRkSTSWOMo&t=1602s – Дата доступа: 02.05.2021.

ПРИНЦИПЫ ПОСТРОЕНИЯ БЕЗОПАСНОЙ ИНФРАСТРУКТУРЫ БЕСПРОВОДНЫХ СЕТЕЙ НА БАЗЕ КОНТРОЛЛЕРОВ CISCO WLC

Д.И. Алейникова

В современном мире беспроводные сети являются неотъемлемой частью человеческой жизни. Это обусловлено удобством их использования, связанным с отсутствием кабелей, а также возможностью подключения к сети не только со стационарного компьютера, но и телефона, планшета и т. д. Следует отметить, что использование беспроводной среды передачи данных приводит к возникновению вопроса о защищенности передаваемой информации. Для того, чтобы перехватить данные, достаточно использовать обычный приемник, находящийся в области распространения сети. Таким образом, при организации защиты информации

в беспроводных сетях следует уделять больше внимания обеспечению конфиденциальности и целостности передаваемых данных, проверке подлинности беспроводных клиентов и точек доступа.

Сетевая инфраструктура крупных организаций, как правило, содержит большое количество беспроводных точек доступа, каждая из которых нуждается в администрировании, обслуживании и обновлении политики безопасности. Cisco WLC (Wireless LAN Controller) предназначен для оптимизации этих процессов и обеспечения стабильного подключения к сети, при переключении пользователя с одной точки доступа на другую по мере передвижения по организации. Данное сетевое устройство централизует управление всеми точками доступа, находящимися в одной локальной сети, позволяет устанавливать различные режимы их работы. Например, в режиме мониторинга единственной задачей точки доступа становится прослушивание частотного спектра в канале и обнаружение атак на стороне беспроводной сети. А при их обнаружении WLC уведомляет об этом сетевого администратора. Также WLC может выступать в роли DHCP-сервера и авторизовывать пользователей.

При внедрении WLC в инфраструктуру локальной сети следует также обеспечить его защиту. Для этого необходимо установить граничное устройство – маршрутизатор или межсетевой экран.

Таким образом, использование WLC позволяет строить масштабные локальные сети, обеспечивает удобство и простоту администрирования сети, безопасность ее работы [1–3].

Литература

1. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=d5irhvYDiGI – Дата доступа: 30.04.2021.
2. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=0lDiFNIKepM – Дата доступа: 01.05.2021.
3. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://ru.it-brain.online/tutorial/wireless_security/wireless_security_quick_guide/ – Дата доступа: 30.04.2021.

ИНТЕГРАЦИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ В УЧЕБНЫЙ ПРОЦЕСС ПРИ ПРОВЕДЕНИИ ЛАБОРАТОРНЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»

В.М. Алефиренко

В учебный план специальности «Электронные системы безопасности» [1] в качестве компонента учреждения высшего образования входит дисциплина «Методы и технические средства обеспечения безопасности», которая читается на 3 курсе в 2-х семестрах и состоит из 2-х частей: «Методы и технические средства обеспечения безопасности информации» и «Методы и технические средства обеспечения безопасности объектов». Первая часть дисциплины посвящена изучению вопросов, связанных с техническими методами и средствами защиты информации. Помимо лекционного материала, она включает практические занятия и лабораторные работы. Одна из лабораторных работ – «Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов» была разработана таким образом, чтобы ее ресурсы (теорию, методику проведения, программу расчета параметров) можно было бы гибко использовать для проведения научных исследований по защите речевой информации различными видами маскирующих сигналов. В качестве маскирующих сигналов

использовались как специально предназначенные для этой цели профессиональные сигналы – «белый шум», «розовый шум», «речевая смесь», так и бытовые сигналы – различные виды музыкальных и хоровых произведений (органная музыка, оркестровая музыка, хоровое пение и др.). Методика проведения, классы качества и нормы слоговой разборчивости речи определялись в соответствии с [2]. Для надежной защиты речевой информации в местах возможного ее перехвата необходимо обеспечивать разборчивость слов менее 60 %. Возможность регулярного проведения лабораторной работы в течение нескольких лет с различным контингентом студентов (аудиторов) позволило получить статистические результаты исследований на основании обработки около 100 данных. Были получены следующие результаты: «чистая речь» – 91 % (класс качества I, норма слоговой разборчивости 86–93 %); «белый шум» – 39 % (ниже IV, 45–60 %); «розовый шум» – 51 % (IV, 45–60 %), «речевая смесь» – 49 % (IV, 45–60 %), органная музыка (произведение Баха) – 75 % (III, 61–75 %); музыкальное произведение (рок-музыка) – 49 % (IV, 45–60 %). Как видно, некоторые виды музыкальных произведений могут конкурировать с профессиональными сигналами, однако это не значит, что они могут успешно использоваться для защиты информации вместо них. Таким образом, при соответствующей подготовке лабораторных работ, они могут использоваться не только для обучения студентов, но и для проведения научных исследований, особенно в тех случаях, когда требуется получение статистических данных на протяжении длительного времени.

Литература

1. Образовательный стандарт Высшего образования ОСВО 1-39 03 01-2013. Минск: МО РБ, 2013. 31 с.

2. СТБ ГОСТ Р 50840–2000. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – Минск: Госстандарт РБ, 2000. 372 с.

БЕЗОПАСНОСТЬ В JAVASCRIPT

М.А. Аниховский, И.Ю. Изгачёв, В.А. Ковалёв, В.Я. Анисимов

В данной работе описываются наиболее распространенные угрозы безопасности веб-сайтов: XSS, SQL-инъекции и CSRF. Рассмотрим их подробнее. XSS или межсайтовый скриптинг (от англ. Cross Site Scripting) - тип атаки на веб-системы, заключающийся во внедрении в страницу вредоносного кода. Уязвимость вызвана недостатками клиентских языков сценариев, таких как HTML и JavaScript. Через XSS злоумышленники могут внедрять сторонний JavaScript код для выполнения вредоносных задач. XSS-атаки могут привести к краже личных данных и распространению вирусов, а иногда и к удаленному управлению браузером пользователя. Предотвратить потенциальные XSS угрозы можно с помощью экранирования пользовательского ввода [1].

Уязвимости SQL-инъекций дают злоумышленникам возможность выполнять произвольный SQL код в базе данных, позволяя им получать, изменять или удалять данные независимо от разрешений пользователя. Типы внедрения SQL включают: внедрение на основе ошибок, внедрение на основе логических ошибок и внедрение на основе времени. Данная уязвимость имеет место быть, если пользовательский ввод напрямую передается в SQL запрос без надлежащего экранирования потенциально опасных символов [2].

CSRF или подделка межсайтовых запросов (от англ. Cross Site Request Forgery) – уязвимость, позволяющая злоумышленникам отправлять авторизованные запросы,

используя данные сессии жертвы. Многие веб-приложения используют cookies для хранения сессии пользователя. Для проведения простейшей CSRF атаки злоумышленнику необходимо оставить ссылку с кодом, который будет отправлять запрос с данными, выгодными злоумышленнику. При переходе по ссылке браузер автоматически прикрепит к запросу cookies жертвы, включая данные его сессии. Для защиты от CSRF уязвимостей чаще всего используются уникальные CSRF-токены для каждой пользовательской сессии (один токен в теле запроса, второй, идентичный – в cookie) [3]. Также можно защитить потенциально опасные действия паролем, который должен ввести сам пользователь.

Литература

1. Palmer S. Web Application Vulnerabilities.
2. Yaworksi P. Real-World Bug Hunting: A Field Guide to Web Hacking.
3. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.

ЭЛЕКТРОДИНАМИЧЕСКИЕ СИСТЕМЫ ПРИБОРОВ СВЧ

И.В. Баженова

Электродинамические системы современных мощных и сверхмощных электронных приборов СВЧ (гиротронов, релятивистских ламп бегущей и обратной волны – ЛБВ и ЛОВ), включая вводы и выводы энергии, представляют собой отрезки нерегулярных волноводов. Причем, режим этих волноводов оказывается чаще всего многоволновым. Улучшение характеристик указанных сверхмощных приборов СВЧ связано прежде всего с оптимизацией профиля их электродинамических систем. Это, в свою очередь, требует развития адекватной теории и методов расчета произвольно-нерегулярных волноводов.

Наиболее эффективной процедурой при расчете нерегулярных волноводов, как с вычислительной стороны, так и в отношении физической интерпретации представляется метод, основанный на отображении произвольно-нерегулярной внутренней поверхности волновода на регулярный цилиндр, коаксиал и т.д. с круговым или прямоугольным сечением [1, 2]. В преобразованной (косоугольной) системе координат решение представляется в виде связных нормальных волн с использованием проекционной процедуры. При этом амплитуды связных волн определяются системой ОДУ с переменными коэффициентами, вид которых определяется профилем неоднородного волновода. Граничные условия к этой системе ставятся в начальном и конечном сечении отрезка нерегулярного волновода (двухточечная задача). Релятивистские черенковские генераторы на нерегулярном гофрированном волноводе широко используются при получении энергии СВЧ сверхбольшой мощности.

Создание сильноточных ускорителей электронов с токами 1 – 35 кА при напряжении 0,3 – 2 МВ позволяет реализовать черенковские генераторы СВЧ с электродинамической системой в виде отрезка периодического гофрированного полого волновода, имеющие выходную мощность 1 – 30 ГВт в сантиметровом и миллиметровом диапазонах при КПД 10 – 50 % [1, 2]. Такие результаты достигнуты с использованием простейших математических моделей, справедливых для неглубокой периодической гофрировки волновода. Повышение КПД и улучшение выходных характеристик генераторов возможно на основе оптимизации всех параметров, включая профиль волновода.

Литература

1. Кураев А.А. Возбуждение продольно-нерегулярных волноводов с круглым сечением // Изв. академии наук БССР, сер. физ.-техн. наук. 1979. № 1. С. 121–127.

2. Кураев А.А. Теория и оптимизация электронных приборов СВЧ. Мн.: Наука и техника, 1979.

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД И ПРИЛОЖЕНИЕ ДЛЯ РАЗМЕЩЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ИЗОБРАЖЕНИЯ ФОРМАТА SVG

Е.А. Блинова, П.П. Урбанович

Цифровые водяные знаки (ЦВЗ) принято рассматривать как элементы стеганографических преобразований, применяемые для защиты контента от подделки или защиты авторского права на электронный контент. В качестве объекта защиты могут выступать векторные изображения в формате SVG – векторные графические файлы, предназначенные для описания смешанной векторной и растровой графики в формате XML [1]. Основные требования к ЦВЗ – надежность и устойчивость к искажениям.

В докладе приводится формальное описание метода и алгоритма встраивания ЦВЗ (или иного скрытого сообщения) в файлы изображения в формате SVG. Файлы формата SVG могут содержать графические элементы, анимацию и текст, а также элементы в виде кривых Безье [2] – вид плоских полиномиальных кривых с одним параметром. Основная идея метода состоит в разделении кубических кривых Безье на несколько кривых в определенном соотношении. Для контроля целостности ЦВЗ используется внедрение тайной информации в контрольные точки кривых Безье. Рассмотрен алгоритм обратного стеганографического преобразования для извлечения тайного сообщения и подтверждения целостности изображения. Разработано приложение для выполнения операций над ЦВЗ. Проанализирована возможность модификации метода за счет использования других видов кривых.

Литература

1. Blinova E., Shutko N. The use of steganographic methods in SVG format graphic files // New Electrical and Electronic Technologies and their Industrial Implementation; proc. of the 10th Intern. Conf., Zakopane, Poland, 23–26.06.2017. P. 45.

2. Блинова Е.А., Урбанович П.П. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG // Труды БГТУ. Сер. 3, Физ.-мат. науки и информатика. 2018. № 1 (206). С. 104–109.

ИНТЕГРИРОВАННАЯ МОДЕЛЬ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ОТРАСЛИ СВЯЗИ РЕСПУБЛИКИ БЕЛАРУСЬ

В.А. Бойправ, Л.Л. Утин

Аудит систем менеджмента информационной безопасности предприятий является основополагающим в совокупности процессов по защите информации, так как направлен на постоянное улучшение эффективности последних. Изложенные в современных международных стандартах рекомендации по проведению аудита систем менеджмента информационной безопасности носят общий характер и должны

быть адаптированы для каждой группы конкретных предприятий с учетом специфики их деятельности и требований национальных нормативных, технических и правовых актов в сфере защиты информации. Процесс адаптации указанных рекомендаций целесообразно начинать с предприятий, состояние информационной безопасности на которых напрямую определяет состояние национальной безопасности страны. К таким предприятиям относятся предприятия отрасли связи, деятельность которых связана с разработкой, использованием и/или обслуживанием критически важных объектов информатизации.

Авторами предложена интегрированная модель аудита систем менеджмента информационной безопасности предприятий отрасли связи Республики Беларусь, которая основана на принципах, изложенных в ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing, а также на:

- принципах классификации информации, соответствующих Закону Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

- принципах классификации типовых информационных систем, соответствующих СТБ 34.101.30-2017;

- требованиях по построению систем защиты информации, изложенных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 г. № 66;

- требованиях по обеспечению безопасности критически важных объектов информатизации, изложенных в Положении об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденное Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 и в Положении об обеспечении безопасности критически важных объектов информатизации, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 октября 2018 г. № 151.

Практическая реализация предложенной модели будет способствовать повышению эффективности аудита систем менеджмента информационной безопасности предприятий отрасли связи Республики Беларусь.

ГИБКИЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ НА ОСНОВЕ ПОРОШКООБРАЗНОГО УГЛЯ ДЛЯ ЗАЩИТЫ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВНЕШНИХ ПОМЕХ

О.В. Бойправ, В.А. Богуш, Л.М. Лыньков

Один из способов защиты средств обработки информации от воздействия внешних помех основан на электромагнитном экранировании помещений, в которых располагаются эти средства. В целях увеличения технологичности реализации такого способа рациональным представляется применение электромагнитных экранов, характеризующихся свойством гибкости. Кроме того, такие экраны должны быть низкостоимостными, так как в рамках рассматриваемого процесса ими покрываются строительные перегородки больших площадей. Авторами разработана методика изготовления электромагнитных экранов на основе порошкообразного угля, характеризующихся обоими из указанных свойств. Разработанная методика основана на:

1) формировании двух полимерных контейнеров, внутренние стенки которых покрыты слоем самоклеящегося материала;

2) заполнении первого из сформированных контейнеров сухим порошкообразным углем, второго – порошкообразным углем, пропитанным до насыщения водным раствором хлорида кальция равновесной концентрации;

3) закреплении посредством распыляемого клея металлизированной пленки на одной из поверхностей контейнера, заполненного порошкообразным углем, пропитанным до насыщения водным раствором хлорида кальция равновесной концентрации;

4) соединении контейнеров друг с другом посредством распыляемого клея таким образом, чтобы металлизированная пленка была задней (относительно фронта распространения электромагнитных волн) стенкой полученного в результате этого электромагнитного экрана.

Установлено, что значения коэффициента отражения электромагнитного излучения в диапазоне частот 0,7…17,0 ГГц электромагнитных экранов, изготовленных в соответствии с разработанной методикой, достигают величины –25,0 дБ, а значения коэффициента передачи – величины –35,0 дБ.

Работа выполнена в рамках НИР «Эластичные и воздухопроницаемые электромагнитные экраны на основе фольгированных материалов для обеспечения информационной и экологической безопасности» по заданию № 1.5 «Разработка новых материалов и технологий для систем электромагнитной защиты радиоэлектронного и информационного оборудования, биологических объектов от воздействия широкого спектра электромагнитных излучений, обеспечения электромагнитной безопасности населения и электромагнитной совместимости электро-, радиотехнических средств и оборудования» ГПНИ «Материаловедение, новые материалы и технологии» на 2021–2025 гг.

МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОГО ОБОСНОВАНИЯ МАТЕРИАЛОВ ДЛЯ ПОЛУЧЕНИЯ ЭЛАСТИЧНЫХ И ВОЗДУХОПРОНИЦАЕМЫХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ

О.В. Бойправ, Н.В. Богуш, Л.М. Лыньков

Одним из актуальных направлений в области разработки функциональных материалов является создание электромагнитных экранов с улучшенными эксплуатационными характеристиками. Авторами предложена и апробирована методика экспериментального обоснования материалов для получения эластичных и воздухопроницаемых электромагнитных экранов, пригодных для использования в целях обеспечения электромагнитной совместимости средств обработки информации. Предложенная методика включает в себя следующие этапы.

Этап 1. Выбор действующих материалов для получения эластичных и воздухопроницаемых электромагнитных экранов. Такие материалы названы действующими, т. к. их физические свойства, такие как электропроводность или относительная магнитная проницаемость, определяют свойства электромагнитных экранов, соответствующие их прямому назначению, т. е. обеспечению ослабления энергии электромагнитного излучения. Критериями выбора действующих материалов являются низкое значение коэффициента передачи электромагнитного излучения в СВЧ-диапазоне длин волн ($\leq -10{,}0$ дБ) и свойство гибкости при стандартных условиях. Для оценки соответствия указанным критериям материалов, предполагаемых для использования в качестве действующих материалов для получения эластичных и воздухопроницаемых электромагнитных экранов, необходимо выполнять следующее:

- измерение значений коэффициента передачи электромагнитного излучения в СВЧ-диапазоне длин волн материалов, предполагаемых для использования в качестве

действующих материалов для получения эластичных и воздухопроницаемых электромагнитных экранов;

- сгибание (до момента соединения противоположных краев) и разгибание вручную материалов, предполагаемых для использования в качестве действующих материалов для получения эластичных и воздухопроницаемых электромагнитных экранов, и визуальная оценка поверхности таких материалов на предмет наличия разрывов и/или расслоений.

Этап 2. Выбор вспомогательных материалов для получения эластичных и воздухопроницаемых электромагнитных экранов. Такие материалы названы вспомогательными, т. к. их физические свойства определяют эксплуатационные преимущества рассматриваемых электромагнитных экранов, т. е. эластичность и воздухопроницаемость. Представленные свойства и являются критериями выбора вспомогательных материалов для получения эластичных и воздухопроницаемых электромагнитных экранов. Таким критериям соответствуют материалы следующих типов: трикотажные, волокнистые и гибкие перфорированные полимерные.

Работа выполнена в рамках НИР «Эластичные и воздухопроницаемые электромагнитные экраны на основе фольгированных материалов для обеспечения информационной и экологической безопасности» по заданию № 1.5 «Разработка новых материалов и технологий для систем электромагнитной защиты радиоэлектронного и информационного оборудования, биологических объектов от воздействия широкого спектра электромагнитных излучений, обеспечения электромагнитной безопасности населения и электромагнитной совместимости электро-, радиотехнических средств и оборудования» ГПНИ «Материаловедение, новые материалы и технологии» на 2021–2025 гг.

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ПЕЧАТНЫХ ПЛАТ ЭЛЕКТРОННЫХ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В.Н. Бондарев

Миниатюризация электронных устройств защиты информации приводит к увеличению плотности поверхностного монтажа, снижению ширины проводников и зазоров, уменьшению диаметров межслойных отверстий печатных плат (ПП). При воздействии термических и механических напряжений на зазоры между проводниками, могут возникать отслоения проводящего рисунка ПП, что приведет к отказу электронного модуля (печатного узла). Поэтому оценке и обеспечению надежности ПП следует уделять особое внимание.

Методы и модели оценки надежности ПП включены в справочники разных стран (Россия, США, Франция) по расчету надежности электронного оборудования [1]. Установлено, что значения показателей надежности ПП отличаются друг от друга в зависимости от того, по какой модели проводился расчет. Цель исследования – систематизация моделей оценки надежности ПП, их анализ и выбор той, которая обеспечивает наиболее достоверные (подтверждаемые практикой) результаты. Из анализа моделей установлено, что наиболее полно конструкторско-технологические особенности ПП учитывает модель прогнозирования эксплуатационной надежности, приводимая в справочнике RDF 2000 (Франции) [2]. Данная модель, в отличие от других моделей, включает параметры, принимающие во внимание габариты ПП и особенности токопроводящих проводников, из-за разрушения которых могут возникать отказы.

Литература

1. Боровиков С.М., Цырельчук И.Н., Троян Ф.Д. Расчет показателей надежности радиоэлектронных средств. Минск: БГУИР, 2010. 68 с.
2. A universal model for reliability prediction of Electronics components, PCBs and equipment. RDF 2000: reliability data handbook. Paris: UTE C 80-810. 2000. 99 p

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

Т.В. Борботько

В современном обществе наблюдается устойчивая тенденция внедрения информационных технологий в различные сферы его жизнедеятельности. Это приводит к ряду положительных эффектов, таких как упрощение доступа населения к различным видам услуг, в промышленности – сведение к минимуму ошибок при реализации технологических процессов, для бизнеса – появление новых рынков сбыта и способов монетизации и т. д. Вместе с тем, доступность информационных систем различного назначения привлекает внимание к ним исследователей, в том числе тех, которые ориентированы на деструктивное вмешательство в процесс функционирования таких систем. Исходя из особенностей действия нарушителя, можно сформулировать следующие принципы.

Первый принцип – информированности. Построение эффективной системы защиты информации основано на понимании модели нарушителя. Это позволяет спланировать и подготовить ряд необходимых организационно-технических мероприятий по противодействию ему.

Второй принцип – многозональности. Любая информационная система содержит информационные ресурсы, критичность которых для обеспечения бизнес процессов в организации различна. Обнаружить и остановить кибератаку на периметре сети – чрезвычайно сложное мероприятие. Исходя из этого информационную сеть необходимо разделить на различные зоны, что позволит ее «замедлить» и выиграть время для ее обнаружения.

Третий принцип – восстанавливаемости. Одна из составляющих ущерба от кибератаки – это время простоя организации, которое может быть обусловлено, например, выводом из строя оборудования вследствие функционирования вредоносной программы.

Изложенные принципы противодействия кибератакам учитывают особенности их реализации и могут быть использованы при планировании соответствующих организационно-технических мероприятий.

ИДЕНТИФИКАЦИЯ КОМПЬЮТЕРА ПОЛЬЗОВАТЕЛЯ В СЕТИ ИНТЕРНЕТ

Ф.Т. Борботько

На сегодняшний одной из важнейших проблем можно считать однозначную идентификацию пользователя в сети Интернет. Причиной возникновения данного вопроса являются противозаконные действия, совершаемые лицами, для получения какой-либо выгоды вопреки установленным нормам. Сложность данной задачи заключается в том, что уникальных идентификаторов, используя которые мы можем установить тождественность искомому лицу, не так уж и много. Стоит так же сказать, что для такого поиска нам нужны те признаки, которые невозможно или очень сложно подменить.

Следует выделить следующие идентификаторы: MAC адрес компьютера, цифровой отпечаток (fingerprint) и адреса DNS серверов. Подменить MAC адрес можно с использованием специального программного обеспечения, например, 0x4553 Intercepter. Цифровой отпечаток, представляет собой хэш, значение которого включает более 10 параметров, которые используются для корректного выполнения html кода страницы. Из этого можно сделать вывод о том, что данный идентификатор подменить гораздо сложнее, т.к. он зависит от некоторых признаков, изменения которых приведут к неудобству просмотра веб-страницы. Цифровой отпечаток позволяет обеспечить точность идентификации до 94–95 %. По адресам DNS серверов можно собрать примерные геоданные о местонахождении персонального компьютера благодаря способу их присвоения. Вместе с тем они так же, как и MAC адрес, могут быть легко заменены с помощью программного обеспечения.

Таким образом, самым надежным из трех вышеперечисленных признаков является цифровой отпечаток, однако существуют другие параметры персонального компьютера, например, версия операционной системы, аппаратное обеспечение компьютера, которые используются или могут быть использоваться для его идентификации [1, 2].

Литература

1. Джуди Новак, Стивен Норткатт, Дональд Маклахлен. Как обнаружить вторжение в сеть (Network intrusion detection an analyst’s handbook). М.: Лори, 2012. 384 с.

2. Что такое отпечаток браузера, и как его скрыть // IPper анонимность в интернете [Электронный ресурс]. 2019. Режим доступа: https://ipper.ru/article/?p=103. Дата доступа: 06.11.2019.

МОДЕЛЬ ОЦЕНКИ ОЖИДАЕМОЙ НАДЕЖНОСТИ ПЛАНИРУЕМЫХ К РАЗРАБОТКЕ ПРИКЛАДНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ СИСТЕМ МОНИТОРИНГА И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

С.М. Боровиков, В.О. Казючиц, С.С. Дик, А.В. Будник

Разработчики прикладного программного обеспечения, в том числе используемого для обеспечения информационной безопасности, хотели бы знать ожидаемый уровень надежности компьютерных программ на ранних этапах их проектирования (до написания кода на языке программирования). Цель работы – получить модель прогнозирования ожидаемой надежности планируемых к разработке прикладных компьютерных программ для систем мониторинга и обеспечения безопасности. Для достижения цели анализировались статистические данные об эксплуатационной надежности компьютерных программ разного назначения. В работе [1] описана модель, ориентированная на оценку надежности компьютерных программ некоторых областей применения. В статье [2] обоснован ее уточненный вид, который использован для получения модели оценки ожидаемой надежности прикладных компьютерных программ для систем мониторинга и обеспечения безопасности.

Доклад подготовлен при выполнении проекта № Ф20МВ-021 на тему «Статистические модели надежности прикладных программных средств и их использование для оценки ожидаемой безотказности компьютерных программ на ранних этапах их разработки» (утвержден Научным советом БРФФИ 22 апреля 2020 г.).

Литература

1. Боровиков С.М., Дик С.С., Лэ В.Н., Клинов К.И. Возможный подход к оценке надежности разрабатываемых программных средств на ранних этапах проектирования информационно-компьютерных систем // Globus: технические науки – от теории к практике. 2020. Вып. 1 (32). С. 4–9.

2. Боровиков С.М., Казючиц В.О., Хорошко В.В., Дик С.С., Клинов К.И. Оценка ожидаемой надежности прикладных программных средств для компьютерных информационных систем // Информатика. 2021. Т. 18, № 1. С. 84–95.

МОДЕЛИРОВАНИЕ ЧАСТОТНЫХ ПРЕОБРАЗОВАНИЙ РАДИОПРИЕМНИКА ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ

Д.Г. Булавко, Д.А. Лисов

Основными требованиями, предъявляемыми к разработке приемников измерительных систем, являются очень широкие частотный и динамический диапазоны, приемлемые уровни отношения сигнал-шум и интермодуляционных искажений, а также минимизация массогабаритных параметров. Применение компьютерного моделирования приемника с помощью пакетов программ схемотехнического моделирования позволяет еще до этапа производства проводить анализ разработанного устройства и формировать техническое задание для смежных с ним блоков аппаратуры.

Проведено моделирование интермодуляционных помех приемника, построенного по супергетеродинной схеме приема с двумя преобразованиями частоты, рабочий диапазон частот принимаемых сигналов от 1 до 18 ГГц. Исходными данными для расчетов являлись параметры, функциональных узлов приемника (параметры элементов графической модели), на которых планировалась его техническая реализация, а также параметры входного сигнала приемника и сигналов гетеродинов. Полученные результаты моделирования показали, что образуется помехи с частотами 950 МГц, 1350 МГц, 1400 и 1600 МГц попадающие в полосу пропускания выходных фильтров приемника. Уровни данных помех составляют от минус 39 до 44 дБм, что является достаточным для детектирования на последующем аналогово-цифровом преобразователе.

Анализ результатов моделирования показывает, что интермодуляционные помехи образуются в значительной степени из-за несовершенства смесителей, малой развязки между входами сигналов гетеродинов и выходами промежуточной частоты. Наиболее приемлемым решением данных проблем является расчет ожидаемых мешающих сигналов и учет их при последующей цифровой обработке сигналов, применение других решений либо вызовет значительное удорожание приемника, либо даст малый результат.

ПРОГРАММИРОВАНИЕ НАВЫКОВ ГОЛОСОВОГО ПОМОЩНИКА НА ПРИМЕРЕ УМНОЙ КОЛОНКИ «АЛИСА»

А.Е. Булай, С.Б. Протосовицкая

Современные технологии развились до того уровня, когда у большинства людей в кармане находится средство управления обширным количеством информации и инструмент, способный решать задачи огромных масштабов – смартфон. Люди, не задумываясь, пользуются поиском, онлайн-сервисами, слушают музыку и смотрят

фильмы. Однако на бытовом уровне человеку все же привычней общаться голосом, разговаривать. Темп и динамика жизни приводят к тому, что у людей нет времени читать длинные сообщения, у них даже нет времени писать текст. Эти и другие факторы стали причиной создания голосового помощника (иначе его называют голосовым ассистентом). В работе рассматривается задача программирования навыков для голосового ассистента Алиса. Под навыком будем понимать сервис, реализующий диалог, который запускается некоторой командой и расширяет возможности голосового ассистента. Объект исследования: голосовые ассистенты. Предмет исследования: программирование голосовых ассистентов. Методы исследования – анализ, обобщение, формализация, эксперимент.

Ведущие ИТ-компании мира (в частности, Apple, Amazon, Google, Microsoft, Alibaba, Baidu) настойчиво рекламируют и внедряют в свои продукты голосовых помощников на основе искусственного интеллекта. «Яндекс Алиса» – виртуальный голосовой помощник, который уникален своей человечностью. С ним, точнее с ней, можно общаться. Она распознает речь, поддерживает диалог, шутит, иногда вольничает и острит, дает ответы на вопросы и, благодаря запрограммированным навыкам, решает простые прикладные задачи.

Когда Алисе задают вопрос, она распознает голос пользователя и превращает его в текст. Эта технология называется SpeechKit. В Алисе собрано более миллиарда сообщений с разными голосами, произношениями и акцентами. После распознавания, помощник проецирует фразу в семантическое пространство широкой размерности. В этом пространстве находится множество точек. Каждая точка этого пространства – высказывание, которое имеет свою тему. Далее голосовой ассистент находит необходимое место и сравнивает запрос с подходящим ответом. Предугадать, что он ответит невозможно. Когда ответ выбран, Алиса его произносит с помощью технологии Text-to-Speech и нейросети, что придает голосу натуральность.

Ко всей полезности и красоте технологии, существуют пару недостатков.

1. На платформе Яндекс.Диалоги, бывает, что добавленный навык не проходит модерацию. Причиной может служить слишком общее имя навыка, например, «погода в Гродно», что схоже с «погода в Минске».

2. Документация платформы Яндекс.Диалоги не всегда соответствует действительности, так как платформа развивается слишком быстро

3. Конфиденциальность данных, используемых в диалоге с Алисой.

Последний пункт хочется выделить особенно: Алиса не слышит пользователя до момента ее активации голосом с помощью уникального слова для ее включения или кнопкой. Помимо этого, вся информация, которую сообщают Алисе, проходит сложное и надежное шифрование. Однако, при использовании голосовых помощников или умных колонок рекомендуется ограничить действия, которые они могут совершать, а также избавиться от случайной активации путем определения уникального слова для его включения [1]. Голосовые помощники облегчают повседневную жизнь людей, помогают людям с ограниченными возможностями, дают ресурсы для реализации потребностей своих пользователей.

Литература

1. Безопасны ли умные колонки? / Защитные решения для дома и бизнеса | Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/how-to-improve-your-smart-speaker-privacy. – Дата доступа: 20.03.2021.

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ С ИСПОЛЬЗОВАНИЕМ РАДИОПРИЕМНЫХ МОДУЛЕЙ ДИАПАЗОНА 433 МГц

М.А. Буневич, Е.Н. Каленкович, А.И. Майоров, И.А. Врублевский

В настоящее время для организации связи между различными устройствами систем широко применяются беспроводные решения. Как правило, для этих целей используют радиомодули, работающие в безлицензионных диапазонах 433, 868 или 2400 МГц [1, 2]. Применение данных частотных диапазонов имеет ряд особенностей, связанных в первую очередь, с условиями распространения радиоволн и допустимыми мощностями передающих устройств. В большинстве случаев мощность ограничена единицами – десятками милливатт, и поэтому максимальное расстояние передачи данных составляет от нескольких десятков время до нескольких сотен метров, т.е. ограничено ближней зоной.

Целью работы являлось определение характеристик двухсигнальной избирательности типовых приемных модулей диапазона 433 МГц для оценки помехоустойчивости и выявления побочных каналов приема. Показано, что для оценки помехоустойчивости приемных устройств радиомодулей можно использовать характеристику избирательности приемного устройства, в частности характеристику двухсигнальной избирательности. Оно позволяет выявить побочные каналы приема и оценить минимальное отношение сигнал/помеха на этих частотах, при котором система передачи данных еще будет выполнять свои функции. Для исследования двухсигнальной избирательности типового радиоприемного модуля, работающего в диапазоне 433 МГц, была собрана экспериментальная установка. Исследование производилось в полосе частот от 420 до 450 МГц. Шаг перестройки частоты 50 кГц. Оценка степени искажения принимаемого сигнала производилась при помощи осциллографа по искажению преамбулы и заголовка полезного информационного сообщения. Уровень полезного сигнала на входе радиоприемного модуля был установлен на уровне минус 75 дБм. В результате проведения эксперимента была построена характеристика двухсигнальной избирательности приемного радиомодуля. Полученные по результатам характеристики измерений, показывают, что приемник RRS-2 построен по супергетеродинной схеме с нижним преобразованием частоты – зеркальный канал находится в районе 432,9 МГц, т.к. ПЧ равна 500 кГц, а зеркальный канал отстоит от частоты приема на две промежуточные.

Литература

1. RRS2-XXX – AM - супергетеродинный приемник с входным LC-фильтром [Электронный ресурс] / Telecontrolli Srl. – Naples, Italy, 2009. – Режим доступа: http://www.telecontrolli.com/pdf/receiver/rrs2.pdf . – Дата доступа: 21.07.2009.

2. Каленкович Е.Н., Мартинович П.В. Программно-аппаратный комплекс для оценки электромагнитной обстановки в безлицензионном диапазоне радиочастот 433 МГц // Технические средства защиты информации: тезисы докладов XVIII Белорусско-российской научно-технической конференции, Браслав, 24–28 мая 2010 г. С. 20.

О НЕКОТОРЫХ ВОПРОСАХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ВОЕННОЙ АКАДЕМИИ РЕСПУБЛИКИ БЕЛАРУСЬ

Е.В. Валаханович, Л.В. Михайловская

В настоящее время уверенное владение методами защиты информации для военных специалистов является жизненно необходимыми навыками.

В связи с этим, на кафедре высшей математики Военной академии Республики Беларусь разработаны и внедрены различные курсы: «Защита информации», «Математические методы обработки информации», «Прикладная математика» для курсантов специальностей «Телекоммуникационные системы (эксплуатация)», «Эксплуатация автоматизированных систем обработки информации», «Телекоммуникационные системы (радиоэлектронная борьба, радиоэлектронная разведка)», «Авиационные радиоэлектронные системы».

Целью изучения названных учебных дисциплин является обучение основным математическим методам теории чисел, теории групп, колец и полей, конечных полей для их последующего использования в защите информации как от помех, так и от несанкционированного доступа, в цифровой обработке сигналов и изображений, в помехоустойчивом кодировании; освоение курсантами основных алгоритмов классической и современной криптографической защиты информации и математических методов формирования и обработки помехоустойчивых кодов.

Особенность преподавания курса «Прикладная математика» состоит в широком использовании информационных технологий в области программирования, в том числе выполнения лабораторных работ, в ходе которых курсанты начального уровня выполняют упрощенные задачи; курсанты среднего уровня – задания с дополнительными условиями; подготовленным курсантам предлагаются задания, требующие хорошей математической подготовки, самостоятельного поиска решений и разработки мини-программ.

Знание математических основ защиты и передачи информации дает все необходимое для усвоения алгоритмов современных инфокоммуникационных и криптографических систем, используемых в практической деятельности военными специалистами.

УЯЗВИМОСТЬ СТАНДАРТОВ WI-FI 802.11 ДЛЯ АТАКИ ДЕАУТЕНТИФИКАЦИИ

А.М. Васюкович, Г.А. Пухир

Современную информационную среду невозможно представить без использования Wi-Fi-технологии. Wi-Fi применяется не только для домашнего пользования, но и в корпоративных сетях. В связи с этим, исследование уязвимостей протокола IEEE 802.11 актуально. Самыми популярными стандартами Wi-Fi на сегодняшний день являются стандарты 802.11b/g/n/ac [1]. Эти стандарты поддерживают все современные устройства и являются основными для подавляющего большинства маршрутизаторов средне/низкого диапазона цены. Однако у этих стандартов существует серьезная уязвимость: подверженность атаке деаутентификации.

Атака деаутентификации – это атака типа «отказ в обслуживании», которая заключается в отправке деаутентификационных фреймов на AP (англ. Access Point – точка доступа) от имени клиента неавторизованным устройством [2]. Такая уязвимость существует из-за того, что эти фреймы при использовании стандартов 802.11b/g/n/ac криптографически не защищены, соответственно, злоумышленнику достаточно узнать MAC-адрес жертвы для реализации атаки. Посредством постоянного повторения атаки, скорость осуществления которой значительно выше скорости повторной авторизации, клиенту можно запретить передачу или получение данных на неопределенный срок.

Существуют несколько способов защиты от данной атаки: использование дорогостоящего оборудования с поддержкой стандарта 802.11w, который обеспечивает шифрование фрейма, однако замедляет скорость Wi-Fi на 20 % [3], или использование нового стандарта шифрования WPA3, что крайне не рекомендуется, из-за найденной

уязвимости Dragon Blood [4]. Кроме этого, существует программы, а также устройства [5], которые позволяют установить факт совершения атаки, однако они не могут локализовать злоумышленника. Следовательно, актуален поиск эффективного способа ее устранения.

Литература

1. Степутин А.Н., Николаев А.Д. Мобильная связь на пути к 6G. В 2 Т. Москва-Вологда: Инфра-Инженерия, 2018. 804 с.

2. Bellado J., Savage S. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions // Proceedings of the 12thUSENIX Security Symposium, Aug 2003, Washington, DC, USA. P. 15–27.

3. Eian M., Mjølsnes S.F. A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities // Proceedings IEEE INFOCOM, March, 2012 in Orlando, Florida, USA. P. 918–926.

4. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // IEEE Symposium on Security and Privacy, 2020. P. 517–533.

5. Горохов Д.Б., Чупин В.Ю. Обнаружение атак типа деаутентификации в сетях стандарта 802.11 с помощью модуля esp8266 // Труды Братского государственного университета. Т.2. Братск, 2019. С. 58–62.

УЯЗВИМОСТЬ ПЕРЕПОЛНЕНИЯ СТЕКА ДЛЯ ИСПОЛНЕНИЯ ВРЕДОНОСНОГО КОДА

А.В. Волощик

Речь пойдет о стеке вызовов. Если кратко, то в нем есть переданные в функцию переменные (аргументы), локальные переменные и адрес возврата. Переполнение стека может привести к его контролю со стороны злоумышленника. А это может повлечь как модификацию локальных переменных в функции, так и подмену ее адреса возврата на вредоносный код. Притом уязвимость может работать и на современных ОС.

В рамках данной работы раскрыта тема использования уязвимости переполнения стека, показана возможность исполнения вредоносного кода. Необходимо отметить, что уязвимость не является распространенной на данный момент, вследствие наличия встроенной защиты в современных высокоуровневых языках программирования. Низкоуровневые языки слабо защищены от этой уязвимости, т. к. позволяют прямо обращаться к памяти. Однако актуальные версии компиляторов (C и C++) предусматривают механизмы защиты и предупреждения, такие как warnings о небезопасных функциях (вроде strcpy, gets), stack canary (дополнительная область стека, перезапись значения которой вызывает срабатывание защиты) и многие другие со стороны самой ОС.

Проанализировав ресурсы OWASP и CWE, исходные коды некоторых продуктов на GitHub (Facebook, Microsoft и др.) можно сказать, что проблема отслеживается указанными компаниями, но в компаниях, которые не выделяют бюджет под InfoSec отделы (мелкий и средний бизнес) могут существовать подобные уязвимости [1–3].

Литература

1. Protostar: Andrew Griffiths&; Exploit Education [Electronic resource]. – Access mode: exploit.education/protostar. – Date of access: 07.05.2021.

2. Exploit Database – Exploits for Penetration Testers, Researchers, and Ethical Hackers [Electronic resource]. – Access mode: www.exploit-db.com. – Date of access: 07.05.2021.

3. Smashing The Stack For Fun And Profit [Electronic resource]. – Access mode: www-inst.eecs.berkeley.edu//~cs161/fa08/papers/stack_smashing.pdf. – Date of access: 07.05.2021.

МЕРЫ ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИОННОЙ СРЕДЫ БАНКА

С.Ю. Воробьёв, Д.А. Жук, В.А. Русак, В.А. Шкред

Для успешного отражения банками Республики Беларусь атак в цифровой информационной среде необходимо выполнение следующих мер:

- создание информационной инфраструктуры, которая позволит надлежащим образом обеспечить информационную безопасность;
- использование соответствующих аппаратных, программных и программно-аппаратных комплексов средств защиты информации;
- мониторинг событий безопасности;
- постоянное повышение квалификации работников, отвечающих за информационную безопасность;
- обучение работников банков основам информационной безопасности;
- поддержание здорового климата в коллективе;
- информирование и обучение клиентов банков финансовой и цифровой грамотности;
- разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке;
- создание команды по расследованию инцидентов информационной безопасности из числа наиболее подготовленных сотрудников;
- скрупулезный подбор персонала в банковские организации с учетом их профессиональных, нравственных и моральных качеств;
- взаимодействие и обмен информацией о кибератаках между банками, правоохранительными органами и организациями, осуществляющими помощь в борьбе с угрозами цифрового пространства.

Создание современной и надежной системы информационной безопасности и соблюдение требований норм последней всеми участниками информационного обмена является залогом доверия не только к конкретной кредитно-финансовой организации, но и ко всей банковской системе государства.

ЭЛЕКТРОХИМИЧЕСКАЯ СТОЙКОСТЬ МАГНИТНЫХ НАНОКОМПОЗИТОВ НА ОСНОВЕ ПОРИСТОГО АНОДНОГО ОКСИДА АЛЮМИНИЯ ДЛЯ ЭЛЕМЕНТОВ ОБРАБОТКИ ИНФОРМАЦИИ

А.И. Воробьева, Е.А. Уткина

Упорядоченные матрицы из пористого анодного оксида алюминия (ПАОА) благодаря их уникальным свойствам широко используются в качестве шаблона (template) при изготовлении новых композитных, в том числе магнитных, материалов. Сравнительный анализ методов исследования электрохимических свойств ПАОА и нанокомпозитов на его основе показал, что наиболее подходят методы линейной и циклической вольтамперометрии. Практический интерес исследований в этом направлении связан также с тем, что встраивание различных наноэлементов

в химически и термически инертную матрицу из оксида алюминия является одним из способов повышения их стабильности при изменении окружающих условий.

Для проведения электрохимических исследований использовали потенциостат/гальваностат AUTOLAB PGSTAT302n (Utrecht, The Netherlands), обработку данных проводили с использованием программного обеспечения NOVA, версия 1,10. Испытания проводили в типичной трехэлектродной ячейке с хлоридсеребряным электродом сравнения ЭВЛ-1-М-1 (Ag/AgCl/KCl). Вспомогательным электродом служила платиновая проволока, рабочим электродом – исследуемый композитный материал. Исследования коррозионных свойств (включая слои титана без композитного покрытия) выполнялись в 0,9 % водном растворе NaCl. Для определения параметров, характеризующих коррозионные свойства образцов, поляризационные кривые были построены в полулогарифмических (тафелевских) координатах потенциал – логарифм плотности тока.

Электрохимические исследования композита показали, что полученный материал обладает достаточно хорошей коррозионной стойкостью в диапазоне потенциалов от –1,4 до +1,4 В (Ag/AgCl) в солевом растворе, широко используемом в коррозионных исследованиях новых материалов. Использовали три известные методики электрохимического анализа: метод экстраполяции кривых поляризации, метод поляризационного сопротивления [1, 2] и метод Белеевского [3]. Все методы дали сопоставимые результаты. Более подробная информация об электрохимических свойствах наностолбиков Ni в ПАОА по сравнению с аналогичными образцами из других источников представлена в работе [4].

Литература

1. McCafferty E. Introduction to corrosion science. Springer, New York, 2010. 501 p.

2. Scully J.R. Polarization resistance method for determination of instantaneous corrosion rates. Corossion. 2000, 56, 199.

3. Beleevskii V.S.; Konev K.A.; Novosadov V.V.; et. al. Estimating corrosion current and tafel constants from the curvature of voltammetric curves near the free-corrosion potential. Protec. Of Met. 2004, 40, 566.

4. Vorobjova A.I., Tishkevich D.I., Vinnik D.A. Formation and Corrosion Behavior of Nickel/Alumina Nanocomposites // Solid State Phenomena. 2020, 299, 100.

ВЫЯВЛЕНИЕ ПРИЗНАКОВ КОНТРАФАКТА В ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЕ АППАРАТНЫХ СРЕДСТВ В АСПЕКТЕ ЗАЩИТЫ ИНФОРМАЦИИ В СНГ

Г.П. Гавдан

По данным Организации экономического сотрудничества и развития Мировой объем торговли контрафактной и пиратской продукцией в мире, в 2013 году составил 461 млрд. долларов, а в 2017 году – свыше 553 млрд. долларов [1]. Исследование, проведенное «Business Week», показало, что поддельный продукт составляет не менее 7% от внешней мировой торговли [2]. В России, согласно данным Росстата, оборот контрафактной продукции в 2017 году приблизился к трем трлн. рублей [3]. Контрафактная экспансия сказалась и на рынке электронных изделий. Сегодня испытательным лабораториям принадлежит устойчивый тренд, связанный с продолжающимся ростом доли контрафакта образцов электронной компонентной базы [4] аппаратных средств (ЭКБ АС). Анализ существующей зарубежной и российской нормативной базы по методам и средствам выявления подозрительных

образцов электронной компонентной базы аппаратных средств показывает, что дела здесь обстоят не так просто, как хотелось бы [5]. В настоящее время в России, к сожалению, имеется недостаток национальных государственных стандартов, содержащих требования к испытательным лабораториям и к определяющим методам и средствам выявления контрафактных ЭКБ АС (отсутствуют за исключением [6–8], которые являются переводом стандартов SAE). В это же время существуют международные стандарты, разработанных для борьбы с контрафактной продукцией в ЭКБ, появившихся как следствие переноса производственных мощностей микроэлектроники из стран Европы и США в Юго-Восточную Азию. Контрафакция на рынке сегодня выгодна и остается достаточно востребованной, то наличие данного направления подтолкнуло российскую промышленность, особенно оборонный и аэрокосмический сегменты заняться разработкой методов выявления контрафактных изделий (в том числе и в ЭКБ АС). Работы [9, 10] в этом направлении ведутся, но совершенствование методов выявления контрафактной микроэлектронной продукции, объединение общих усилий в их внедрении и др. остается, сегодня одним из важных направлений в России и в совместной работе стран содружества независимых государств (СНГ).

Литература

1. Материалы VI Международного форума «Антиконтрафакт–2018». Итоговые документы. С. 155.
2. Урличич Ю., Данилин Н., Чернов Д., Белослудцев С. Контрафактная продукция на рынке электронных компонентов // Современная электроника № 5/2006. С. 7.
3. Материалы VI Международного форума «Антиконтрафакт–2018». Итоговые документы. С. 33.
4. Лактионов А.В., Левин Р.Г., Емельянова И.В., Ершов Л.А., Малютенкова С.Э. Опыт выявления электронных компонентов с признаками контрафактного происхождения в ИЦ АО «РНИИ «Электронстандарт» // Петербургский журнал электроники. 2018, № 1 (90). С. 27–46.
5. Кессаринский Л.Н., Ширин А.О., Коваль К.А., Тайибов Ф.Ф., Каменева А.С. Выявление признаков контрафакта в изделиях электронной компонентной базы в аспекте обеспечения промышленной кибербезопасности // Безопасность информационных технологий. 2018. Т. 26, № 2. С. 117–128.
6. ГОСТ Р 57880-2017 Система защиты от фальсификаций и контрафакта. Электронные изделия. Предотвращение получения, методы обнаружения, сокращение рисков применения и решения по использованию фальсифицированной и контрафактной продукции.
7. ГОСТ Р 57881-2017 Система защиты от фальсификаций и контрафакта. Термины и определения.
8. ГОСТ Р 57882-2017 Система защиты от фальсификации и контрафакта. Изделия электронные. Критерии верификации для оценки соответствия практики и методов организаций требованиям по противодействию обороту фальсифицированной и контрафактной продукции.
9. Кессаринский Л.Н., Артамонов А.С., Тайибов Ф.Ф., Коваль К.А., Каменева А.С., Бойченко Д.В., Грайр А. Овсепян Идентификация элементной компонентной базы киберфизических систем // Безопасность информационных технологий. 2018. Т. 25, № 3. С. 67–78.
10. Дураковский А.П., Кессаринский Л.Н, Ширин А.О., Артамонов А.С., Бойченко Д.В., Тайибов Ф.Ф. Идентификация элементной компонентной базы с целью исключения контрафакта и анализа результатов радиационных испытаний. Актуальные направления

развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации: XI Всероссийская межведомственная научная конференция: материалы и доклады. Орел, 5–6 февраля 2019 г. В 10 ч. Ч. 5 / под общ. ред. П.Л. Малышева. – Орел: Академия ФСО России, 2019. С. 65–67.

РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ ПРОТИВОДЫМНОЙ ВЕНТИЛЯЦИИ ГАРАЖЕЙ-СТОЯНОК

В.Е. Галузо, О.В. Калита, В.В. Мельничук, А.И. Пинаев

В гаражах-стоянках (ГС) закрытого типа следует предусматривать для удаления продуктов горения системы вытяжной противодымной вентиляции (ПДВ) [1]. При работе системы ПДВ перепад давления на закрытых дверях путей эвакуации не должен превышать 150 Па [1]. Однако, при проведении аэродинамических испытаний систем ПДВ, это требование часто не обеспечивается. Водяное тушение как обязательный атрибут системы пожарной безопасности ГС [2] призвано предотвратить распространение пожара от его очага. При тушении из-за большой теплоемкости воды температура в очаге пожара не превышает 110 °С [3]. На выходах из ГС в незадымляемые лестничные клетки выгораживаются тамбур-шлюзы (ТШ) с подпором наружного воздуха. При работе ПДВ через открытый дверной проем ТШ должен циркулировать воздух со скоростью не менее 1,3 м/с, чтобы не пустить дым в незадымляемые лестничные клетки. Выходов из ГС должно быть не менее двух, значит и ТШ может быть два. При нормируемых размерах дверного проема, а также подсосов через неплотности въездных ворот и дверей шахт лифтов для незадымляемости ТШ из ГС достаточно удалять L = 23000 м^3/ч газодымовой смеси. В [1] рекомендуется весовой расход удаляемой газодымовой смеси G = 23000 кг/ч, что при ее плотности ρ = 0,92 кг/м^3, соответствующей температуре в очаге пожара 110 °С [3], дает L = 25000 м^3/ч. Это согласуется с вышеприведенным значением L. При таких значениях L перепад давления на закрытых дверях не превышает 150 Па.

В тоже время, в случае эвакуации из помещения ГС непосредственно наружу дымоудаление из помещения ГС необходимо не для обеспечения эвакуации, а для последующей работы пожарных расчетов и запускаться оно должно не автоматически, а вручную, как это делается при удалении газообразных огнетушащих веществ.

Литература

1. ТКП 45-4.02-273-2012. Противодымная защита зданий и сооружений при пожаре. Системы вентиляции. Строительные нормы и правила проектирования.

2. НПБ 15–2007. Область применения автоматических систем пожарной сигнализации и установок пожаротушения.

3. Хорошко В.В., Глинистый Р.В., Глинистый Р.Р., Шнейдеров Е.Н., Королев А.Г., Король О.М. Эффективность электронных систем пожарной безопасности в зоне горения автомобилей для подземных гаражей-стоянок жилых зданий // Доклады БГУИР. 2020. Т. 18, № 7. С. 63–70.

ПЛАЗМОН-ПОЛЯРИТОННЫЕ ВОЛНЫ В ГЕТЕРОСТРУКТУРЕ «ГРАФЕН/SiO_2»

Д.Ч. Гвоздовский, М.С. Баранова

Поверхностные плазмоны (ПП) представляют собой связанные колебания электромагнитного поля и электронов проводимости, распространяющиеся вдоль

поверхности проводника. Их можно интерпретировать как электромагнитные волны, захваченные поверхностью металла вследствие взаимодействия со свободными электронами. В ходе этого взаимодействия электроны проводимости коллективно реагируют на электромагнитное воздействие, осциллируя в резонансе со световой волной.

Условием существования ПП на плоской границе двух сред является отрицательное значение диэлектрической или магнитной проницаемости [1]. Исследование возможности реализации в планарной периодической структуре на основе графеновых монослоев и диэлектрической подложки поверхностных волн сводится к поиску частотных областей, где действительная часть комплексной диэлектрической проницаемости принимает значения меньше нуля. Использование численного эксперимента позволяет удешевить, упростить и ускорить процесс поиска решения и дать объяснение возникающим низкоразмерным эффектам.

Отклик материала на воздействие электрического поля световой волны полностью определяется его диэлектрической проницаемостью при этой частоте. Диэлектрическая проницаемость материала с любой конечной (не равной нулю) электрической проводимостью является комплексной величиной, то есть ее можно записать как сумму действительной и мнимой частей.

Проведено квантово-механическое моделирование оптических свойств графена, подложки SiO_2 и гетероструктур на их основе. Расчеты проводились на основе теории функционала плотности DFT с использованием методов, учитывающих силы Ван-дер-Ваальса [2]. Отрицательные участки действительной части диэлектрической проницаемости для графена наблюдаются на частотах от 4,05 до 5,28 эВ. Установлено, что контакт графена с диэлектрической подложкой может привести к образованию двумерного электронного газа. Величина заряда, который возникает вследствие контакта, составляет 0,07 е/атом.

Литература

1. Шейнман И.Л. Поверхностные волны на релятивистских плазменных потоках // Журнал технической физики. 2001. № 71 (5). С. 28–34.

2. Parr R.G., Yang W. Density-Functional Theory of Atoms and Molecules. Oxford University Press, 1989.

BYOD И ЗАЩИТА ИНФОРМАЦИИ: ЭКОНОМИЧЕСКИЙ АСПЕКТ

Ю.Ю. Григорьева, Д.К. Дедович, В.В. Бахтизин

Считается [1], что предложенная в 2004–2005 годах выпускником Стэнфорда Рафаэлем Баллагасом (Rafael Ballagas) технология Bring Your Own Device (BYOD, Принеси Свое Собственное Устройство) позволяет сократить затраты на образовательный процесс до 40 %. Но при использовании сотрудниками производственной компании личных гаджетов (например, смартфонов) в служебных целях возрастает нагрузка на службу информзащиты компании, которая должна исключить посещение сотрудниками сайтов с вирусами, шпионскими программами и т. д. Для снижения этой нагрузки имеется практика выдачи компанией своим сотрудникам служебных гаджетов, которые легче контролировать. Для компании это дорого, но служебная информация практически полностью защищена.

Интуитивно понятно, что защищать информацию учреждения образования надо лишь в некоторых редких случаях, поэтому использование личных смартфонов здесь оправдано. Для крупной производственной компании с большим объемом

конфиденциальной служебной дорогостоящей информации более целесообразны служебные гаджеты. Но руководству средней производственной компании неясно, какие гаджеты лучше использовать сотрудникам – личные или служебные.

Эту проблему в докладе предлагается решать путем экономической оценки вариантов выбора гаджетов сотрудников. Приводится алгоритм предлагаемой оценки и способы поиска исходных данных для нее.

Литература

1. Дедович Д.К., Евдокименко М.Н., Микулик Т.Н., Николаенко В.Л., Сечко Г.В. Повышение производственной безопасности учреждений образования и науки за счет использования служебных гаджетов // Межд.науч.-техн. сборник «Теоретическая и прикладная механика». 2019. Вып. 34. С. 291–295.

К ВОПРОСУ ИНТЕРАКТИВНОГО ОБУЧЕНИЯ СТУДЕНТОВ

М.С. Гурский

Краеугольным камнем в университетском образовании должно быть обучение студентов масштабно и перспективно мыслить, осуществляя творческий поиск истины. В последнее время основные методические инновации в образовании связаны с применением интерактивных методов обучения. Сохраняя конечную цель и основное содержание образовательного процесса интерактивное обучение изменяет привычные транслирующие формы на диалоговые, основанные на взаимодействии и взаимопонимании участников. Введение диалога в учебный процесс – это один из важнейших аспектов проблемы активизации познавательной деятельности в процессе обучения. Сегодня лекционный вид занятий чаще всего носит характер монотонного и неэффективного способа обучения, не позволяющего активизировать познавательную деятельность сегодняшнего студента из-за его недостаточной подготовленности к диалоговому общению. К сожалению, современная средняя школа не дает своим выпускникам навыков самообучения, командной работы, а пандемийная ситуация еще более «расхолодила» стремление к профессиональному становлению через самостоятельную работу. А между тем самостоятельная работа студентов способствует не только продвижению их в профессиональном поле, но и вырабатывает навыки самоконтроля, умение планировать и организовывать свою умственную деятельность, возможность активно участвовать в дискуссии. На протяжении последних ряда лет автор делал активные попытки использовать интерактивное обучение при подготовке специалистов по специальности «Электронные системы безопасности», работая с выпускниками при изучении курса «Монтаж, наладка и эксплуатация электронных систем безопасности» при проведении лабораторных работ и практических занятий. К сожалению, общетехническая и специальная подготовка выпускников в большинстве случаев не позволяет организовать коллективное обсуждение предлагаемых технических вопросов, предложить альтернативные варианты решения поставленной задачи. Большинство студентов не в состоянии четко сформулировать свои мысли, опираясь на предыдущие знания, полученные по другим дисциплинам. Как правило, при таком обсуждении доминирует мнение одного, наиболее подготовленного члена бригады, а остальные просто соглашаются с предложенным решением при отсутствии аргументации своей позиции [1].

Литература

1. Гурский М.С. Интерактивные методы обучения в техническом вузе // Высшее техническое образование: проблемы и пути развития: материалы IX Международной научно-методической конф. Минск, 1–2 ноября 2018 г. С. 117–119.

УПРАВЛЕНИЕ МАСКИРУЮЩИМИ СИГНАЛАМИ В СИСТЕМАХ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

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

Обеспечение защиты речевой информации может быть выполнено двумя основными способами. Это повышение звукоизоляции помещений, в которых циркулирует речевая информация в виде акустических волн, для исключения ее распространения за пределы помещения. Второй способ обеспечения защиты речевой информации заключается в создании помех в акустических каналах, по которым может распространяться речевая информация, путем создания маскирующих речевые сигналы акустических помех. Маскирующие сигналы создают в ограждающих элементах конструкций помещений, а также на трубах коммуникаций и в вентиляционных каналах акустические помехи, по уровню превышающие речевой сигнал более чем на 15 дБ. Маскирующие сигналы создают не совсем комфортные условия в помещении, так как присутствующие шумы от маскирующих сигналов ощущаются человеком на слух.

Для создания более комфортных условий работы в защищаемом помещении предлагается включать маскирующие сигналы в те промежутки времени, когда в помещении присутствует речевая информация в виде акустических волн. Однако, на ряду с акустическими сигналами, принадлежащими речевой информации, в помещении присутствуют акустические сигналы, сопровождающие нахождение людей в защищаемом помещении. Это хлопки, разного рода ударные волны, шорох от передвижения и другие. Поэтому чтобы управлять маскирующими сигналами в зависимости от акустической речевой информации необходимо выделить акустическую речевую информации от других акустических сигналов, присутствующих в помещении.

В результате проведенных исследований установлено, что допустимое время, за которое необходимо принять решение, являются ли акустические сигналы в помещении речевыми, составляет не более 100 мс. Это обусловлено тем, что среднее время звучания одной фонемы составляет порядка 30–70 мс. С учетом того, что можно допустить прослушивание двух фонем без потери конфиденциальности речевой информации, то время принятия решения о том, является ли звуковой сигнал не речевым сигналом, составляет 100 мс. Таким образом, все звуковые сигналы, тип которых за время 0,1 с не определен как не речевые, будут отнесены к сигналам, по которым будет включаться маскирующие сигналы.

Итак, как показали экспериментальные исследования акустических шумов в защищаемом помещении, многие виды шумов имеют кратковременной импульсный характер с затуханием акустических шумов, обусловленным реверберацией звука в помещении. Длительность таких процессов составляет 10–20 мс с уменьшением амплитуды от максимального значения на 8–10 дБ, а с затуханием на величину более 20 дБ происходит за время порядка 60–80 мс.

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ КОМБИНИРОВАННЫМИ МАСКИРУЮЩИМИ СИГНАЛАМИ

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

Широкое распространение для защиты речевой информации получили маскирующие сигналы в виде «белого» шума. В литературных источниках рассматриваются и другие виды маскирующих сигналов: «розовый» шум и речеподобные сигналы, представляющие собой сумму трех источников речевых сигналов (речевой хор). Впервые о комбинированных маскирующих речь сигналах, состоящих из суммы «белого» шума и речеподобных сигналов, говорится в работе [1]. Комбинированные маскирующие сигналы предлагалось использовать для защиты речевой информации с высокими требованиями по показателю низкой разборчивости речи. Комбинированные маскирующие сигналы включают «белый» шум и речеподобные сигналы. Речеподобные сигналы по своим формальным свойствам близки к слитной речи, однако имеются временные участки, где речеподобный сигнал отсутствует, как и в естественной речи, поэтому эти промежутки необходимо заполнять шумовым сигналом чтобы не было пропусков и не попал информационный сигнал на пустые не заполненные шумом участки.

Разборчивость речи, маскированной комбинированными сигналами, оценить аналитически весьма сложно, так как соотношения речевой сигнал – комбинированная помеха со временем будет изменяться в небольших пределах и необходимо при этом учитывать вероятности совпадения формант речевого сигнала и формант речеподобной помехи. Поэтому наиболее приемлемым решением является использование при расчетах метода предельных состояний и проведение экспериментальных исследований.

Для проведения экспериментальных исследований были отобраны фонетически сбалансированные тексты, дикторы и аудиторы с высокими показателями слуховой чувствительности в соответствии с методикой [2]. Экспериментальные исследования разборчивости речи, маскируемой только «белым» шумом дали следующие результаты: при соотношении сигнал шум –24 дБ разборчивость речи составила менее 1 %. Разборчивость речи маскируемой комбинированными сигналами, включающими «белый» шум и речеподобные сигналы, составила менее 1 % для соотношения сигнал/комбинированный маскирующий сигнал –14 дБ. Результаты экспериментальных исследований в полной степени коррелируют с результатами, полученными S.J. Bradley для английского языка.

Литература

1. Устройство защиты речевой информации от утечки по вибрационным и акустическим каналам: полезн. модель пат. BY 3053 / В.И. Воробьев, А.Г. Давыдов, Г.В. Давыдов, А.И. Ивонин, Д.В. Лещенко, Б.М. Лобанов, Л.М. Лыньков, В.А. Попов, А.В. Потапович. – Опубл. 30.10.2006.

2. Seitkulov Y.N., Boranbayev S.N., Yergaliyeva B.B., Davydau H.V., Patapovich A.V. Method for speech intelligibility assessmentwith combined masking signals // Journal of Theoretical and Applied Information Technology. 2020. Vol. 98, No 08. P. 1173–1186.

МОДЕЛИРОВАНИЕ ШАГОВЫХ ПЕРЕМЕЩЕНИЙ СИНХРОННЫХ ДВИГАТЕЛЕЙ С ОДНОПОЛЯРНЫМИ И ДВУХПОЛЯРНЫМИ МАГНИТНЫМИ ДОРОЖКАМИ

И.В. Дайняк

В докладе рассматриваются вопросы построения линейных синхронных двигателей с магнитной дорожкой на статоре, которые могут использоваться как элементная база средств защиты информации. Наиболее известными типами магнитных дорожек статора являются однополярные с расстоянием между полюсами, двухполярные с расстоянием между полюсами и двухполярные без зазоров между полюсами [1]. В работе получены аналитические выражения тяговых сил и графики положения точек позиционирования на одном периоде для указанных типов магнитных дорожек при перемещении в режиме полного шага и при дроблении шага перемещения, которые показывают, что при малых шагах перемещения (малом шаге дискретности координатной системы) величина шага может быть нестабильной. В результате двухполярные двигатели с магнитной дорожкой с интервалом между полюсами непригодны для построения прецизионных систем перемещения. Для остальных типов магнитных дорожек в работе предложены расчетные модели тяговых сил электромагнитных фазных модулей, получены годографы результирующей тяговой силы и распределение точек позиционирования на одном периоде.

Для получения равномерного дробления полного шага перемещения необходимо неравномерно дробить амплитуду намагничивающей силы фаз электромагнитного фазного модуля. В этом случае при проектировании реальных приводов на каждом периоде магнитной дорожки в пределах рабочего поля перемещения приходится учитывать ряд факторов, влияющих на координаты размещения точек позиционирования. При малых шагах перемещения эти параметры являются индивидуальными для каждой магнитной дорожки и каждого фазного модуля. Аналитически рассчитать такие системы практически невозможно, поэтому наладку таких приводов производят с помощью специально разработанных методик с использованием прецизионных средств измерений [2].

Литература

1. Жарский В.В., Карпович С.Е., Дайняк И.В. Системы многокоординатных перемещений и исполнительные механизмы для прецизионного технологического оборудования. Минск, 2013. 208 с.

2. Дайняк И.В. Алгоритмические методы повышения точности позиционирования прецизионных систем перемещений // Математические методы в технике и технологиях: сб. тр. Междунар. науч. конф. СПб., 2017. Т. 12, ч. 2. С. 13–18.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ БЫСТРОГО ПРЕОБРАЗОВАНИЯ УОЛША

Т.Н. Дворникова, Н.М. Семитко

В настоящее время идет бурное развитие средств обработки информации. Функции Уолша находят широкое применение в областях передачи и обработки цифровой информации, области машинного обучения. Они используются в беспроводной системе связи с LDPC OFDM кодированием, а в области машинного обучения для road/path трекинга, сопоставления образов изображений с базой, синтеза

текстур в дополненой реальности. Несмотря на многочисленные работы математиков и работы, в которых рассматриваются вопросы об инженерном использовании функций Уолша, для более широкого их применения необходимы дополнительные исследования, направленные на изучение свойств этих функций.

Функции Уолша являются кусочнопостоянными функциями с нормированным интервалом определения [0, 1) или [–0,5, +0,5) и интервалом изменения аргумента, который зависит от порядка системы функций Уолша и равен $\frac{1}{2^n}$, где n = 1, 2,… Преобразование Уолша осуществляется с помощью быстрых алгоритмов. К настоящему времени имеется определенное количество таких алгоритмов, которые получены в основном используя факторизации матриц Уолша в различных упорядочениях. Все алгоритмы не равноценны, кроме того, выделяются так называемые «замечательные» алгоритмы быстрого преобразования Уолша.

В докладе рассматривается разработка программной реализации извлечения алгоритмов быстрого преобразования в системе упорядочений Уолша – Адамара, Уолша – Качмажа и Уолша – Пэли, которые являются симметричными и относятся к «замечательным». Для каждого алгоритма реализовано вычисление выходного вектора и построения графа. Программный код представлен в виде высокоуровневой библиотеки, написанной на языке C++. Данная форма позволяет использовать программную реализацию как самостоятельное консольное приложение для проверки правильности вычислений, а также интегрировать библиотеки в любое программное обеспечение, написанное на языке C++, или интерпретировать код в более низкоуровневый, что позволит использовать его в ПЛИС.

Полученные библиотеки могут быть использованы для извлечения алгоритмов быстрого преобразования Уолша в различных системах упорядочений [1, 2].

Литература

1. Голубов Б.И., Ефимов А.В., Скворцов В.А. Ряды и преобразования Уолша: теория и применения. М.: Наука, 1987. 344 с.

2. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах. М.: Советское радио, 1975. 208 с.

АЛГОРИТМ ДИАГНОСТИКИ ЭЛЕМЕНТНОЙ БАЗЫ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Денис, А.В. Гринкевич

Диагностика электрической схемы представляет из себя процесс определения неисправных компонентов, которые вызывают сбои в работе цепи. Затянувшийся поиск неисправности приводит к простою.

С учетом разнообразия конструкторских исполнений технических средств защиты информации разработка эффективных алгоритмов диагностики является актуальной задачей.

В работе предложен алгоритм, который состоит из ряда последовательных действий, являющийся решением указанной проблемы.

В первую очередь внимание при диагностике уделяется визуальному осмотру. Проверяется наличие компонентов, имеющих видимые повреждения, разрывов проводников, признаков повреждения подложки.

Если электронное устройство не включается, то проводится электрическое тестирование с целью выявления коротких замыканий в цепи, обрывов цепи, измерения

электрических параметров элементов. При наличии образцовой печатной платы необходимо провести сравнение с диагностируемой. Следующим шагом производится проверка параметров всех дискретных элементов и микросборок на соответствие заданным.

Если электронное устройство включается, но работает некорректно, то следует проверить потребление тока и наличие теплонагруженных областей на печатной плате. Также проводится измерение напряжения в контрольных точках, на трансформаторных обмотках, преобразователях, известных микросхемных сборках. Производится проверка тактовых сигналов, интерфейсов человек-машина. Далее следует функциональное тестирование цифровых и аналоговых компонентов. Проводится запуск пользовательских тестов, которые заключаются в проверке срабатывания реле, определения работоспособности цифро-аналоговых и аналого-цифровых преобразователей и т. д. Замена компонентов проводится по мере необходимости. Такой алгоритм позволяет значительно сократить время, затрачиваемое на восстановление элементной базы технических средств защиты информации [1].

Литература

1. ГОСТ 18322-2016 «Система технического обслуживания и ремонта техники» – 01.09.2017 – Межгосударственный совет по стандартизации, метрологии и сертификации, 2017.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ПРИ ОБНАРУЖЕНИИ И ОБРАБОТКЕ СИГНАЛОВ В ЗАЩИЩЕННЫХ КАНАЛАХ СВЯЗИ

А.А. Добрынин, Т.Н. Дворникова

Нейронные сети являются мощным инструментом, применимым для решения широкого спектра задач и известным еще с середины прошлого века, но только начавшим стремительное распространение в начале 21-го. Возможность обучения демонстрирует одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. В процессе обучения нейронная сеть способна самостоятельно выявлять сложные зависимости между входными и выходными данными, а также выполнять функцию кластерного анализа. Отсутствие прямой корреляции и детерминированного алгоритма работы позволяют значительно повысить устойчивость систем перед потенциальными попытками взлома.

В работе рассмотрена нейронная сеть представленная единичным перцептроном, принимающим бинарный вектор входных признаков. Данные обучающей и тестовой выборок сформированы с различными коэффициентами зашумленности. В случае успешного обучения, при неполных и/или частично искаженных входных данных, нейронная сеть показывает возможность получить верный результат на основании данных, которые присутствовали в обучающей выборке. Расширение нейронной сети показывает увеличение вероятности правильного результата.

Базируясь на виде передаваемой в защищенном канале связи информации, возможно применять различные архитектуры нейронных сетей, каждая из которых обладает своими специфическими свойствами. Способность к самоанализу и стойкость к искажению данных, при интегрировании в существующие системы, дают конкуренцию классическим решениям и способствуют дальнейшим исследованиям в этой области [1, 2].

Литература

1. Емельянова Ю.Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. 2011. Т. 2, № 3. С. 3–15.

2. Гонтаренко Б.В. Проблемы реализации искусственных нейронных сетей на FPGA // Информатика и компьютерные технологии-2011. 2011. С. 15–18.

ОПТИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ КРЕМНИЕВЫХ СВЕТОДИОДОВ, ИЗЛУЧАЮЩАЯ СВЕТ В ОПРЕДЕЛЕННОМ НАПРАВЛЕНИИ

А.В. Долбик, А.А. Лешок

В государственных структурах, банковской сфере, медицинской отрасли, в офисах – защита визуальной информации является неотъемлемой частью обеспечения безопасности. Устройства отображения информации, излучающие свет только в вертикальном направлении по отношению к поверхности экрана, могут использоваться в целях защиты информации, отображаемой на экране.

Нами разработана оптическая система, состоящая из мембраны макропористого кремния и источника света, которая может обеспечить распространение света только в вертикальном направлении, относительно плоскости мембраны.

Экспериментальная структура источника света была создана осаждением алюминиево-кремниевой нанокомпозитной пленки толщиной 0,1 мкм магнетронным распылением с последующим осаждением чистой алюминиевой пленки толщиной 1 мкм на кремниевые подложки *n*-типа. Осажденные пленки были подвергнуты анодной обработке в 20 % водном растворе ортофосфорной кислоты через предварительно сформированную фоторезистивную маску на их поверхностях, что привело к формированию композитной пленки наноструктурированного кремния встроенного в матрицу оксида алюминия. Непроанодированные области, защищенные фоторезистивной маской, образуют металлические электроды между анодированными областями, формируя контакты Шоттки, которые могут испускать свет в режиме лавинного пробоя. Также были сформированы сквозные кремниевые микроканальные пластины (мембраны) толщиной 100–150 мкм с диаметром пор 5–6 мкм по маршруту, описываемому в [1], которые использовались для направления луча света.

Источником света являлся наноструктурированный кремниевый светодиод, технология его изготовления описана выше, либо лазерный луч с длиной волны в видимой области спектра (532 нм). Кремниевый фотодиод использовался для регистрации света, проходящего через мембрану. Индикатриса рассеивания светового луча, прошедшего через микроканальную кремниевую пластину, показала, что излучение распространяется только в вертикальном направлении относительно плоскости мембраны.

Литература

1. Lazarouk S.K., Leshok A.A., Kozlova T.A., Dolbik A.V., L.D. Vi, Ilkov V.K., Labunov V.A. 3D Silicon Photonic Structures Based on Avalanche LED with Interconnections through Optical Interposer // International Journal of Nanoscience. 2019. Vol. 18. P. 1940091 (1–5).

ОСНОВНЫЕ ПРИНЦИПЫ И НАПРАВЛЕНИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

М.Н. Дудак

Развитие информационной инфраструктуры и высоких технологий является характерной чертой современного социума. Сфера защиты информации становится незаменимой частью экономической политики страны. Она сказывается на состоянии экономической, политической, оборонной и других составляющих безопасности Республики Беларусь. Угроза информационной безопасности развивается одновременно с процессами информатизации. Требования к специалистам в области защиты информации высоки, сегодня требуется персонал нового поколения, умеющий быстро адаптироваться к постоянно модифицирующимся угрозам информационной безопасности, владеющий высочайшей степенью профессиональной компетентности. Прогресс системы подготовки специалистов, функционирующих в области защиты информации, относится к первостепенным задачам национальной политики.

Существуют базисные принципы обеспечения достойного уровня подготовки профессионалов по части защиты информации, которые учитывают активное взаимодействие с работодателями сферы защиты информации, ориентацию образовательного процесса на постоянные изменения угроз, синхронизацию с потребностями региона, создание инновационной образовательной сферы вуза. В качестве перспективных путей увеличения эффективности образовательного процесса предложены современные подходы – компетентностный и инновационный. Компетентностный подход увеличивает практикоориентированность образования, подчеркивает важность опыта, умений практически реализовать знания, описывает в качестве итога формирование компетенций. Развитие научно-исследовательской и инновационной деятельности рассматривается как основа фундаментализации образования, как неотъемлемая часть подготовки кадров, основа истинного участия университета в процессах модернизации экономики. Сформулированы педагогические условия, исполнение которых обеспечит высококачественную подготовку профессионалов по части защиты информации. Приоритетным курсом увеличения качества подготовки является организация научно-исследовательской и инновационной деятельности в области защиты информации. Реализация предложенных педагогических условий способствует обеспечению высокого качества подготовки специалистов в области защиты информации, формированию профессиональной компетентности и мотивационно-ценностной включенности в инновационную деятельность [1].

Литература

1. Агибова И.М., Кистерева С.Н. Профессиональная подготовка специалистов в области информационной безопасности на основе реализации компетентностного подхода // Наука. Инновации. Технологии. 2011. № 1. С. 3–9.

ФОРМИРОВАНИЕ НАНОСТРУКТУРИРОВАННЫХ АНТИОТРАЖАЮЩИХ ПОКРЫТИЙ ДЛЯ ОПТИЧЕСКИХ УСТРОЙСТВ

В.В. Дудич, Д.А. Сасинович, К.А. Антипов, Н.Н. Стешиц

Антиотражающие покрытия представляют интерес для разработки и создания оптоэлектронных и дисплейных устройств. Нами предложена методика формирования

наноструктурированных пористых антиотражающих покрытий на титане, которая основана на напылении на поверхность обрабатываемой детали композитной пленки алюминий-титан с последующим анодным окислением данной пленки и селективным вытравливанием оксида алюминия [1]. Полученное описанным методом покрытие имеет коэффициент зеркального отражения 0,1–0,33 % в пределах спектра излучения видимого диапазона. Полученные покрытия обладают высокой термической и механической устойчивостью. Описанная методика может быть использована для создания антиотражающих покрытий с применением других вентильных металлов. Разработанный метод может быть использован для формирования антиотражающих покрытий титановых корпусов, используемых в системах спутниковой фотосъемки.

Литература

1. Lazarouk S.K., Sasinovich D.A., Borisenko V.E. Nanoporous oxides of refractory metals: fabrication and properties // Phys. Stat. Sol. (c). 2008. No. 5. P. 3690.

ОБ УГРОЗАХ ПРИМЕНЕНИЯ И ОЦЕНКЕ ДОСТОВЕРНОСТИ МЕТОДОВ ВЫЯВЛЕНИЯ КОНТРАФАКТНЫХ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ В ТЕХНИЧЕСКИХ СРЕДСТВАХ

А.П. Дураковский, Л.Н. Кессаринский, Е.А. Симахин, А.О. Ширин

Очевидной угрозой потери устойчивости технологических процессов является использование контрафактной элементной базы в условиях наблюдаемого общего увеличения доли контрафактной продукции, в том числе и в изделиях электронной компонентной базы (ЭКБ). Наиболее распространенными видами продукции в почтовых отправлениях были электронное оборудование (32 %) и лекарства (16 %) [1]. Нельзя отрицать, что это проблема монументального масштаба, и она только усугубляется. Текущие оценки ежегодных потерь для электронной промышленности из-за контрафактных компонентов превышают 5 миллиардов долларов. С такими высокими оценками неудивительно, что криминальные предприятия становятся все более изощренными в своих попытках нажиться на контрафактных деталях [2]. Угроза применения контрафактных изделий ЭКБ распространяется практически на все виды техники и может приводить к опасности для жизни и здоровья человека, существенному ущербу для промышленности. Предлагается системный подход применения комплекса методов выявления уязвимостей и оценки достоверности результатов испытаний электронной компонентной базы в аппаратном обеспечении средств защиты информации (СЗИ). Важно, чтобы выявление контрафакта в ЭКБ осуществлялось не только с позиций охраны объектов интеллектуальной собственности, но и стало первым шагом в ходе сертификационных (а также постсертификационных) испытаний по требованиям безопасности информации аппаратных СЗИ. Для испытательных лабораторий такая постановка задачи связана с организацией достаточно нового вида деятельности в условиях недостаточности соответствующей нормативной базы. В работе представлены подходы и типовые примеры выявленных контрафактных и подозрительных образцов ЭКБ в ходе идентификации: неоднородность выборки образцов для испытаний (по размеру кристалла, по конструкции корпуса и размерам кристалла, по контролю массы образцов одной партии), хотя внешняя маркировка на корпусе соответствует описанию на всех образцах выборки. Разработан подход к количественной оценке достоверности результата испытаний комплексом методов. Разработана матрица эффективности методов – эволюционирующая структура на основе экспериментальных результатов,

постоянного мониторинга публикаций, появления новых методов и признаков. Обзор зарубежных нормативных документов, определяющих методы и средства выявления контрафакта в ЭКБ, может быть использован в качестве начальной основы для формирования отечественной нормативной базы [3].

Литература

1. European Commission Taxation and Customs Union, Report on EU customs enforcement of intellectual property rights Results at the EU border 2015. P. 7.

2. Билл Кардосо. 10 способов сделать рентгеновские снимки, которые помогут выявить контрафактные детали // Электронное издание: «Evertiq New Media AB». 2017.

3. Дураковский А.П., Кессаринский Л.Н., Ширин А.О. Развитие терминологии нормативной базы испытаний на выявление признаков контрафакта в изделиях электронной компонентной базы аппаратуры объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2020. Т. 27, № 1. С. 19–27.

ПРОТОКОЛ ESP-NOW В СИСТЕМАХ БЕСПРОВОДНОГО ПИТАНИЯ

А.П. Жмойдяк, А.И. Янович

В системах беспроводного питания необходимо наличие двухсторонней связи между приемной и передающей стороной для контроля параметров передачи и оперативного изменения режимов работы [1]. При этом довольно часто помимо передачи энергии требуется осуществлять обмен информацией с питаемым устройством.

Такую связь можно реализовывать на беспроводных модулях ESP32 от компании Espressif Systems, представляющих собой SoC с интегрированным Wi-Fi и Bluetooth контроллерами. Модуль также имеет поддержку множества проводных интерфейсов: Ethernet, UART, CAN и др. [2].

В случае если в системе беспроводного питания не требуется передача больших объемов данных для связи между приемником и передатчиком энергии можно использовать упрощенный протокол связи ESP-NOW. При использовании данного протокола можно осуществлять передачу информации объемами до 250 байт между модулями ESP. Для осуществления передачи требуется только начальное сопряжение на основе MAC-адресов после чего устанавливается неразрывное соединение [3].

При передаче информации возможно использование шифрования по технологии CCMP, при этом используется встроенный в модуль криптографический ускоритель. Модуль поддерживает основной мастер-ключ (PMK) и до шести локальных мастер-ключей (LMK). PMK спользуется для шифрования LMK алгоритмом AES-128, а в свою очередь LMK используется уже для шифрования передаваемой информации по технологии CCMP.

Литература

1. Отчет МСЭ-R SM.2303-1. Беспроводная передача энергии с использованием технологий, не предусматривающих передачу с помощью радиочастотного луча. Женева, Швейцария, 2015. 78 с.

2. ESP32 Series Datasheet [Электронный ресурс]. – Режим доступа: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf. – Дата доступа: 04.05.2021.

3. ESP-NOW User Guide [Электронный ресурс]. – Режим доступа: https://www.espressif.com/sites/default/files/documentation/esp-now_user_guide_en.pdf. – Дата доступа: 04.05.2021.

АЛГОРИТМИЧЕСКАЯ ПРОБЛЕМА ВЫДЕЛЕНИЯ КОНТУРОВ ОБЪЕКТОВ НА РАСТРОВЫХ ИЗОБРАЖЕНИЯХ

Д.В. Заерко, В.А. Липницкий

Алгоритмы выделения контуров основываются на разрывности яркости сигнала [1]. Обработка растровых изображения $f(x,y)$ с помощью пространственной фильтрации – один из популярных способов. Пространственная фильтрация – это процесс оперирования с маской – квадратной матрицей M, состоящей из компонентов $M(x,y)$ или коэффициентов над соответствующей группой пикселей растрового изображения $f(x,y)$.

Процесс фильтрации представляет собой перемещение маски фильтра от пикселя к пикселю изображения $f(x,y)$. Для каждого из пикселей определяется отклик $R(x,y)$ фильтра с учетом маски фильтра. Полученный отклик в точке (x,y) характеризует перепады яркости. При их обнаружении используются дискретные аналоги производных первого и второго порядка. Вычисление первой производной цифрового изображения основано на различных дискретных приближениях двумерного градиента [2]. Направление контура в точке (x,y) всегда перпендикулярно направлению вектора градиента в ней. Это общие описание этапов определения контуров объектов. Так же, для решения этой задачи можно использовать операторы: Робертса, Привитта, Собеля, Шарра [1]. Принцип работы прост: применение матрицы специального вида (маски) к исходному изображению. При использовании оценки яркости в точке с учетом точек в ее окрестности возникает вопрос: как ведет себя оператор для граничных точек изображения? Упомянутые операторы используют схему двумерной свертки, при которой граничные пиксели не обрабатываются из-за выхода алгоритмов за пределы границ исходного изображения. Алгоритм с пиксельным дополнением должен удовлетворять жестким требованиям: не уменьшать скорость обработки изображения, не приводить к ложным и скачкообразным изменениям крутизны яркости, учитывать особенности приближенного вычисления градиента, быть универсальным для целого класса алгоритмов. Безусловно, такой дополненный алгоритм был бы полезен при распознавании объектов на растровых изображениях и нашел бы широкое применение целых классов алгоритмов. В докладе обсуждается проблема построения такого оптимального алгоритма.

Литература

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М: Техносфера, 2005. 1007 с.

2. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т. 1. М.: Физматлит, 2003. 680 с.

АЛГОРИТМ ПОВЫШЕНИЯ РАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ДОМЕННОЙ ИНТЕРПОЛЯЦИИ

А.В. Захаренко

При интерпретации снимков возникают проблемы, связанные с подавлением высокочастотных составляющих на изображении, которые могут привести к потере данных и сложности идентификации объектов. Улучшение параметров изображений было бы возможным путем изготовления матриц с большим числом фотоприемных элементов и создания на их основе новых оптоэлектронных приборов. Однако

подобный подход на сегодняшний день является плохо реализуемым из-за увеличения габаритов, веса и стоимости изделия. В связи с этим основным направлением обработки изображений являются цифровые методы, благодаря развитию которых задача повышения разрешения изображений стала крайне актуальной.

Алгоритм повышения разрешения изображений на основе доменной интерполяции может использоваться для повышения разрешения изображений в $S = 2^N$ раз, где S – коэффициент масштабирования, а N – целое положительное число. При этом количество изображений низкого разрешения совпадает с коэффициентом масштабирования, что устанавливает ограничения на число используемых для интерполяции изображений. Исходными данными для формирования изображения высокого разрешения является серия изображений низкого разрешения, сдвинутых относительно друг друга на 1 пиксель. В ходе работы алгоритм формирует одно изображение высокого разрешения [1].

Оценка эффективности алгоритма на основе значения среднеквадратической ошибки (MSE) показала, что изображения, сформированные алгоритмом повышения разрешения изображений на основе доменной интерполяции, имеют в среднем в 4 раза меньшее значение MSE, чем изображения, сформированные алгоритмами билинейной и бикубической интерполяции.

Литература

1. Богуш, В.А. Методика углового оптического сканирования плоских поверхностей для систем технического зрения // Доклады БГУИР. 2016. № 2 (96). С. 123–126.

КОНТРОЛЬ ЭФФЕКТИВНОСТИ КОДИРОВАНИЯ ИНТЕГРАЛЬНЫХ СХЕМ

Л.А. Золоторевич, В.А. Ильинков

В последние годы для защиты проектов интегральных схем применяются методы и средства аппаратного кодирования комбинационных блоков интегральных схем (ИС) [1]. Для совершенствования подобной защиты проектов необходимы средства контроля эффективности применяемых методов кодирования. Предлагается метод взлома кода при наличии информации о структуре закодированного объекта и возможности доступа к физической модели. Задача решается на основе описания закодированной структуры в виде КНФ функции разрешения, решения задачи выполнимости (SAT) и физического моделирования объекта.

Исходными данными для декодирования структуры цифрового устройства является структурная реализация закодированной схемы, которая может быть получена методом обратного проектирования (проектирования по прототипу), а также активированный физический образец интегральной схемы, в защищенную от несанкционированного доступа память которой заказчик загрузил правильное значение ключа. Этот образец может использоваться в виде модели черного ящика Y = eval (X). Основная идея SAT – атаки взлома ключа состоит в том, чтобы определить правильный ключ, не прибегая к исследованиям на большом интервале входно-выходных переменных. Два ключа $\vec{K}_1$ и $\vec{K}_2$ являются эквивалентными ($\vec{K}_1 = \vec{K}_2$), тогда и только тогда, когда для входного значения $\vec{X}_i$ закодированная схема выдает одинаковое выходное значение $\vec{Y}_i$ для ключей $\vec{K}_1$ и $\vec{K}_2$. Для определения правильного ключа итеративно исключаются ключи из класса эквивалентности, которые выдают неправильные значения выходов, в крайней мере для одного входного шаблона. Класс эквивалентных ключей определяется на некотором входно-выходном векторе

решением выполнимости функции $Cir_b(\vec{X}_j, \vec{K}, \vec{Y}_j)$ полным методом. Входной вектор $\vec{X}^d$ называется различающим, если реакция схемы при использовании ключа $\vec{K}_1$ равна $\vec{Y}_1^d$ и отличается от реакции $\vec{Y}_2^d$ при использовании ключа $\vec{K}_2$. При наличии различающего набора можно проверить реакцию активированной схемы для входа $\vec{X}^d$ и использовать ее, чтобы исключить ключ $\vec{K}_1$ или $\vec{K}_2$ как не входящий в класс эквивалентности правильных ключей.

Литература

1. Золоторевич Л.А. Аппаратная защита цифровых устройств // Вестник Томского государственного университета. Управление, вычислительная техника, информатика. 2020. № 50. С. 69–78. DOI: 10.17223/19988605/50/9.

МЕТОДЫ ОЦЕНКИ СОСТОЯНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ

Е.П. Зуенок

На сегодняшний день все большую ценность и значимость приобретают информационные ресурсы. И чем более они ценны, тем важнее ее безопасность. А значит безопасность ее носителей и каналов передачи. Потеря данных большой компании может принести ей огромные убытки. Следовательно, одной из первых ее задач – обеспечить защиту своих серверов и рабочих станций. Для оценки антивирусной защиты программы следует учитывать следующие критерии: качество эвристического анализа, скорость реакции обнаружения вирусов, качество сигнатурного анализа, качество поведенческого блокиратора, способность к лечению активных заражений, способность к выявлению активных руткитов, качество самозащиты, возможность поддержки упаковщиков, частота ложных срабатываний. Однако кроме этого имеют значение количество необходимых для корректной работы программы ресурсов, устойчивость к сбоям, количество ложных срабатываний, стоимость программы и прочее. Тестирование и анализ существующих антивирусных программ проводился неоднократно. В докладе рассматривается метод оценки антивирусных программ, учитывающий технические характеристики программ. В 2016 г. компанией Microsoft была проанализирована эффективность антивирусов с учетом распространенности угроз. Этот метод позволяет учитывать в большей степени те угрозы, которые чаще встречаются в различных регионах. В 2018 г. был проведен сравнительный анализ антивирусных программ на основе значений показателей защиты от вирусов. Этот метод позволяет глубже разобрать возможности антивирусных программ. При этом среднестатистический пользователь, не имеющий глубоких знаний в этой области, как правило, оценивает программу по тому, насколько ей удобно и просто пользоваться, не создает ли она неудобств для работы с компьютером. Если взять выборку по рейтингу всех этих анализов, то результаты будут отличаться. У каждой программы свои минусы и свои плюсы. И при этом ни одна из них не может обеспечить абсолютную защиту. И наиболее эффективным ее вариантом будет комплексная защита, при создании которой учитываются все особенности программ и условия их работы. Кроме того, для поддержания уровня защищенности необходимы постоянный мониторинг и развитие действующей системы защиты. Рассмотренный метод позволяет найти наиболее оптимальное решение защиты от вредоносных программ, учитывая возможности рабочей техники и запросы пользователей [1, 2].

Литература

1. Сравнительный анализ антивирусов. Сравнение антивирусов по эффективности защиты от новейших вредоносных программ Сравнение двух антивирусных программ по информатике [Электронный ресурс] – Режим доступа: https://polarize.ru/game/sravnitelnyi-analiz-antivirusov-sravnenie-antivirusov-po. – Дата доступа: 04.05.2021.

2. Эффективность антивирусов с учетом распространения угроз [Электронный ресурс] – Режим доступа: https://www.comss.ru/page.php?id=3072. – Дата доступа: 04.05.2021.

СРАВНИТЕЛЬНАЯ ОЦЕНКА СИММЕТРИЧНОГО И АСИММЕТРИЧНОГО ШИФРОВАНИЯ

А.А. Иванов

Современные методы шифрования представляют собой математические преобразования (алгоритмы), в которых сообщения рассматриваются как числа или алгебраические элементы в некотором пространстве. В криптографии определены некоторые методы, которые можно разделить в зависимости от количества ключей, которые используются в соответствующих алгоритмах: одноключевые, двухключевые и бесключевые. Алгоритмы шифрования делятся на два больши класса: симметричные и асимметричные. Симметричные алгоритмы шифрования используют один и тот же ключ для зашифровывания информации и для ее расшифровывания, а асимметричные алгоритмы используют два ключа – один для зашифровывания, другой для расшифровывания. Такая разница хоть и кажется простой, но она представляет большие функциональные различия между двумя формами шифрования и способами их использования. Основными различиями являются: длина ключей (128 бит в симметричном шифровании и 2048 бит – в асимметричном) и распределение ключей (в симметричном шифровании ключ передается всем, кому потребуется доступ, что создает определенные риски, а в асимметричном – открытый ключ, который могут знать все участники, используется для шифрования, а приватный, который знает только получатель, – для дешифрования).

В результате подробного изучения различных методов шифрования, а также проведенного сравнительного анализа было установлено, что симметричные методы шифрования отличаются высокой скоростью обработки данных и незначительным временем для генерации ключей, но при этом для несанкционированного дешифрования данных, зашифрованных симметричным методом шифрования, например, AES, требуется около 2^{256} операций. В то время как для данных, зашифрованных асимметричным методом шифрования, например, RSA, требуется 2^{1024} операций, что объясняет его использование для защиты программного обеспечения, цифровой подписи, аутентификации пользователей, в протоколах SSL, IPsec и др. [1–3].

Литература

1. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.

3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.

ИСПОЛЬЗОВАНИЕ «СОЛИ» ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ХЕШИРОВАНИЯ

И.Ю. Изгачёв, М.А. Аниховский, В.А. Ковалёв, А.В. Галковский

В настоящее время хеширование используется для хранения паролей пользователей веб-приложений. Тем не менее регулярно конфиденциальные данные «утекают» в сеть в результате взломов аккаунтов пользователей веб-сервисов [1].

Хеширование – это процесс трансформации произвольного массива данных в строку фиксированной длины. Этот процесс необратим, т.е. невозможно восстановить данные по хешу. Это свойство хешей позволяет использовать их для хранения паролей, ведь захешированное значение невозможно получить, однако возможно проверить его на соответствие с введенной строкой. Однако, злоумышленник может подобрать необходимый для авторизации хеш используя таблицы поиска – таблицы со списком наиболее распространенных паролей и соответствующими хешами. Также используются радужные таблицы [2], которые используют дополнительную память для более эффективного поиска необходимого пароля. Атаки с использованием подобных таблиц эффективны по причине того, что процесс хеширования для каждого пароля происходит одинаково, т. е. значения хеша для двух идентичных паролей будут совпадать. Для рандомизации значений хеша необходимо перед хешированием добавить к паролю строку из случайных символов («соль»).

Использование «соли» делает атаку с помощью таблиц поиска и радужных таблиц неосуществимой, однако для этого «соль» должна быть уникальной для каждого пароля [3]. Этого можно добиться формированием «соли» с помощью криптографически безопасного генератора псевдослучайных чисел, использующего, например, текущее системное время [4]. Также в качестве дополнительной меры безопасности можно использовать секретный ключ, добавляемый к итоговому хешу. Такой ключ необходимо сохранять на отдельном защищенном сервере.

Литература

1. CSO Online [Электронный ресурс]. – Режим доступа: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. – Дата доступа: 12.04.2021

2. Dafydd Stuttard, Marcus Pinto, «The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws»

3. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse. The Mobile Application Hacker’s Handbook.

4. David Litchfield, Chris Anley, John Heasman, Bill Grindlay. The Database Hacker’s Handbook: Defending Database Servers.

РИСКИ ИСПОЛЬЗОВАНИЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОКТОРИНГА

А.М. Кадан, Т.Е. Козляк

Системами прокторинга становятся популярны в учебных заведениях. Так, в условиях пандемии они позволяют проводить экзамены в удаленной форме. В такой системе, как правило, требуется первоначально пройти проверку личности и предоставить удаленный доступ к своему компьютеру. Данные, собранные во время экзамена в режиме реального времени, отправляются на удаленный сервер, который, помимо хранения информации, обрабатывает ее с помощью алгоритмов

искусственного интеллекта (AI) с целью поиска нарушений. Как и все системы, предполагающие использование AI, такая форма организации учебного процесса подвержена существенным рискам. Во-первых, это академические риски – применение прокторинга вынуждает изменять процедуры проведения экзаменов, усложнять их техническое оснащение и предполагает упрощение заданий экзамена, вызванное сокращением времени на обдумывание ответов и соблюдением ограничительных мер. Также не все экзамены возможно осуществлять в дистанционном формате, особенно если учитывать неподготовленность преподавателей к внедрению дистанционных форм учебного процесса. Во-вторых, это финансовые риски для бюджета учебных заведений, связанные с использованием коммерческих систем, поскольку рынок бесплатных систем прокторинга отсутствует. В-третьих, это риски информационной безопасности, связанные с передачей личной информации и данных об устройстве внешним структурам, обеспечивающим управление системами прокторинга, несмотря на предоставляемые ими документальные гарантии защиты такой информации. Определенный риск представляет получение удаленного доступа системой прокторинга к компьютеру обучаемого, что в условиях использования несертифицированных коммерческих систем, позволяет использовать более широкие, чем заявлено, и недокументированные возможности. В-четвертых, противодействие со стороны обучаемых, связанное с восприятием систем прокторинга, как вторжения «большого брата» в личную жизнь, что в совокупности с определенными негативными особенностями мировоззрения, усиленными возможностями современных информационных коммуникационных технологий, провоцирует обучаемых на поиск возможностей обхода ограничений систем подобного рода. Таким образом подобные системы контроля учебных мероприятий далеко не идеальны, требуют ответственного отношения к их использованию и гарантий прав обучаемых.

ВЫБОР ИНФОРМАТИВНЫХ ПАРАМЕТРОВ ДЛЯ ПРОГНОЗИРОВАНИЯ ИНДИВИДУАЛЬНОЙ НАДЕЖНОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

В.О. Казючиц, С.М. Боровиков, Е.Н. Шнейдеров

Одним из способов повышения надежности электронных устройств обеспечения безопасности является постановка в их конструкции высоконадежных полупроводниковых приборов (ППП), которые могут быть отобраны методом прогнозирования индивидуальной надежности из однотипных экземпляров. Для прогнозирования надежности ППП необходимо знать информативные параметры. Их поиск выполняется с помощью экспериментального исследования выборки однотипных ППП [1]. Цель работы – найти информативные параметры для транзисторов типа КП744А. Для достижения цели у выборки объемом 200 экземпляров в начальный момент времени были измерены электрические параметры, предполагаемые на информативность. Далее проводились ускоренные испытания выборки на длительную наработку с периодическим контролем времени потери ее экземплярами работоспособности. Выполняемый в дальнейшем корреляционный анализ [2] позволил выявить информативные параметры и выбрать те, измерение которых не вызывает сложности. Доклад подготовлен при выполнении проекта № Т20МВ-026 на тему «Прогнозирование эксплуатационной надежности мощных ППП с использованием методов и алгоритмов машинного обучения» (утвержден Научным советом БРФФИ 22 апреля 2020 г.).

Литература

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

2. Казючиц В.О., Шнейдеров Е.Н. Корреляционный анализ в решении задачи поиска информативных параметров транзисторов большой мощности // Электронные системы и технологии: сборник материалов 57-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 19–23 апреля 2021 г. С. 544–546.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ФОРМИРОВАНИЯ КЛЮЧА PBKDF2 НА БАЗЕ FPGA

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

В настоящее время для разрешения доступа пользователей к электронным данным широко используются пароли. Из-за плохой случайности и произвольной длины этих паролей они не могут использоваться в качестве ключей криптографических алгоритмов шифрования. В большинстве случаев ключи получают на основе паролей с использованием криптографических хэш-функций. Функция PBKDF2 (Password Based Key Derivation Function v2) является одним из важнейших криптографических алгоритмов [1], широко используемым в различных системах, таких как WiFi Protected Access (WPA/WPA2), Microsoft .NET framework, Apple OSX Operating System, Apple iOS, Blackberry и др. Характерной особенностью данной функции является большое (несколько тысяч или десятков тысяч) число повторений использования механизма HMAC (hash-based message authentication code – код проверки подлинности сообщений, использующий хэш-функции). В результате процесс формирования ключа занимает значительное время. В докладе рассматривается подход к конвейеризации процесса вычисления ключей в процессоре PBKDF2 на основе алгоритма SHA-1, который можно использовать в различных встраиваемых системах с достаточно высокой производительностью. Так как алгоритм вычисления ключа PBKDF2 носит итерационный характер, то максимальная производительность может быть получена при полной развертке алгоритма. Однако такая развертка характеризуется большим количеством ступеней (модулей SHA-1) – порядка нескольких десятков тысяч. Реализовать такое количество ступеней в рамках FPGA не представляется возможным. Компромиссное решение заключается в конвейеризации процесса вычисления хэш-значений в алгоритме SHA-1 с сохранением итерационного процесса вычисления ключей PBKDF2. При этом процессор может вычислять не один ключ, а одновременно несколько ключей по количеству ступеней в конвейере.

Рассматриваемый в докладе подход предполагает конвейеризацию алгоритма SHA-1 на уровне раундов, т. е. на каждой ступени конвейера реализуется один раунд алгоритма и модуль SHA-1 содержит 4 ступени [2]. Так как каждый раунд состоит из 20 шагов, то каждое входное значение итерационно 20 раз прокручивается на ступени конвейера, последовательно проходя через все 4 ступени. Полный конвейер одной итерации вычисления ключа PBKDF2 строится на базе двух модулей SHA-1 и состоит из 8 ступеней. В процессор PBKDF2, построенный на базе такого модуля SHA-1, можно последовательно загрузить 8 входных значений и организовать одновременное вычисление 8 ключей. Через промежуток времени, равный времени вычисления одного ключа, на выходе процессора последовательно будут получаться 8 значений ключей.

Цикл работы процессора PBKDF2 составляет 23 такта. Через каждые 23 такта в процессор загружается 8 входных значений. Время формирования ключа составляет

920000 тактов, после чего на выход через каждые 23 такта последовательно выдаются 8 вычисленных значений ключа.

Характеристики реализации процессора PBKDF2 с использованием пакета ISE 14.7 для кристалла FPGA семейства Virtex7 XC7VX485T-1: 8493 триггеров секций, 5575 просмотровых таблиц (LUT), рабочая тактовая частота по оценкам процедуры синтеза – 253 МГц.

Литература

1. NIST SP 800-132. Recommendation for Password-Based Key Derivations. Desember 2010. [Электронный ресурс]. – Режим доступа: http://nvlpubs.nist.gov/ nistpubs/Legacy/SP/ nistspecialpublication800-132.pdf. – Дата доступа: 03.05.2021.

2. Jae-woon Kim, Hu-ung Lee, Youjip Won. Design for high throughput SHA-1 hash function on FPGA, 2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN), July.4-6 2012, Phuket, Thailand. [Электронный ресурс]. – Режим доступа: http://www.esos.hanyang.ac.kr/files/publication/conferences/international/Design_for_high_throughput_SHA-1_hash_function_on_FPGA.pdf. – Дата доступа: 03.05.2021.

КЛАССЫ ДЛЯ РАБОТЫ С ПАРОЛЯМИ В КРОССПЛАТФОРМЕННОМ ФРЕЙМВОРКЕ Qt

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

При решении различного рода криптографических задач нередко возникает необходимость обеспечения эффективной работы с паролями. К таким задачам относятся задачи, связанные с обеспечением корректной работы программного средства, предназначенного для управления паролями. При работе с паролями используются многосимвольные алфавиты, обеспечивающие корректное генерирование паролей с использованием как существующих символов национальных алфавитов, цифр и специальных символов, так и искусственно сгенерированных символьных последовательностей, необязательно являющихся общеупотребительными символами в том или ином регионе.

В то же время любой пароль является сложно организованным структурированным числовым кодом, для которого можно использовать представление в системе счисления с произвольным основанием. При этом пароль может иметь произвольное количество полей, длина которых может динамически изменяться, и код в которых может быть в общем случае представлен в различных системах счисления. При работе с паролями приходится выполнять различное количество математических операций над сложными динамическими структурами, представленными в произвольных системах счисления. Существующие инструментальные системы разработки программного обеспечения не позволяют эффективно выполнять действия, связанные с обработкой кодов паролей, что затрудняет решение практических задач.

Для решения практических задач генерирования сложных паролей, состоящих из произвольного количества полей, в среде Qt были созданы два класса: ParolField на базе класса QByteArray [1] и ParolMultiField на базе класса ParolField. Классы позволяют создавать объекты в виде сложных паролей, использующие произвольный алфавит и имеющие динамически изменяющуюся длину для любого поля пароля. Максимальное количество символов в алфавите может составлять 256. Над паролями для каждого класса определены базовые и дополнительные математические операции, позволяющие выполнять математические действия над агрегатированными кодами,

представленными в индивидуальной системе счисления для каждого поля кода пароля, имеющего произвольную длину.

Разработанные классы позволили эффективно решать задачи генерирования и обработки сложных паролей с использованием кроссплатформенного фреймворка Qt.

Литература

1. Шлее М. Qt 5.10 Профессиональное программирование на C++. СПб.: БХВ-Петербург, 2018. 1072 с.

ТЕОРЕТИЧЕСКИЕ РАСПРЕДЕЛЕНИЯ СТАТИСТИК ТЕСТА КУМУЛЯТИВНЫХ СУММ ДЛЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ДЛИНАМИ 192 И 1024 БИТА

Н.Г. Киевец

Для оценки качества работы генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) может использоваться двухуровневое тестирование вырабатываемых ГСЧ случайных последовательностей (СП).

В случае применения двухуровневого тестирования к СП с длинами практически используемых криптографических ключей требуется нахождение теоретического распределения тестовой статистики теста при каждой длине СП [1].

В докладе обсуждаются полученные автором теоретические распределения тестовых статистик теста кумулятивных сумм для СП с длинами 192 и 1024 бита. Теоретические распределения представлены в виде графиков. Приводятся результаты двухуровневого тестирования СП с длинами 192 и 1024 бита, выработанных ГСЧ десяти ЭПК с микроконтроллером К5004 ВЕ2. Полученные результаты свидетельствуют о высоком качестве работы ГСЧ ЭПК и подтверждают их пригодность для выработки криптографических ключей с длинами 192 и1024 бита.

Литература

1. Киевец, Н.Г. Оценка качества работы генераторов случайных чисел на основе двухуровневого тестирования // Проблемы инфокоммуникаций. 2017. № 1 (5). С. 19–23.

О ВЛИЯНИИ ДИФФЕРЕНЦИАЛЬНЫХ ПРОСТРАНСТВ ВОДОРОДОПОДОБНЫХ АТОМОВ НА ПЕРЕДАЧУ ДАННЫХ В КРИПТОГРАФИЧЕСКИХ КАНАЛАХ СВЯЗИ

И.П. Кобяк

Полученные на основе дифференциальных и интегральных преобразований соотношения позволили определить внутренние преобразования центроаффинных пространств атома водорода с учетом перехода его параметров на комплексной плоскости. Основой для проведения исследований послужила гипотеза о влиянии релятивистских пространств на помехоустойчивость криптографических каналов связи при передаче информации. В соответствии с поставленной задачей была доказана следующая теорема.

Теорема. *Re*-пространственная оболочка ядра атома водорода радиуса $\vec{r}_{st}$ в процессе обретения внешней энергии «струн» является образующим началом пространства электрона с радиусом $\vec{r}_{0,L}$, преобразуемым в орбиту шестого измерения

$j\vec{r}_{st,c}^{\tau=1}$, расширяемую далее до уровня $j\vec{r}_{0,L}(1-\vec{\psi})$ на скорости $-\left(\vec{c}\sqrt{2}-\Delta\vec{c}\right)$. Для доказательства теоремы рассмотрено влияние процесса изменения радиуса ядра на уровень изменения нулевого радиуса $\vec{r}_{0,L}$ с использованием механизма дифференцирования преобразованного соотношения для боровского радиуса. С этой целью на первом шаге базовое соотношение было возведено в квадрат, после чего выполнялось его дифференцирование. Это позволило в процессе преобразования установить закономерность перехода пространства боровского радиуса в пространство шестого измерения.

Анализ принципа дифференцирования преобразованного соотношения для нулевого радиуса с общетехнической точки зрения следует считать обоснованным механизмом выделения энергии ядра в релятивистское пространство, формируемое по центроаффинному закону.

В представленной в данной работе концепции исследования пространств скорость вращения внешней оболочки ядра оказалась близкой к скорости света. На классическом радиусе $\vec{r}_{st}=1,23\cdot10^{-13}$ см эта скорость оказалась равной $\vec{v}_{st}\approx 299{,}792\ 457\ 92\cdot10^{8}$ см/с. Данное значение может рассматриваться как приобретенная (наиболее вероятная) скорость вращения наночастицы, порождаемая принципом связи ядра с энергией «струн».

СКРЕМБЛИРОВАНИЕ ЗАШУМЛЕННЫХ СООБЩЕНИЙ В МНОГОЯДЕРНОЙ ВЫЧИСЛИТЕЛЬНОЙ СРЕДЕ

И.П. Кобяк

В представляемой работе рассмотрен метод нахождения детерминизма в зашумленных сообщениях с использованием многоядерных процессоров. Сущность метода заключается в декомпозиции последовательности T^n из n символов на m подмножеств с последующим удалением шума в каждом из подмножеств. Вновь сформированные последовательности E^m рассматривается как кодированные сообщения некоторого выбранного языка с фиксированной длиной букв равной l ($l = l_1, l_2, \ldots$). За каждым из m подмножеств символов закрепляется свое ядро многоядерной системы, реализующее функцию раскодирования. На шаге два наборы двоичных бит E^m проверяется на принадлежность кодировкам заданного языка из таблицы t_k всевозможных кодов символов с 2^l ячейками. При совпадении символов и кодов формируется буквенное слово, которое записывается в свой слот общего фрейма системы. В качестве фрейма используется виртуальный объект, состоящий из m призм с s гранями. При этом каждая i-я (i = 1, 2, … ,s) грань призмы длиной m является слотом соответствующего ядра процессора. Под действием алгоритма выполняется заполнение слотов всех призм фрейма. Далее осуществляется программное «вращение» призм друг относительно друга с выбором лингвистической подсистемой некоторого «осмысленного» сообщения, что соответствует приведенному в [1] алгоритму скремблирования. Положительным моментом представленной системы является параллельное формирование шумов, приводящее к сокращению времени в фазе преобразования $T^n \rightarrow E^m$ с $f(2^n)$ до $f(2^m)$. Максимальное же время «лингвистического» вращения в составе фрейма определяется как $f(s^m)$.

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ. 2001. 480 с.

РЕГУЛИРУЕМЫЕ АНТЕННЫЕ ОПОРЫ ЕМКОСТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ

А.Н. Коваленко

На основе емкостного принципа преобразования микродвижений постоянно разрабатываются новые технические средства охраны, устанавливаемые как внутри помещений, так и на периметрах охраняемых объектов. При этом повышенное внимание уделяется вопросам устойчивости емкостных устройств, размещаемых на открытом пространстве и подвергающихся воздействию различных факторов. В частности, осадки или увеличение влажности воздуха могут оказывать большое влияние на места крепления чувствительного элемента, снижая чувствительность емкостного преобразователя и вызывая ложные сигналы тревоги в системе охраны. Электромагнитные поля от посторонних источников воздействуют на приемный электрод неэкранированного чувствительного элемента как на приемную радиоантенну, вызывая паразитную модуляцию электрического сигнала, индуцируемого генераторным электродом.

Периметры охраняемых объектов оборудуются различными емкостными датчиками обнаружения. Датчики подключаются к антенному устройству, состоящему из двух флангов равной длинны от 10 до 500 м каждый, с максимальной емкостью не более 12000 пФ и имеющих разброс емкостей флангов антенного устройства не более чем на 10 % относительно друг друга. Зачастую на практике мы сталкиваемся с разницей по емкости антенных плеч более 10 %. Для решения данной задачи предлагается использование регулируемых антенных опор на периметре. Это позволит производить по месту точную настройку симметрии емкости антенного полотна. При точной настройке емкостного полотна, исключается применение «подстроечного» конденсатора, тем самым повышается стабильность работы емкостных датчиков обнаружения [1, 2].

Литература

1. Минкин В.А. Исследование возможностей идентификации человека. – ООО «Элсис» 2012. [Электронный ресурс]. – Режим доступа: http://vi.elsys.ru/storage/nto.pdf. – Дата доступа: 24.03.2020.

2. Стратов, Д.С. Емкостные датчики (извещатели) обнаружения типа «Микрос-101». [Электронный ресурс]. – Режим доступа: http://mikros.ru/datchiki/6/35/ – Дата доступа: 15.04.2020.

ЗНАЧЕНИЕ ПЕДАГОГА В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Д.Г. Козленко

Решение проблем подготовки специалистов в области защиты информации должно проходить под руководством знающих, квалифицированных педагогов, учитывающих все необходимые составляющие как единого педагогического процесса, так и широкого спектра аспектов защиты информации (технических, нормативно-правовых и др.). Указанное требует повышения компетентности педагогов, которая должна объединять и высокую профессиональную и развитую социальную компетентности. Следует отметить, что в подготовке специалистов в области защиты информации имеют значение не только глубокие знания технической и программной базы, но и уверенное владение правилами и основами информационной культуры и информационной этики.

Возможно выделить следующие задачи социального характера деятельности педагога в подготовке специалистов в области защиты информации, не затрагивающие непосредственно содержание соответствующих учебных дисциплин: 1) формирование устойчивых убеждений и ответственности в области информационной безопасности и защиты информации; 2) формирование устойчивых поведенческих навыков в области информационной безопасности и защиты информации; 3) развитие способности распознавать и противостоять информационным угрозам.

Решение этих задач должно выполняться комплексно и систематически в течение всего срока подготовки специалистов, так или иначе связанных с защитой информации. При этом важно сформировать осознанные самостоятельные умения обучающихся безопасно работать с информацией, применять знания и умения ее защиты. В этих целях возможно проведение факультативных занятий, дополнительных бесед, практикумов, тренингов и других мероприятий [1, 2].

Литература

1. Пунченко О.П. Защита информации как маркер цивилизационного развития человечества // Труды БГТУ. Серия 6: История, философия. 2014. № 5. С. 82–86.

2. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 Создание глобальной культуры кибербезопасности [Электронный ресурс]. – Режим доступа: https://www.ifap.ru/ofdocs/un/57239.pdf. – Дата доступа: 28.04.2021.

УГРОЗЫ И УЯЗВИМОСТИ БЕЗОПАСНОСТИ СИСТЕМ ПРОКТОРИНГА

Т.Е. Козляк

В связи с переходом к проведению занятий в удаленной форме, учебные заведения столкнулись с проблемой обеспечения безопасности удаленных экзаменов и обоснования достоверности их результатов. В связи с этим резко вырос интерес к использованию систем прокторинга. Прокторинг – это процедура контроля на онлайн-экзамене, где за всем процессом наблюдает администратор – проктор. В системах такого вида, как правило, требуется первоначально пройти проверку с администратором и предоставить системе прокторинга удаленный доступ компьютеру. Далее администратор осмотрит комнату, рабочий стол, сделает фотографию удостоверение личности, соберет дополнительную информацию об компьютере сдающего и будет следить за всем происходящим во время экзамена. Во время экзамена данные будут собираться в режиме реального времени и отправляться на сервер. Сервер, помимо хранения информации, обрабатывает ее с помощью AI-алгоритмов. В то же время такая система оценивания знаний далеко не идеальна и имеет уязвимости. Основными рисками информационной безопасности таких систем является то, что эффективная система прокторинга должна работать в режиме «автопрокторинга», без участия администратора. Поэтому основными ее уязвимости будут следующие. Наличие «слепых зон» для видеокамеры. В зависимости от того, где расположена и как ориентирована видеокамера испытуемого, слепые зоны могут располагаться перед испытуемым, на его рабочем столе и под рабочим столом. Использование студентом средств невербального общения, которые не регистрируется видеокамерой и микрофоном. Это проблемы, связанные с мимикой, движениями глаз, положением руг и глаз, условными сигналами и прочими проявлениями, для которых пока нет удовлетворительных решений. Недостатки алгоритма интеллектуального анализа данных видеопотока, реализованного в рамках конкретной системы прокторинга. Во-первых, любая

программа может дать сбой или не распознать нештатную ситуацию. Во-вторых, программа может выдавать лишь рекомендации администратору, что предполагает отсрочку времени принятия окончательного решения.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕАЛИЗАЦИИ КВАНТОВОГО ШИФРОВАНИЯ

А.С. Кривда

Шифрование информации на протяжении всей своей истории человечество всегда было весьма актуальной темой, поэтому и появилась целая наука – криптография. На сегодняшний день криптография широко используется для защиты данных в сети. Базовой задачей криптографии является шифрование данных и аутентификация отправителя. Это легко выполнить, если отправитель и получатель имеют криптографический ключ. Криптографический ключ – это числовая последовательность определенной длины, созданная для шифрования информации. Перед началом обмена каждый из участников должен получить ключ, причем эту процедуру следует выполнить с наивысшим уровнем конфиденциальности, так, чтобы никакая третья сторона не могла получить доступ даже к части этой информации. Задача безопасной пересылки ключей может быть решена с помощью квантовой криптографии, которая позволяет обеспечить постоянную и автоматическую генерацию ключей. Технология квантового распределения криптографических ключей решает одну из основных задач криптографии – гарантированное распределение ключей между удаленными пользователями по открытым каналам связи, при этом любая попытка злоумышленника вмешаться в процесс передачи криптографических ключей вызовет высокий уровень ошибок. На сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью. Надежность метода основывается на законах квантовой механики.

Необходимо отметить, что проблемы реализации квантового шифрования остаются. Кодировать данные в квантовых состояниях достаточно сложно, для этого нужно уметь генерировать и детектировать одиночный фотон, что является непростой технологической задачей. Так же квантовые состояния уязвимы и могут разрушаться под действием тепловых шумов и других помех. Реальные квантовые устройства остаются уязвимыми для некоторых типов атак [1–3].

Литература

1. Cambridge Journal of science and policy. Quantum Key Distribution: Advantages, Challenges and Policy [Electronic resource]. – Access mode: https://www.repository.cam.ac.uk/bitstream/handle/1810/311529/CJSP_Paper_Lovic.pdf?sequence=1. – Date of access: 28.04.2021.

2. Quantum Cryptography, Explained [Electronic resource]. – Access mode: https://quantumxc.com/quantum-cryptography-explained/. – Date of access: 28.04.2021.

3. Квантовая криптография / шифрование [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/. – Дата доступа: 28.04.2021.

ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.М. Кузьмицкий

Для эффективной защиты информации, наряду с техническими мерами следует предусматривать организационные, которые проводятся систематически, эпизодически и спорадично. К безотлагательным мерам по обеспечению достаточного уровня

физической защиты надо отнести неукоснительное соблюдение пропускного и внутриобъектового режима на объектах информатизации. В обязанности должностных лиц, отвечающих за работы по поддержке функционирования и управлению средствами, включается контроль за работой персонала системы и за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС. В период проектирования и эксплуатации проводить анализ состояния и оценка эффективности мер и применяемых средств защиты.

К периодически проводимым мероприятиям относятся распределение реквизитов разграничения доступа (паролей, криптографических алгоритмов и пр.) Проводятся анализ системных журналов и принятие мер по выявленным нарушениям правил работы. Меры по пересмотру правил разграничения доступа пользователей к информации пересматриваются один раз в полугодие. Анализ состояния и оценки эффективности мер и применяемых средств защиты необходимо проводить с приглашением внешних специалистов по безопасности.

П необходимости осуществляются мероприятия при организационно-штатных изменениях в составе персонала системы. Все изменения в архитектуре сети и программном обеспечении рассматриваются, проверяются на удовлетворение требованиям защиты и утверждаются руководителем. Не стоит ослаблять внимания на потенциальных внутренних и комбинированных нарушителей. Отбор и расстановка кадров осуществляется после проверки принимаемых на работу. Затем проводится обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты [1, 2].

Литература

1. Постановление Совета Безопасности Республики Беларусь 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь».

2. Голиков В.Ф., Лыньков Л.М., Прудник А.М., Борботько Т.В. Правовые и организационно-технические методы защиты информации. Минск, БГУИР, 2004. 81 с.

ОБЗОР ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ СОЗДАНИЯ УСТАНОВКИ ДЛЯ ПОВЕРКИ АТТЕНЮАТОРОВ

А.Н. Кузюков, Д.Г. Булавко

В последние годы одним из важнейших направлений развития радиоэлектроники стало продвижение в область миллиметрового диапазона длин волн. Это связано с резким ростом числа радиоэлектронных устройств и систем, в связи с чем стала ощущаться нехватка свободных частот в диапазоне менее 30 ГГц. Имеющиеся в эксплуатации средства измерения ослабления электромагнитных колебаний в волноводных трактах в диапазоне частот от 37,5 до 178,4 ГГц не обеспечены поверкой и калибровкой из-за отсутствия образцовых средств измерений и эталонов, что создает определенные сложности в обеспечении точности и достоверности измерений, а выпускаемые за рубежом аналогичные средства измерений ослабления электромагнитных колебаний весьма дорогостоящи, что не позволяет их приобретать из-за отсутствия валютных средств. Для создания отечественной установки для поверки аттенюаторов в диапазоне частот от 37,5 до 178,4 ГГц понадобится следующая элементная база: генератор СВЧ-сигналов, эталонные аттенюаторы, смесители СВЧ-сигналов, УПЧ со схемой сравнения, полосовой фильтр, амплитудный детектор, узкополосный фильтр, фазовый детектор, гетеродин, эталонный аттенюатор ПЧ, генератор ПЧ, индикаторный блок, персональный компьютер, блок управления.

Создание отечественной установки позволит сократить отток валютных средств и позволит проводить исследования, поверку, калибровку измерителей ослабления и комплексных коэффициентов передачи в диапазоне частот от 37,5 до 178,4 ГГц.

ВЕРИФИКАЦИЯ ДИКТОРА ПО ГОЛОСУ НА БАЗЕ МЕТОДА ДИНАМИЧЕСКОГО ИСКАЖЕНИЯ ВРЕМЕНИ

Ю.О. Куницкий, О.Б. Зельманский

Широкое применение биометрических систем влечет за собой повышенный интерес со стороны злоумышленников, направленный на разработку атак по их взлому. Наиболее часто применяемой является атака, суть которой заключается в том, что в систему передаются биометрические признаки, предъявленные ранее, например, силиконовый муляж пальца или магнитофонная запись парольной фразы. Таким образом, разработку систем биометрической идентификации необходимо вести с учетом защиты от этих атак. Свести к минимуму недостатки указанных выше методов биометрической идентификации пользователей позволит разработка новых методов и алгоритмов идентификации, основанных на предъявлении случайно сформированных ключевых признаков из биометрической базы эталонов пользователей. К подобному методу биометрической идентификации пользователей информационных систем относится идентификация по голосу, позволяющая получать и передавать в удостоверяющий центр биометрические данные без применения специализированных и дорогостоящих считывателей биометрической информации: достаточно иметь телефон или микрофон, подключенный к компьютеру. Однако, не смотря на все преимущество такого подхода, необходимо уделить особое внимание проблеме вариативности речи.

Проблема вариативности речи, а именно изменчивость длины разных вариантов одного и того же слова или аллофонов этого слова обычно решается с применением методов динамического искажения времени (DTW-алгоритм) [1]. Измерение расстояния между двумя временными рядами нужно для того, чтобы определить их подобие и классификацию. Таким эффективным измерением является евклидова метрика. Для двух временных последовательностей это просто сумма квадратов расстояний от каждой *n*-ой точки одной последовательности до *n*-ой точки другой. Однако использование евклидова расстояния имеет существенный недостаток: если два временных ряда одинаковы, но один из них незначительно смещен во времени (вдоль оси времени), то евклидова метрика может посчитать, что ряды отличаются друг от друга. DTW-алгоритм был введен для того, чтобы преодолеть этот недостаток и предоставить наглядное измерение расстояния между рядами, не обращая внимание как на глобальные, так и на локальные сдвиги на временной шкале.

Быстрый DTW-алгоритм обладает линейной пространственной и временной сложностью и использует многоуровневый подход с тремя ключевыми операциями [2]: уменьшение детализации; планирование; обработка. Одним из возможных решений проблемы вариативности речи при разработке программного модуля биометрической верификации является использование быстрого DTW-алгоритма.

Литература

1. Stuart N. Wrigley. Speech Recognition by Dynamic Time Warping. University of Sheffield, 1998.

2. Salvador S., Chan P. Fast DTW: Toward Accurate Dynamic Time Warping in Linear Time and Space // Intelligent Data Analysis. 2004. No. 11 (5). P. 70–80.

ТОНКАЯ ПЛЕНКА СВЕРХПРОВОДНИКА В СЛАБОМ НЕОДНОРОДНОМ МАГНИТНОМ ПОЛЕ

В.Н. Кушнир, С.Л. Прищепа

Перспективным направлением сверхпроводниковой спинтроники является разработка логических устройств на основе слоистых структур сверхпроводник (*S*) – ферромагнетик (*F*) [1]. Существенным фактором, влияющим на электрофизические характеристики *S*/*F*-структур, является поле рассеяния ферромагнетика. В данной работе предлагается экспериментальный метод исследования этого влияния путем включения диэлектрических прослоек (*I*) различной толщины между *S*- и *F*-слоями. Показано, что наиболее чувствительной характеристикой к изменениям поля рассеяния является зависимость критического тока, J_c, тонкой *S*-пленки от температуры *T*. В первую очередь был выполнен эксперимент по измерению характеристики $J_c(T)$ структуры *S*/*I*/*F* с толстым слоем диэлектрика для двух состояний *F*-слоя – размагниченного (*D*) и с остаточной планарной намагниченностью (IPR). В этом случае поле рассеяния является возмущением, не приводящим к образованию в сверхпроводнике абрикосовских вихрей. Более того, расчетом поля рассеяния слоя ферромагнетика, используемого в эксперименте, показано, что пространственное распределение этого поля хорошо аппроксимируется гармоническими функциями с волновыми числами, зависящими от магнитного состояния. Найденные аппроксимации позволили рассчитать в формализме уравнений Гинзбурга – Ландау температурные зависимости критического тока для *D*- и *IPR*-состояний *F*-слоя. В результате был объяснен эффект слияния обеих характеристик $J_c(T)$ при температурах, близких к критической температуре, и их расхождение при низких температурах, как эффект за счет различной топологии поля рассеяния [2].

Литература

1. Tagirov L.R., Kupriyanov M.Yu., Kushnir V.N., Sidorenko A. Superconducting triplet proximity and Josephson spin valves. In: Functional Nanostructures and Metamaterials for Superconducting Spintronics (From Superconducting Qubits to Self-Organized Nanostructures): Ed. A. Sidorenko. Vol. 1. Springer Series NanoScience and Technology, 2018. P. 31–47.

2. Kushnir V.N., Prischepa S.L., Trezza M., Cirillo C., Attanasio C. // Coatings. 2021. Vol. 11, No. 5. P. 507 (14).

ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ АЛЮМИНИЕВОЙ РЕШЕТКИ, ВСТРОЕННОЙ В АНОДНЫЙ ОКСИД АЛЮМИНИЯ

С.К. Лазарук, В.В. Дудич, Д.А. Сасинович, Г.С. Паскробка

Одним из способов защиты информации от утечки по техническим каналам является электромагнитное экранирование. Авторы изготовили и исследовали экраны электромагнитного излучения на основе алюминиевой решетки и анодного оксида алюминия. Алюминиевая решетка формировалась на стеклянной подложке при помощи операций, используемых в технологии изготовления встроенной алюмооксидной металлизации интегральных схем [1]. Период алюминиевой решетки составлял 1 мм. Установлено, что значения коэффициента отражения электромагнитного излучения в диапазоне частот от 5,0 до 12,0 ГГц изготовленных экранов изменяются в пределах от –10,0 дБ до –27,0 дБ. Определено, что для снижения коэффициента

передачи электромагнитного излучения изготовленных экранов необходимо уменьшать период входящей в его структуру решетки. В частности, проведенные расчеты показывают, что при уменьшении до 20,0 мкм периода решетки коэффициент передачи электромагнитного излучения экранов, в структуру которых она входит, будет менее –40,0 дБ, что позволяет рассматривать эти экраны в качестве эффективных средств защиты информации от утечки по технических каналам.

Литература

1. Lazarouk S., Katsouba S., Demianovich A., Stanovski V., Voitech S., Vysotski V., Ponomar V. // Solid-State Electronics. 2000. Vol. 44, No. 5. P. 815–818.

КОНДЕНСАТОРЫ ПОВЫШЕННОЙ ЕМКОСТИ НА ОСНОВЕ ПОРИСТОГО АЛЮМИНИЯ С ИСПОЛЬЗОВАНИЕМ ВОДНОГО РАСТВОРА ХЛОРИДА НАТРИЯ В КАЧЕСТВЕ ВТОРОЙ ОБКЛАДКИ

С.К. Лазарук, Л.П. Томашевич, Н.А. Казимиров, К.А. Антипов,
Н.Н. Стешиц, О.В. Купреева

Сфера применения суперконденсаторов достаточно разнообразна. Их используют в качестве источников основного и резервного питания как в системах общественного транспорта, так и в различной радиоэлектронной и бытовой технике. В настоящее время для производства конденсаторов высокой емкости в качестве токосъемника положительного электрода используется алюминий, который является хорошим электрическим проводником и образует на поверхности пассивную пленку, обеспечивающую превосходную коррозионную стойкость.

Для сравнения электрофизических характеристик были сформированы конденсаторные структуры на основе планарного и пористого алюминия. Наноструктурирование алюминиевой поверхности проводили в электролитах на основе водного раствора NaCl при анодном напряжении до 50 В и плотности тока от 200 мА/см^2 до 800 мА/см^2. Исследования на электронном микроскопе показали, что в результате электрохимической обработки образуется пористая структура с минимальными размерами до 100 нм, толщина полученных пленок варьировалась от 10 до 130 мкм. Далее на пористой алюминиевой поверхности формировали слой анодного оксида алюминия при помощи электрохимического анодирования в 1 % водном растворе лимонной кислоты. Такой же слой анодного оксида был сформирован и на образцах планарного алюминия. Верхняя обкладка конденсаторной структуры формировалась с помощью водного раствора хлорида натрия. Регистрация значений емкости с помощью измерителя иммитанса показали, что использование в качестве нижней обкладки конденсатора пористого алюминия позволяет повысить удельную емкость конденсаторов более чем на порядок по сравнению с аналогами, у которых в качестве нижней обкладки используется планарная алюминиевая пленка.

Таким образом, было установлено, что применение пористого алюминия в производстве суперконденсаторов является весьма перспективным, так как позволяет на порядок увеличить емкость таких структур по сравнению с конденсаторными структурами на основе планарного алюминия.

ГЕНЕРАТОР СВЧ ДЛЯ ИМИТАЦИИ СИГНАЛОВ ОТ ВОЗДУШНЫХ ЦЕЛЕЙ

Д.А. Лисов, А.Н. Кузюков

На базе научно-технического обеспечения Центра 1.9 «Научно-производственно-образовательный инновационный центр СВЧ технологий и их метрологического обеспечения» разрабатывается модуль имитатора цели генератора сложных СВЧ сигналов в диапазоне частот 1–20 ГГц. Данный модуль предназначен для формирования в реальном масштабе времени сигналов промежуточной частоты, необходимых для проведения испытаний, наладки и функционального контроля приемных устройств радаров. Имитатор обеспечивает формирование сигналов на промежуточной частоте, адекватных реальным сигналам приемного устройства радара с учетом мешающих отражений, внутренних шумов, активных шумовых и импульсных помех, а также формирование основных синхросигналов станции.

Входные сигналы поступают в модуль и подаются через входной буфер в программируемую логическую интегральную схему (ПЛИС). Выходные цифровые сигналы ПЛИС поступают на цифро-аналоговый преобразователь для представления их в аналоговом виде. В ПЛИС реализованы следующие функциональные компоненты: генератор эхо-сигналов целей, генератор сигналов мешающих отражений, генератор активных помех, генератор импульсных помех, генератор шума, мультиплексор, два комплексных сумматора, схемы тактирования и управления.

Генератор эхо-сигналов целей обеспечивает формирование эхо-сигналов от целей с учетом дальности, скорости сближения и флуктуаций. Генератор сигналов мешающих отражений обеспечивает формирование эхо-сигналов от подстилающей поверхности и других объектов с учетом погодной обстановки. Генератор сигналов активных помех обеспечивает имитацию сигналов от помехопостановщиков. Генератор импульсных помех обеспечивает имитацию сигналов от передатчиков других импульсных РЛС, работающих в том же диапазоне частот и других импульсных источников помех. Генератор шума обеспечивает имитацию внутреннего случайного шума приемного тракта РЛС.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТИ «ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

В.М. Логин

В современных условиях рынок систем безопасности (СБ) требует новых подходов к системе подготовки специалистов в области безопасности. Многофункциональные интеллектуальные СБ, построенные на IP и IT-технологиях, становятся наиболее востребованными, вытесняя традиционные системы [1]. Выпускники специальности «Электронные системы безопасности» могут в совершенстве разрабатывать любые инновационные системы безопасности. Наряду с фундаментальной подготовкой будущие специалисты (инженер-проектировщик) имеют теоретические знания и практические навыки по следующим направлениям: современные методологии и технологии защиты объектов, их материальных и информационных ресурсов, а также персонала; информационные технологии и программирование, в том числе встраиваемые в СБ компьютерная и микропроцессорная техника; радиоэлектроника и автоматика; телекоммуникационные и компьютерные системы и сети; надежность технических систем и эффективность функционирования СБ на промышленных объектах; интернет-технологии распределения и передачи

данных; специальные системы и средства (реального времени, защиты информации); исполнительные устройства, датчики, видеотехника СБ и систем контроля и управления доступом; организация и функционирование сложных электронных систем [2]. Выпускники специальности могут работать: на промышленных предприятиях, производящих или эксплуатирующих вычислительную, электронную и оптическую аппаратуру; в организациях, производящих программное обеспечение, консультационные и другие сопутствующие услуги; на предприятиях и в организациях, занимающихся деятельность в области телекоммуникаций; в организациях, осуществляющих инженерно-техническое проектирование.

Литература

1. Электронные системы безопасности [Электронный ресурс]. – 2017. – Режим доступа: https://fkp.bsuir.by/enrollee/specialties/electronic-security-systems. – Дата доступа: 03.05.2021.

2. ОСВО 1-39 03 01-2013. Электронные системы безопасности. – Введ. 01.09.2013. – Минск: Министерство образования Республики Беларусь, 2013.

ТЕХНИЧЕСКИЕ СРЕДСТВА ПЕРЕДАЧИ АУДИОСИГНАЛА ПО ЦЕПИ ПИТАНИЯ

В.М. Логин

Скрытый съем информации по цепи питания представляет большой интерес в системах, где выделение отдельной линии для обмена данными вызывает затруднения, либо нецелесообразно, либо в принципе невозможно. Более того, оборудование телеметрии, сбора данных, датчиков присутствия и т.п. обычно не энергоемко и не требует больших скоростей для передачи данных [1]. Для этих целей предлагается использовать сетевой низкочастотный передатчик и приемник. Передатчик излучает низкочастотные колебания (50–300 кГц) в сеть, используя провода сети в качестве антенны. Данное устройство имеет очень высокую скрытность, т.к. практически не излучает сигналы в окружающее пространство. Для передачи полезной информации используется частотная модуляция с частотой несущей 95 кГц. Такой радиопередатчик питается от сети через бестранформаторный блок питания. Частотный модулятор, собранный на микросхеме 561ЛА7, представляет собой генератор прямоугольных импульсов, управляемый напряжением. Частота следования импульсов моделируется напряжением звуковой частоты (ЗЧ), поступающего с соответствующего усилителя. Промодулированные колебания ЗЧ поступают на усилитель мощности, собранный на транзисторах типа КТ315. Нагрузкой служит трансформатор, первичная обмотка которого образует колебательный контур, настроенный на частоту несущей. Такой сигнал необходимо принимать на специальный приемник. Сверхрегенеративный приемник работает как составная часть простой портативной радиостанции, настроенной на диапазон порядка 140 кГц [2]. Такое двухкомпонентное устройство передачи аудиосигнала по цепи питания при определенной модернизации может иметь достаточно малые размеры и использоваться для скрытой съема информации в стационарных условиях.

Литература

1. Алейников А.Г., Ровдо М.С., Гайдукевич П.В. Оптимизация устройства обмена информацией по цепи питания для передачи аудиосигнала // Научные вести. 2019. № 1 (6). С. 245–249.

2. Логин В.М., Цырельчук И.Н., Толстая А.И. Аппаратные средства защиты информации: лабораторный практикум. Минск: БГУИР, 2012. 52 с.

ЗАЩИТА ИНФОРМАЦИИ КАК ВАЖНЫЙ АСПЕКТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТИ «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ»

А.В. Ломако

Продолжающийся научно-технический прогресс в области вычислительной техники, информационных технологий и средств инфокоммуникации привел к тому, что реальностью стали кибервойны между государствами [1]. Одним из способов ведения военных действий в такой войне является проникновение в автоматизированные информационные системы (АИС) противника и нанесение ему при этом разного рода ущерба. Реализуется это боевыми командами специально подготовленных высококлассных специалистов (военных хакеров). Стратегия и тактика обороны и нападения в кибервойне – это новое направление военной науки. Для минимизации потенциальных потерь в подобной войне необходимо создавать такие АИС, которые будут устойчивы к атакам хакеров разного рода.

Изложенное выше обусловливает особую важность учета вопросов защиты информации при подготовке специалистов по специальности 1-53 01 02 «Автоматизированные системы обработки информации» (АСОИ) в соответствии с требованиями образовательного стандарта. Поколение 3+ данного стандарта вступает в действие в нашей стране с 2021 года. Вопросы защиты информации в рамках специальности АСОИ были важны и раньше, но сейчас их значимость существенно возросла. Имеются 4 основные обеспечивающие подсистемы АИС, при реализации которых защита информации является актуальной и важной задачей: это организационное, информационное, программное и техническое обеспечение АИС. Анализ учебного плана специальности показывает, что, как минимум, в 17 учебных дисциплинах плана («Базы данных», «Проектирование автоматизированных систем», «Аппаратно-программное обеспечение ЭВМ и сетей», «Администрирование и программирование распределенных приложений», «Интернет технологии и веб-программирование» и др.) должна рассматриваться эта задача, чтобы студенты получили знания, навыки и умения, необходимые для ее решения. Также в учебный план включена профильная для рассматриваемой задачи дисциплина «Основы информационной безопасности», которая, наряду с другими должна дать студентам специальную компетенцию: «Обеспечивать безопасность информации с учетом способов ее представления и модели нарушителя».

Литература

1. Савин Л. Стрелы кентавра. Кибервойна по-американски. М.: ЛитРес, 2020. 590 с.

ОПРЕДЕЛЕНИЕ КОЭФФИЦИЕНТА ПОТЕРЬ НА ПРОХОЖДЕНИЕ В ИМПЕДАНСНЫХ ТРУБКАХ

Д.М. Лютыч

На данный момент в мире наблюдается растущее внимания к проблемам защиты конфиденциальных переговоров. На фоне данной проблемы вопросы проектирования специальных конструкций становятся более значимыми для производителей, а, следовательно, значимыми становятся вопросы акустического испытания материалов.

Для создания требуемой акустической среды необходима информация об акустических характеристиках ее материалов. Архитекторы, проектировщики и инженеры определяют вклад материалов в общие свойства среды, такие как поглощение, отражение, импеданс, адмитанс и потерю при передаче, проводя испытания их акустических характеристик. Эффективные испытания материалов должны быть стабильными и точными; кроме того, необходимо иметь возможность обновлять прогнозные модели, экспортируя в них получаемые данные.

Звукоизолирующие характеристики разрабатываемых материалов и конструкций невозможно предсказать с высокой точностью без проведения испытаний. Поэтому остро стоит проблема определения их акустических характеристик и создания инновационных методов оценки звукоизоляции.

Суть данного метода такова: имеется некая трубка, в одном конце которой устанавливается источник звука, в другом конце – образец материала, акустические параметры которого необходимо рассчитать. Источник звука, функции которого выполняет динамик, производит генерацию широкополосных постоянных произвольных звуковых волн. Данные волны распространяются как плоские в трубе, попадают на образец и отражаются. Происходит суперпозиция волн, вследствие которой возникает интерференционная картина стоячих волн. Следовательно, измеряя давление звука в двух фиксированных местах, и вычисляя комплексную передаточную функцию с помощью двухканального цифрового частотного анализатора, можно определить необходимые параметры.

Следует отметить, что используемый частотный диапазон зависит от диаметра трубки и расстояния между микрофонами.

АНАЛИЗ МЕТОДА ЧЕТЫРЕХ МИКРОФОНОВ ДЛЯ ИЗМЕРЕНИЯ КОЭФФИЦИЕНТА ПОТЕРЬ НА ПРОХОЖДЕНИЕ В ИМПЕДАНСНОЙ ТРУБКЕ

Д.М. Лютыч, С.Н. Петров

Из-за растущего внимания к проблемам защиты конфиденциальных переговоров, вопросы проектирования специальных конструкций становятся более значимыми для производителей, а, следовательно, значимыми становятся вопросы акустического испытания материалов. Например, важно спрогнозировать влияние материалов на свойства конструкции на ранней стадии разработки. За последние 20 лет метод четырех микрофоном заменил традиционный метод стоячей волны в качестве предпочтительного метода измерения коэффициента потерь на прохождение. Данный метод позволяет получать результаты измерения с более высокой разрешающей способностью. Быстрое тестирование позволяет проводить большее количество измерений, что приводит персонал к уверенности в результатах. Существует ряд вопросов связанных с неопределенностью конечных результатов. Стандарты ISO 10534-2:1998 и ASTM E1050-10 содержат предложения по проведению высококачественных измерений, но не содержат подробностей, необходимых новым пользователям для начала работы. Измерение коэффициента потерь на прохождение затруднено по ряду причин. Фундаментальная проблема заключается в том, что нет эталонного материала, с которым можно было бы сравнить результаты. Эта проблема осложняется тем фактом, что существуют различия в изготовлении звукопоглощающих материалов. Стоит учесть, что подготовка и монтаж образцов вносят дополнительные изменения в результаты измерения, также отсутствие подготовки персонала зачастую приводят к запутанным и противоречивым результатам.

Существуют дополнительные неопределенности, связанные с измерением коэффициента потерь на прохождение. К ним относятся: неопределенность, когда

коэффициент низок, особенно на низких частотах; неопределенность, в которой коэффициент имеет резонанс; неопределенность, когда коэффициент приближается к верхнему пределу частоты измерения.

Как мы видим, метод четырех микрофонов – это простой способ измерений коэффициента потерь на прохождение материалов. Однако он может обманчиво простым, когда дело доходит до проведения эффективных точных измерений. Пользователи должны обратить внимание на ряд факторов, связанных с подготовкой образцов. Также стоит подчеркнуть, что одно выборочное измерение ничего не говорит о достоверности. В качестве решения проблемы уменьшения неопределенности предлагается вырезать несколько идентичных образцов из листа материала, чтобы получить надежный результат.

ОСОБЕННОСТИ ВНЕДРЕНИЯ НОРМАТИВНО-ПРАВОВЫХ АКТОВ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ГОСУДАРСТВЕННЫХ ПРЕДПРИЯТИЯХ

А.М. Мажейко

Создание системы защиты информации любой организации начинается с разработки политики информационной безопасности. В государственных предприятиях как правило наиболее оптимальным способом разработки является внедрение локальных нормативно-правовых актов, разработанных на основе требований законодательства, а также требований и рекомендаций государственного органа, осуществляющему регулирование сферой защиты информации. Данный способ имеет преимущества по сравнению с вариантом, когда разработку политики информационной безопасности поручают сторонним организациям, специализирующимся в сфере защиты информации. В данном случае государственные предприятия экономят значительные финансовые ресурсы на разработку политики, а также имеют возможность более конструктивно встроить требования безопасности в собственные бизнес-процессы.

Основой для разработки политики безопасности в Беларуси могут стать Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [1], Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в сфере защиты информации» [2] и приказ оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [3].

Однако существуют и недостатки, которые могут быть допущены руководством и работниками такого государственного предприятия при внедрении политики информационной безопасности. Создание локальных нормативно-правовых актов является лишь первым шагом. На втором шаге необходимо выполнить аудит информационной безопасности согласно принятой политике. Практика показывает, что после внедрения актов и ознакомления с ними работников существуют факты инцидентов информационной безопасности. Таким образом? создание политики информационной безопасности на основе вышеназванных документов является простым и дешевым инструментом, однако требующим последующего контроля за исполнением требований по защите информации государственного предприятия.

Литература

1. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Республики Беларусь, 10 ноября 2008 г., № 455-З // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H10800455. – Дата доступа: 28.04.2021.

2. О совершенствовании государственного регулирования в области защиты информации [Электронный ресурс]: 9 декабря 2019 г., Указ Президента Республики Беларусь № 449 // Официальный интернет портал Президента Республики Беларусь. – Режим доступа: https://president.gov.by/bucket/assets/uploads/documents/2019/449uk.pdf. – Дата доступа: 28.04.2021.

3. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс]: Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 20 февраля 2020 г., № 66 // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: https://oac.gov.by/public/content/files/ files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа: 23.04.2021.

СТАНОВЛЕНИЕ И ОБЗОР БЛОКЧЕЙН ТЕХНОЛОГИЙ И ИХ СВЯЗЬ С КРИПТОСИСТЕМАМИ И РАСПРЕДЕЛЕННЫМ РЕЕСТРОМ

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

В работе рассмотрена кратко история появления технологий распределенного реестра (блокчейн технологии) и применения двухключевых криптосистем, обеспечивающих защиту достоверности данных. Дальнейшее развитие новейшей истории рассматривается на примере существующих в Российской Федерации платформ и приложений этих технологий.

1. На базе платформы Мастерчейн существует сервис цифровых банковских гарантий, находится на этапе промышленной эксплуатации.

2. «Сбер» подключил к своей блокчейн-платформе распределенный реестр от Waves Enterprise.

3. Блокчейн-платформа Factorin в области торгового финансирования объявила о выходе на рынок непродовольственной розницы.

4. Касперский» создал систему для государственных выборов через интернет.

5. В «Лаборатории Касперского», команда проекта Polys, разработала систему дистанционного электронного голосования (ДЭГ) «Polys.ГОСТ», которая полностью удовлетворяет требованиям российского законодательства в части применения криптографии для защиты информации [1–8].

Литература

1. ARMONK, (2017). Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on blockchain [Electronic resource]. – Access mode: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss. – Date of access: 20.12.2017.

2. BitFury Group Limited, (2017). Prof of Stake versus Proof of Work, White Paper [Electronic resource]. – Access mode: http://bitfury.com/content/5-whitepapers-research/pos-vs-pow-1.0.2.pdf. – Date of access: 20.12.2017.

3. Dickson, B. (2016). Blockchain has the potential to revolutionize the supply chain. Techcrunch [Electronic resource]. – Access mode: https://techcrunch.com/2016/11/24/. – Date of access: 20.12.2017.

4. Raval S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O`reilly, Sebastopol, California, 2016.

5. Gilbert, D. (2016). Blockchain Technology Could Help Solve $75 Billion Counterfeit Drug Problem. Ibtimes [Electronic resource]. – Access mode: http://www.ibtimes.com. – Date of access: 20.12.2017.

6. Houy, N., (2016). The Bitcoin Mining Game. Ledger. pp. 151 [Electronic resource]. – Access mode: http://www.ledgerjournal.org/ojs/index.php/ledger/article. – Date of access: 20.12.2017.

7. Robinson, A. (2016). What is Blockchain Technology, and What Is Its Potential Impact on the Supply Chain? (online) Cerasis [Electronic resource]. – Access mode: http://cerasis.com/2016/06/29/blockchain-technology/. – Date of access: 20.12.2017.

8. Walch A. The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk // Journal of Legislation and Public Policy. 2016. Vol. 18 (837). P. 851–852.

ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛАБОРАТОРИЙ ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Макатерчик, В.В. Маликов

Проведение экспериментальных исследований в области информационной безопасности сопряжено с наличием следующих затруднений [1]:

- наличие изолированной и не задействованной в бизнес-процессах компьютерной сети с большим числом разнотипного сетевого оборудования и сетевых узлов максимально имитирующее реальный сетевой дизайн;
- воспроизводимость условий проведения экспериментов;
- исключение внешних, не задекларированных воздействий на нее.

Одним из решений данной проблемы является создание виртуальных лабораторий для проведения экспериментальных исследований в области информационной безопасности.

Построение таких лабораторий возможно несколькими способами [2]:

- использование виртуальной среды операционной системы (ОС) отдельной ПЭВМ;
- использование облачной виртуальной среды;
- гибридные решения;
- использование готовых решений.

По результатам экспериментальной проверки наиболее гибким является использование виртуальной среды ОС на облачной PaaS.

Литература

1. Хочешь мира – готовься к войне или зачем нужен киберполигон. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/512874.php. – Дата доступа: 25.04.2021.

2. Виртуальный полигон. Делаем лабораторию сетевого хакера – «Хакер» [Электронный ресурс]. – Режим доступа: https://xakep.ru/2020/06/18/virtual-lab/. – Дата доступа: 25.04.2021.

ТЕСТИРОВАНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПОЧТОВЫХ СЕРВИСОВ ОТ СКАНИРОВАНИЯ ВНЕШНИХ E-MAIL ТРЕКЕРОВ

В.В. Маликов, А.В. Макатерчик

Возможности дистанционных сервисов на основе информационно-коммуникационных технологий (ИКТ) позволяют существенно снизить издержки организаций при значительном росте качества/эффективности предоставляемых услуг/продуктов. Массовый переход на использование дистанционных сервисов на основе ИКТ позволил обеспечивать потребности граждан, а также изменил фокус внимания злоумышленников.

Информация, полученная на основе технологий сканирования внешних e-mail трекеров может быть использована для проведения как легитимных, так и не легитимных операций.

Авторами проведено исследование уровня эффективности защиты 4-х почтовых сервисов (gmail.com, yandex.by, tut.by, mail.ru) от технологий сканирования 3-х внешних e-mail трекеров (mailtracking.com, didtheyreadit.com, getnotify.com). Проведенное авторами исследование осуществлялось строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий (fair use/fair dealing).

В ходе исследования оценивалась потенциальная возможность сканирования/извлечения информации по работе почтового сервиса на основе 20 параметров/показателей, например, таких как:

- дата и время каждого открытия/прочтения/переадресации письма;
- IP-адреса/порты получателей письма, а также имя интернет-провайдера;
- физическое местонахождение (город/страна) получателя (или его интернет-провайдера);
- переходы по URL-адресам вложений в письмо (дата/время/URL-адрес);
- браузер/программное обеспечение электронного почтового сервиса, используемого получателем и т.д.

Проведенное исследование показало, что из заданных 20 параметров / показателей сканирования / извлечения информации по работе почтового сервиса возможно верифицированное извлечение от 5 до 12 параметров/показателей.

ЗАЩИТА РЕЧЕВОГО СИГНАЛА В РАДИОКАНАЛЕ

А.И. Митюхин

В работе рассматривается решение задачи технической зашиты сигнала речи в радиоканале с выбранным значением ширины полосы пропускания в сечении радиотракт –демодулятор. Анализируется технический метод, обеспечивающий энергетическую и структурную скрытность кодированного сигнала речи в специальных радиолиниях. Требование ограничения полосы частот радиолинии определяет минимальное значение ширины спектра модулирующего кода, вид ФМ-модуляции, значения нестабильности частот задающих кварцевых генераторов кодеков и несущего колебания. С учетом заданного технического ограничения, получения на выходе декодера необходимого значения вероятности ошибки на информационный бит или степени разборчивости речи, предлагаемая техническая защита речи реализуется на основе трех подходов: временного, спектрального и энергетического. Временная составляющая связана с уменьшением времени активного присутствия в радиоканале. В этом случае решение задачи радиоэлектронного обнаружения сигнала пассивными

средствами наблюдения и несанкционированный доступ к информации усложняется [1]. Начальный этап обработки включает в себя запись речи в реальном времени и разбиение полученного цифрового сигнала на последовательные фрагменты. Уменьшение времени передачи информации достигается за счет: проведения процесса декорреляции (эффективного спектрального и энтропийного кодирования) [2]; передачи предварительно записанных цифровых эквивалентов фрагментов речи с высокой скоростью. Энергетическая и структурная составляющие скрытности связаны с формированием несистематических слов низкоскоростного шумоподобного кода с изменяющимися через определенный временной интервал, задающими код, полиномами. В этом случае неопределенность относительно актуальной формы полинома, равномерное распределением энергии сигнала в полосе радиоканала приводит к уменьшению его спектральной плотности мощности и тем самым к энергетической и структурной скрытности передачи речи. Приводится оценка предельно возможного значения скорости передачи речи с заданным отношением сигнал/шум по мощности на выходе радиоканала.

Литература

1. Ипатов В. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. – Москва: Техносфера, 2007.

2. Митюхин А.И. Кодирование и сжатие сегментированного изображения // Кодирование и цифровая обработка сигналов в инфокоммуникациях: материалы междунар. науч.-практ. конф. Минск, 4 апреля 2019 г. С. 61–65.

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПЕРЕНОСА НОСИТЕЛЕЙ ЗАРЯДА В ГЕТЕРОСТРУКТУРНЫХ ПРИБОРАХ С ИСПОЛЬЗОВАНИЕМ ГРАФЕНА И ЕГО МОДИФИКАЦИЙ

В.В. Муравьев, В.Н. Мищенко

Рассмотрены вопросы моделирования процессов переноса носителей заряда в гетероструктурных приборах с использованием графена и его модификаций. Высокое значение подвижности электронов, высокая теплопроводность и ряд других положительных свойств делают графен перспективным материалом для использования в полупроводниковых приборах и микросхемах. Однако прямое использование графена в конструкциях полевых транзисторов и других приборов затруднено из-за ряда особенностей этого материала, главной из которых является отсутствие зазора между зоной проводимости и валентной зоной, что не позволяет реализовать эффективное переключение такого рода структур и способствует появлению ряда других отрицательных свойств. Для устранения отмеченных недостатков графена используется ряд способов коррекции его свойств, главные из которых заключаются в формировании гетероструктур, а также в создании модифицированных графеновых структур, когда в слой графена добавляются атомы других химических элементов, например, атомы водорода, фтора и т.д. Для анализа новых гетероструктурных приборов с использованием графена и атомов водорода и фтора выполнено моделирование их свойств из первых принципов (ab-initio) с применением программного комплекса Quantum Espresso. При моделировании в рамках теории функционала электронной плотности с использованием обменно-корреляционных функционалов вида PBE (Perdew-Burke-Ernzerhof) были получены значения основных электрофизических параметров исследуемых структур. Применение отмеченного подхода позволит создать полупроводниковые приборы с регулируемым зазором между зоной проводимости

и валентной зоной и соответственно с более высокими коммутационными и выходными характеристиками. Реализация гетероструктурных приборов с использованием графена и его модификаций позволит получить новые устройства, которые найдут широкое применение в системах приема, усиления и обработки сигналов в диапазонах СВЧ и КВЧ.

ЛАБОРАТОРНЫЕ РАБОТЫ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

В.Н. Мухаметов, Н.Л. Боброва

Использование сервиса IaaS (Infrastructure as a Service, Инфраструктура как сервис) с арендой ресурсов в Public Cloud (публичном облаке) позволяет обеспечить каждого студента качественным, унифицированным и в то же время уникальным для каждой лабораторной работы рабочим местом, виртуальной машиной (ВМ). Облачный провайдер, предоставляющий услуги IaaS, обычно обеспечивает возможность быстрого развертывания из одного образа (Image) нужного количества одинаковых экземпляров (Instances) виртуальных машин требуемого типа, с предустановленным программным обеспечением. Возможна предварительная подготовка собственного образа на базе предоставляемого [1, 2]. Таким образом, можно создать уникальный образ ВМ для каждой лабораторной работы. Если повторяющееся создание образа перед каждым циклом лабораторных работ требует больших временных затрат, его можно сохранять. Авторы имеют опыт как создания образа непосредственно перед проведением занятия с последующим удалением, так и хранения образов для их повторного использования. Следует отметить, что использование ВМ в публичном облаке в качестве рабочего места при проведении дистанционной лабораторной работы позволяет одновременно работать всей группе, а не подгруппе до 12–15 студентов (если методика проведения занятия позволяет преподавателю работать с большим количеством студентов). Методическая основа проведения лабораторных работ с использованием облачных сервисов IaaS имеет мало отличий от проведения лабораторных работ в компьютерных классах учебного заведения. Методики проведения лабораторных работ зависят от используемого программного обеспечения, установленного на рабочих местах (персональных компьютерах) в соответствии со спецификой каждой лабораторной работы.

Литература

1. Мухаметов В.Н., Полубок В.А. Опыт проведения лабораторной работы в облачном сервисе «Amazon Web Services» // «Высшее техническое образование: проблемы и пути развития»: материалы VI междунар. науч.-метод. конф., Минск, ноябрь 2012. С. 260–261.

2. Мухаметов В.Н., Боброва Н.Л. Опыт проведения лабораторной работы в облачном сервисе «Microsoft Windows Azure» // «Высшее техническое образование: проблемы и пути развития»: материалы VI междунар. науч.-метод. конф., Минск, ноябрь 2012. С. 259–260.

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ КАК ОБЪЕКТЫ ПРАВА ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

А.Э. Павлович

При отнесении средств и методов защиты информации к объектам права промышленной собственности применяют индексы Международной патентной

классификации (МПК), например: B 44F 1/12 – в отношении использования антистоксовых люминофоров, чувствительных к воздействию ИК – излучения; G 06K 9/00 и G 09C 5/00 – в отношении применения растровых структур, включающих в себя закодированное полутоновое изображение; G 07D 7/00 – в отношении визуализации скрытых изображений с помощью линейного поляризатора и фазосдвигающей пластинки; G 06F 21/16 – в отношении защиты от подмены электронных документов на вычислительных устройствах; H 04L 9/00 – в отношении управления защитой информации в распределенных системах управления, в том числе для IP-сетей и для сетей с иными протоколами передачи данных; и др. Такие объекты права промышленной собственности могут быть запатентованы, согласно нормативно-правовых актов Республики Беларусь [1] и Российской Федерации [2], как изобретения, полезные модели и промышленные образцы. При государственной экспертизе заявляемых на патентование объектов промышленной собственности к ним предъявляются критерии охраноспособности: для изобретений – новизна, изобретательский уровень и промышленная применимость, для полезных моделей – новизна и промышленная применимость, для промышленных образцов – новизна и оригинальность. Существует режим открытых публикаций запатентованных решений и режим «секретных» объектов промышленной собственности, на которые могут выдаваться патенты без открытой публикации их содержания. Кроме того, такие объекты не патентуются, если принадлежат к нераскрытой информации: государственной, служебной и коммерческой тайне. При этом к ним предъявляются требования по ценности, по доказательствам принадлежности создателям и по применяемым мерам обеспечения конфиденциальности.

Литература

1. Законодательство в сфере промышленной собственности [Электронный ресурс]. – Режим доступа: https://нцис.бел/zakonodatelstvo/promyshlennaya-sobstvennost/. – Дата доступа: 06.05.2021.

2. Документы [Электронный ресурс]. – Режим доступа: https://www1.fips.ru/documents/. – Дата доступа: 06.05.2021.

МЕХАНИЗМЫ ОПЕРАЦИОННЫХ СИСТЕМ ASTRA LINUX ДЛЯ КОНТРОЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

С.И. Павлович

Под безопасностью информационных сетей следует понимать такое их состояние, при котором они защищены от внутренних и внешних угроз, направленных на нарушение свойств конфиденциальности, целостности и/или доступности циркулирующей в рамках них информации. В связи с этим контроль безопасности информационных сетей заключается в периодической реализации оценки указанных свойств их объектов. Такая оценка может проводиться как с помощью специального программного обеспечения, так и с помощью тех механизмов, которые включены в состав используемых в рамках информационных сетей операционных систем. Автором выполнен анализ механизмов операционных систем специального назначения Astra Linux, которые могут быть использованы для контроля безопасности информационных сетей, в рамках которых используются эти системы. Определено, что к таким механизмам относятся следующие.

1. Средства контроля целостности, в частности:

- подсчета контрольных сумм;

- контроля соответствия дистрибутиву;
- регламентного контроля целостности;
- средства проверки электронной подписи.

2. Фильтрация сетевого потока.

3. Контроль подключения съемных носителей.

4. Средства управления протоколированием, в частности:

- утилита fly-admin-viewaudit, применяемая для выборочного просмотра журналов аудита;
- команда getfaud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении файловых объектов;
- команда useraud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении действий пользователей;
- команда psaud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении какого-либо выбранного процесса;
- команда parselog, применяемая для анализа двоичных файлов аудита, записанных с помощью parlogd;
- команды kernlog и userlog, применяемые для анализа двоичных файлов регистрации событий, связанных с функционированием ядра операционной системы и действиями пользователей соответственно;

5. Средства централизованного аудита и протоколирования.

Механизмы, представленные в пп. 1–3, могут быть отнесены к механизмам, реализуемым операционной системой, а механизмы, представленные в пп. 4, 5 – к механизмам, используемым администратором информационной сети.

ТЕХНОЛОГИЯ ИЗГОТОВЛЕНИЯ ТРУДНОВОСПЛАМЕНЯЕМЫХ КОМПОЗИЦИОННЫХ ПОКРЫТИЙ ДЛЯ КОНСТРУКЦИЙ, ПРИМЕНЯЕМЫХ В ЦЕЛЯХ ЭЛЕКТРОМАГНИТНОГО ЭКРАНИРОВАНИЯ ПОМЕЩЕНИЙ

Д.И. Пеньялоса Овальес, М.В. Тумилович

К конструкциям, применяемым в целях электромагнитного экранирования помещений, предъявляются такие требования, как трудновоспламеняемость и низкие значения коэффициента отражения электромагнитного излучения в диапазоне частот побочного электромагнитного излучения радиоэлектронного оборудования, располагаемого внутри таких помещений. Соблюдение первого из указанных требований необходимо для того, чтобы соблюсти требования пожарной безопасности, предъявляемые к помещениям, в которых эксплуатируется радиоэлектронное оборудование. Соблюдение второго из указанных требований необходимо для того, чтобы снизить уровень пассивных электромагнитных помех, формируемых в пределах указанных помещений и оказывающих влияние на эксплуатируемое в них радиоэлектронное оборудование.

В целях обеспечения указанных требований авторами предложено использовать покрытия на основе порошкообразных алюмооксидов в процессе изготовления конструкций для электромагнитного экранирования помещений или в процессе улучшения эксплуатационных свойств таких конструкций. Предложенные покрытия представляют собой композиционные материалы, связующим веществом которых является водоэмульсионный огнезащитный состав или водный раствор силиката натрия, а наполнителем – порошкообразный электрокорунд или глинозем. Объемное соотношение наполнителя и связующего вещества в указанных композиционных материалах составляет 1,0:1,0. Указанные материалы являются трудновоспламеняемыми ввиду того, что их связующее вещество характеризуется соответствующим свойством,

а также ввиду того, что порошкообразные электрокорунд и глинозем являются природными антипиренами.

Установлено, что значения коэффициента отражения электромагнитного излучения в диапазоне частот 0,7…17,0 ГГц указанных материалов, нанесенных слоем толщиной 3,0±1,0 мм на целлюлозные подложки, закрепленные на металлических подложках, изменяются в пределах от –5,0 до –30,0 дБ.

На основе представленных свойств предложенных композиционных покрытий можно сделать вывод о том, что они представляются перспективными для использования в процессе изготовления или совершенствования эксплуатационных свойств конструкций для электромагнитного экранирования помещений.

ТОНКОПЛЕНОЧНЫЕ ТЕХНОЛОГИИ В ПОВЫШЕНИИ НАДЕЖНОСТИ ЭЛЕМЕНТНОЙ БАЗЫ ЭЛЕКТРОННЫХ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Р.В. Пигаль

В работе с использованием источников [1, 2] рассмотрено влияние тонкопленочной технологии на надежность элементной базы электронных устройств обеспечения информационной безопасности и изменение эксплуатационных характеристик конструктивных частей технических изделий. Выполнен анализ применения тонкопленочной технологии для получения гибридно-пленочных микросхем, коммутационных плат микросборок, металлических межсоединений при производстве полупроводниковых микросхем. Установлено, что химическая чистота напыляемых тонких пленок повышает эксплуатационную надежность элементов, а применение тонкопленочных покрытий обеспечивает более высокую коррозионную стойкость конструктивных частей технических изделий, улучшает их механические характеристики, а также способствует подавлению нежелательных электромагнитных излучений и уменьшает уровень наводимых паразитных сигналов, что является важным для электронных устройств защиты информации.

На основе проведенного анализа сделаны выводы о влиянии и значимости технологии тонкопленочного нанесения материалов для повышения надежности элементов и улучшения эксплуатационных характеристик конструктивных частей электронных устройств защиты информации.

Литература

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

2. Seshan, K. Handbook of Thin-Film Deposition Processes and Techniques. Norwich, NY, 2002. 646 p.

МЕТОДИКА ОПТИМИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ДАТА-ЦЕНТРОВ В БАНКОВСКОЙ СФЕРЕ

П.И. Питкевич, Д.Н. Одинец

К дата-центрам банков в Республике Беларусь предъявляются дополнительные требования по защите аппаратных и программных средств, входящих в их состав. Эти требования продиктованы основной спецификой объекта исследования – критичностью систем, размещаемых в дата-центрах [1]. Основной задачей исследования является создание максимально эффективной системы защиты дата-

центров банков от несанкционированного доступа к данным с сохранением максимальной гибкости в работе.

В ходе создания методики были проанализированы современные решения по информационной безопасности, которые соответствуют заявленным критериям поставленной задачи [2], обоснованы основные элементы, которые включает себя дата-центр банка: платформы виртуализации (VMware vSphere, Microsoft Hyper-V, Citrix XenServer или KVM); инфраструктуры хранения данных – СХД разных типов и файловые сервера; сетевая инфраструктура, обеспечивающая связь между компонентами ЦОД, а также виртуальные сети [3]. Возможные варианты виртуализации проанализированы в подготовленной тестовой среде. В результате экспериментальных исследований выбраны те варианты виртуализации, которые максимально соответствуют заявленным критериям к безопасности, спроектирована максимально гибкая система защиты дата-центра для банков, обоснованы аспекты защиты от несанкционированного доступа к аппаратным ресурсам дата-центра, а также описаны системы защиты данных.

Предложенная методика позволила создать максимально гибкую и динамичную систему, которая удовлетворяет всем параметрам служб информационной безопасности и сохраняет при этом заданную производительность. Разработанная на основе методики система защиты дата-центров, удовлетворяет всем критериям, предъявляемым к банкам Республики Беларусь.

Литература

1. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Менеджмент рисков информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.nbrb.by/legislation/documents/ ttpib_4_1-2020.pdf. – Дата доступа: 12.04.2021.

2. Гасанов Э.Э., Кудрявцев В.Б. Интеллектуальные системы. Теория хранения и поиска информации: учебник для вузов. Москва: Издательство Юрайт, 2021. 271 с.

3. Митропольский Ю.И. Мультиархитектурные вычислительные суперсистемы. Перспективы развития. М.: Техносфера, 2020. 146 с.

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.А. Поплавская

Одним из важнейших условий дальнейшего прогрессивного развития Республики Беларусь является обеспечение информационной безопасности. В условиях рекордной цифровизации большинства отраслей республики и эпидемии коронавируса с вызванным ею режимом удаленной работы, информационная сфера приобретает доминирующее значение и порождает всеобъемлющее влияние на происходящие процессы в республике. Трендом защиты информации АСУ ТП в этом году становится многоступенчатый подход для создания злоумышленникам многоресурсной траты, сегментирование ИТ и ОТ-сети, непрерывный мониторинга сети, защита рабочих станций и серверов АСУ ТП, безопасность программной среды.

В 2020 г. процветало вымогательское ПО, атаки на индивидуальные сети, RDP и VPN, использование пандемии с целью проникновения в целевые системы, прогресс атак, спонсируемых внешними государствами, основным супервайзером которых был шпионаж, взломы через API-интерфейсы, атаки на цепочки поставок, применение 5G-устройств в качестве оружия для усовершенствованных атак, нарастание deep fake с целью дезинформации и манипуляции общественным мнением и избежания средств

аутентификации, новые механизмы избежания многофакторной аутентификация MFA, нападение на open-source компоненты.

В 2021 году рост указанных выше видов киберпреступности и количества атак продолжается, в том числе на критические инфраструктуры. Прицел направлен на современные периферийные сетевые среды, в том числе и на квантовые вычисления, применение спутниковых сетей для распространения вредоносных программ, появление вишинга – голосового фишинга. Поэтому особенно важно использовать защитные продукты и решения, отвечающие требованиям времени, внедрять автоматизацию обеспечения информационной безопасности, усиливать аутентификацию удаленных пользователей [1, 2].

Литература

1. Тренды защиты информации АСУ ТП в 2021 году [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/resources/blog/special-project/3-trenda-zaschity-informatsii-asu-tp-v-2021-godu. – Дата доступа: 30.04.2021.

2. Прогноз развития киберугроз и средств защиты [Электронный ресурс]. – Режим доступа: инфhttps://www.anti-malware.ru/analytics/Threats_Analysis/2021-Cyber-Threats-and-Information-Security-Forecast. – Дата доступа: 01.05.2021.

ФОТОЧУВСТВИТЕЛЬНЫЙ ПРИЕМНИК НА ОСНОВЕ КОНТАКТА ШОТТКИ МЕЖДУ ПОЛУПРОВОДНИКОМ И ГРАФЕНОМ

С.Л. Прищепа, И.В. Комиссаров, А.Л. Данилюк, Н.Г. Ковальчук, А.А. Головач, М.М. Михалик, Ю.М. Кукуть, Е.А. Дронина

Контакты графен-полупроводник являются перспективными гибридными структурами для оптоэлектроники. Полупроводник при этом выполняет функцию источника неравновесных носителей заряда, а графен – прозрачного электрода, аккумулирующего индуцированные вследствие оптического излучения носители заряда. При этом, в силу рекордных значений подвижности носителей заряда в графене, данные контакты обладают высоким быстродействием [1]. В данной работе сообщается об изучении параметров таких гетеропереходов. Контакты были сформированы нанесением выращенного на медной подложке методом химического парофазного осаждения графена на подложки из кремния с уровнем легирования 10^{16} $см^{-3}$ толщиной не более 20 мкм [2]. Перед нанесением естественный слой оксида SiO_2 стравливался. Проводилось измерение вольт-амперных характеристик (ВАХ) в темновом режиме и при различных мощностях облучения. Исследования свойств проводились в двух режимах, – вентильном (при отсутствии источника питания во внешней цепи) и фотодиодном (на фотодиод подавалось напряжение от внешнего источника). Кроме того, с использованием трехэлектродной схемы исследовалось изменение ВАХ при подаче напряжения на подложку (режим транзистора). В результате проведенных исследований были определены основные параметры фотодиода: фактор идеальности ВАХ, напряжение лавинного пробоя, величина барьера Шоттки, ток утечки.

Литература

1. Konstantatos G. // Nature Commun. 2018. Vol. 9. P. 5266–5269.

2. Scagliotti M., Salvato M., De Crescenzi M., Kovalchuk N.G., Komissarov I.V., Prischepa S.L. // Carbon. 2019. Vol. 152. P. 543–651.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОЦЕССЕ ОБУЧЕНИЯ МАТЕМАТИКЕ СТУДЕНТОВ ТЕХНИЧЕСКИХ ВУЗОВ

З.Н. Примичева

В настоящее время реформирование системы образования привело к тому, что роль информационных технологий в ней возрасла. Это обусловлено тем, что с помощью данных технологий педагоги могут качественно изменять методы и организационные формы работы, развивать индивидуальные особенности обучаемых.

Использование информационных технологий в процессе обучения позволяет развивать у студента технического вуза умение самостоятельно приобретать, обобщать и актуализировать знания, работать с информацией и применять ее для решения поставленных задач. Применение информационных технологий можно осуществлять на различных этапах обучения: на лекциях при объяснении нового материала с использованием презентации, созданной в программе PowerPoint; на практических занятиях при проверке домашнего задания для закрепления и повторения материала с использованием тестов; при проведении самостоятельных и контрольных работ, коллоквиумов; в исследовательской деятельности студентов.

Поскольку современная математическая наука является мощным инструментом анализа и прогнозирования технических и технологических процессов, природных явлений и общественных ситуаций, необходимо включать в учебные программы базовой математической подготовки будущих специалистов новые разделы математики путем уплотнения стандартного курса математики, перераспределения академических часов между темами внутри самого курса, использования новых специальных курсов.

Новым и перспективным направлением осуществления профессиональной подготовки студентов технических вузов является использование в процессе обучения математике компьютерных математических систем, в частности системы Mathematica. Однако следует отметить, что компьютерная математика не способна заменить традиционную математику, поскольку любая компьютерная программа имеет свои границы применимости и для ее написания необходимо провести предварительный анализ решаемой задачи, опираясь на математические, физические, экономические закономерности.

Таким образом, использование информационных технологий в процессе обучения позволяет педагогу в наглядной и доступной форме излагать материал, проводить контролируемую самостоятельную работу студентов, поднимать уровень успеваемости и сокращать время, отведенное на объяснение материала.

АСПЕКТЫ ВЫБОРА СГЛАЖИВАЮЩЕГО ФИЛЬТРА ДЛЯ АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАТЕЛЯ

П.Л. Прудников, Г.А. Власова

Сглаживающие фильтры нижних частот широко применяются для коррекции высокочастотных шумов [1, 2]. При выборе фильтра нижних частот (ФНЧ) на практике руководствуются такими его параметрами, как коэффициент передачи в полосе пропускания, коэффициент передачи в полосе задерживания, неравномерность в полосе пропускания, применимая для фильтров Чебышева, и частота среза, которая определяет границу полосы пропускания фильтра. Для уменьшения искажений полезного сигнала из-за неравномерности коэффициента передачи фильтра частоту среза следует выбирать значительно больше верхней частоты в спектре полезного сигнала. Так, в [2] рекомендуемая частота среза ФНЧ на порядок выше частоты сигнала.

Однако, следует иметь в виду наличие помех в реальных каналах передачи информации. Для гауссова канала и идеального ФНЧ мощность шума на выходе фильтра прямо пропорциональна частоте среза. Коэффициент пропорциональности равен спектральной плотности мощности шума на входе фильтра. Значение мощности (дисперсии) шума на выходе ФНЧ влияет на вероятность выхода шумовой составляющей за пределы шага квантования. Исходя из этих соображений, для уменьшения мощности шума частоту среза следует выбирать как можно ниже.

Расчет мощности шума на выходе неидеальных фильтров производится путем интегрирования по частоте квадрата модуля коэффициента передачи фильтра, умноженного на значение мощности шума на входе. Вычисления показывают, что в случае применения фильтра Баттерворта с увеличением его порядка мощность шума на выходе быстро снижается, приближаясь к значению мощности шума на выходе идеального фильтра нижних частот. Так, мощность шума на выходе фильтра Баттерворта второго порядка отличается от мощности шума на выходе идеального фильтра всего на 11,07 %. В то время как мощность шума на выходе фильтра Баттерворта первого порядка отличается от мощности шума на выходе идеального фильтра значительно существеннее – на 57,08 %. Поэтому в целях упрощения схемотехнической реализации устройства и его удешевления целесообразно применять в качестве фильтра нижних частот фильтр Баттерворта второго порядка.

Литература

1. Титце У., Шенк К. Полупроводниковая схемотехника. М.: ДМК Пресс, 2008. 942 с.

2. Бейкер Б.К. Частотный подход к проектированию сглаживающего фильтра для АЦП // Электроника+. 2018. № 2. С. 43–45.

МЕТОДИКА АНАЛИЗА УЯЗВИМОСТЕЙ ПРИ ТЕСТИРОВАНИИ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ВЕБ-ПРИЛОЖЕНИЙ

А.Ю. Пузеева

Проведение тестирования на проникновение регулируется стандартами и методиками, которые упорядочивают этапы тестирования, устанавливают последовательность действий для выявления различных угроз и уязвимостей и прочее. Наиболее распространенными методиками на сегодняшний день являются стандарт NIST SP 800-115, OWASP Web Security Testing Guide, методика OSSTMM, стандарт PTES и другие. Методика OSSTMM и стандарты NIST SP 800-115, BSI носят больше теоретический характер, при этом NIST SP 800-115 и BSI фактически являются стандартами стран-разработчиков, которых необходимо придерживаться, проводя тестирование на проникновение в этих странах. Стандарт PTES является практико-ориентированными и содержат широкий набор технических рекомендаций и конкретных уязвимостей, которые необходимо проверять в ходе тестирования на проникновение. Методика OWASP является узконаправленной на тестирование веб-приложений. Подробное изучения и анализ вышеперечисленных методик позволил приступить к разработке методики анализа уязвимостей при тестировании безопасности инфраструктуры веб-приложений. Данная методика включает следующие этапы: выбор перечня инструментов для проведения тестирования, настройка виртуальной среды; сбор информации об тестируемом приложении, а именно сканирование портов, исследование видимого контента и др.; анализ уязвимостей веб-приложения, посредством тестирования приложения на возможность реализации инъекций (SQL, SOAP, LDAP, XPATH и т.д.), XSS-уязвимостей, XML-сущностей и др.;

анализ механизмов аутентификации и авторизации пользователей; проверка найденных уязвимостей путем попытки их эксплуатации; составления отчета о результатах тестирования.

Данная методика была апробирована на веб-приложении Railsgoat, в результате чего был получен подробный отчет, содержащий не только информацию о выявленных уязвимостях, но и подробные рекомендации по их ликвидации. Таким образом, данную методику можно рекомендовать для тестирования безопасности инфраструктуры клиент-серверных веб-приложений, использующих различные технологии и построенные на основе различных языков программирования [1–4].

Литература

1. Technical Guide to Information Security Testing and Assessment [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf – Дата доступа: 29.04.2021.

2. OWASP Web Security Testing Guide [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-web-security-testing-guide/v42/ – Дата доступа: 29.04.2021.

3. The Open Source Security Testing Methodology Manual [Электронный ресурс]. – Режим доступа: https://www.isecom.org/OSSTMM.3.pdf – Дата доступа: 29.04.2021.

4. PTES Technical Guidelines [Электронный ресурс]. – Режим доступа: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines – Дата доступа: 29.04.2021.

СНИЖЕНИЕ РАДИОЛОКАЦИОННОЙ ЗАМЕТНОСТИ ТЕХНИЧЕСКИХ ОБЪЕКТОВ В УСЛОВИЯХ ДЕЙСТВИЯ ВЫСОКИХ ТЕМПЕРАТУР

Т.А. Пулко, В.С. Колбун, Н.В. Насонова

Предложены покрытия на основе алюмооксидной керамики, для снижения радиолокационной заметности технических объектов, функционирующих в условиях высоких температур. Получены электромагнитные характеристики образцов температуростойких радиопоглощающих покрытий на основе диэлектрической алюмооксидной матрицы, легированной следующими материалами: жаропрочный сплав $Fe_{69}Cr_{25}Al_6$, соединениями Ti-Al, Fe-Al, Ti_3SiC_2, Ni-Al, $MoSi_2$, в диапазоне концентраций 10–50 мас. %.

Исследуемые образцы покрытий $Al_2O_3/Fe_{69}Cr_{25}Al_6$ обладают свойствами поглощения электромагнитных волн, что характеризуется уровнем ослабления и коэффициентом отражения ЭМИ в диапазоне частот 8–12 ГГц. Коэффициент отражения находится в интервале –0,75…–2,2 дБ, а ослабление ЭМИ составляет от 2,2 до 8,3 дБ. Изменение концентрации наполнителя в образцах незначительно влияет на коэффициент отражения, значения которого находятся в интервале –0,7…–2,5 дБ. Наиболее равномерная частотная зависимость наблюдается при максимальной концентрации наполнителя. Следовательно, рост концентрации наполнителя приводит к увеличению доли поглощенной энергии ЭМИ в диапазоне 8–12 ГГц. Коэффициент отражения ЭМИ образцами на основе $MoSi_2$ составляет –0,5…–1,6 дБ. Увеличение концентрации приводит к увеличению коэффициента отражения и, соответственно, к увеличению экранирующих свойств композиционного порошкового материала в диапазоне 8–12 ГГц. Экранирующие характеристики исследуемых образцов Al_2O_3/TiAl характеризуются в диапазоне частот 8–12 ГГц коэффициентом отражения $S11$ –0,05…–1,8 дБ и коэффициентом передачи $S21$ –2,0…–6,8 дБ с минимальными значениями на частотах 11,4 ГГц и 12,0 ГГц.

Показано, что воздействие температур (до 1700 °С) на композиционные покрытия позволяет сформировать качественные покрытия, обладающие высокими механическими характеристиками – прочностью (9,9–10,8), твердостью (наибольшая твердость получена на покрытиях из композиций на основе интерметаллида FeAl (66,2 HRA) и MAX-фазы Ti_3SiC_2 (61,8 HRA), наименьшая – на композиции с интерметаллидом TiAl (41,6 HRA)) и микротвердостью (наибольшую микротвердость Hμ = 400 – 469 кгс/мм^2 показывают зоны насыщенные MAX-фазой Ti_3AlC_2 и карбидом титана TiC), невысокой шероховатостью (12,9–21,5 для различных материалов).

ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ ВОЗДЕЙСТВИЯ МОЩНЫХ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ

Г.А. Пухир, Н.В. Насонова

Воздействие сверхкоротких электромагнитных импульсов большой мощности (как природного, так и искусственного происхождения) на низковольтные сети, приводит не только к выходу из строя электроустановок, кабелей, распределительных щитов, но также и к повреждению оконечного оборудования и сбоям в его работе. Это связано с насыщенностью современных зданий и сооружений информационной, телекоммуникационной и другой цифровой техникой, имеющей очень низкий уровень защиты от импульсных перенапряжений и помех. Подобные сбои могут привести к крупным экологическим катастрофам и большим человеческим жертвам, способны причинить значительный материальный ущерб из-за сбоев систем управления автоматических производственных линий, неустойчивой работы линий связи, потери информации в компьютерах и т. д. [1].

На практике, воздействие сверхкоротких электромагнитных импульсов на телекоммуникационные системы приводит к потере (искажению) информации, ложным срабатываниям систем охранной, пожарной и др. сигнализаций, сбоям в работе оборудования, блокирование каналов передачи информации (как проводных, так и беспроводных), сбоям и отказам электронных устройств [2].

Все это вызывает необходимость проведения соответствующих защитных мероприятий. С целью снижения нежелательного воздействия ЭМИ на радиоэлектронные устройства и человеческий организм разработаны нормы предельно допустимых уровней излучения технических средств [3]. Комплексный подход в защите информации актуален и в данном направлении. Он предусматривает весь возможный спектр мероприятий от использования более надежных микросхем, выдерживающих большее напряжение и токи, предохранителей и ограничительных устройств, до резервного копирования программных продуктов и информационных активов, позволяющего ускорить восстановление после сбоев. К дополнительным техническим мерам можно отнести фильтрацию опасных сигналов и экранирование электромагнитного излучения. Последнее, с учетом поглощаемой мощности излучения сверхкороткого электромагнитного импульса, можно считать определяющим.

Литература

1. Чаплыгин А.В., Гребенкин А.В. Электромагнитная совместимость электронных технических средств. Реальная необходимость или необходимая реальность // Алгоритм безопасности. 2017. № 5. С. 54–57.

2. Акбашев Б.Б., Еряшев Д.И., Корнев А.Н. Механизм деструктивного воздействия мощных сверхширокополосных импульсов на радиоэлектронные системы // Технологии ЭМС. 2011. № 2 (37). С. 21–25.

3. МЭК 61000-2-13. Electromagnetic compatibility (EMC) – Part 2-3: Environment – High-power electromagnetic (HPEM) environments – radiated and conducted», 2004. P. 16.

БЕЗОПАСНОСТЬ КООРДИНАЦИИ АГЕНТОВ В СИСТЕМАХ УПРАВЛЕНИЯ

А.К. Пушкина

В системах координации взаимодействующих агентов регулярно возникает потребность решения задач о динамическом назначении свободным агентам новых возникающих задач [1], по мере их поступления, и реоптимизации существующих решений о назначении с учетом текущего состояния. Задачи координации агентов чаще всего сводятся к известным задачам дискретной оптимизации. Важно учитывать реальные отношений между агентами и задачами, что приводит к экспоненциальной сложности алгоритма формирования их оптимального паросочетания и часто ограничивает возможности обеспечения безопасности систем управления.

Используя понятия наиболее раннего и позднего срока начала исполнения задач, появляется возможность проводить жадный упреждающий поиска окончательного назначения. Предполагаются операции реализации стандартных функциональных требований безопасности с работой процедур оптимизации управления на интервалах ожидания событий. Такая процедура назначения дополняет граф оптимального паросочетания при поступлении новых заявок, а время реакции на заявку определяется сложностью обработки последней группы заявок.

Безопасность предлагаемой схемы проактивного управления гарантирует формализм рекуррентных сетевых моделей, состояние которых соответствует графу текущего паросочетания с выделением оптимального решения. Переход между состояниями сети реализуется инкрементальными версиями алгоритмов решения линейных задач о назначении, задачи коммивояжера и поиска кратчайших путей на графах. На параметры таких задач проецируются особенности процессов обслуживания, включая векторные критерии и разнообразные отношения вложенности. Таким образом, процедуры поиска очередного решения оказываются строго привязанными во времени к этапам контроля условий целостности и безопасности.

Литература

1. Gerkey B.P., Mataric M.J. A Formal Analysis and Taxonomy of Task Allocation in Multi Robot Systems // The International Journal of Robotics Research. 2004. Vol. 23, no. 9. P. 939–954.

ИСПОЛЬЗОВАНИЕ ПРОСТРАНСТВЕННО-ЦВЕТОВЫХ ПАРАМЕТРОВ ТЕКСТОВЫХ ДОКУМЕНТОВ-КОНТЕЙНЕРОВ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

М.Г. Савельева

Методы текстовой стеганографии можно разделить на три основные категории: основанные на формате, или синтаксические методы, лингвистические, или основанные на обработке естественного языка, методы, а также основанные на случайной и статистической генерации [1].

В данной работе были рассмотрены методы текстовой стеганографии, использующие в качестве контейнера документы, созданные в программе Microsoft Word. Среди современных синтаксических методов можно выделить следующие: метод непечатаемых символов (заключается во встраивании секретного сообщения в цвет

непечатаемых символов в формате RGB) [2], метод Similar English Font Types (заключается в выборе трех различных похожих шрифтов с последующим кодированием всех букв и пробела как тройки заглавных букв), метод подчеркивания символов (заключается в добавлении невидимых стилей подчеркивания к символам), метод масштабирования символов (заключается в скрытии бит за счет увеличения / уменьшения масштаба текстовых символов на 1%), метод границ предложения (заключается в использовании возможности добавления левых и правых границ к предложению с цветами, которые незаметны пользователю ввиду особенностей строения человеческого глаза), метод границ абзаца (заключается в добавлении левой и правой границы к абзацу и задания им цветов, неотличимых для человека от фонового цвета документа), метод отслеживания изменений (заключается в использовании средств отслеживания изменений документов MS Word при совместном написании).

Исходя из сравнительного анализа перечисленных методов видно, что наибольшей емкостью встраивания обладает метод подчеркивания символов, за ним следует метод масштабирования символов, а наименьшую емкость встраивания имеет метод Similar English Font Types, все методы оказывают небольшое влияние на размер документа, количество невидимых символов составляет лишь небольшую часть от числа всех символов.

Литература

1. Bennett, K. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. cERIAS Tech Report 2004-13 (2004).

2. Шутько Н.П., Урбанович П.П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста // Информационные технологии: материалы 83-й НТК профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4–15 февраля 2019 г. С. 41–43.

ИССЛЕДОВАНИЕ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК БОЛОМЕТРА

В.В. Садченко, И.Ю. Ловшенко

Болометр представляет собой резистивный элемент, сконструированный из материала с очень малой теплоемкостью и большим температурным коэффициентом, чтобы поглощаемое излучение вызывало большое изменение сопротивления. Разработка неохлаждаемых FPA (FPA – Focal Plate Arrays, фокально-плоскостные матрицы) в настоящее время идет в двух направлениях [1]: матрицы для военных и коммерческих устройств высокого класса с максимально возможной производительностью; матрицы для коммерческих устройств с минимально возможной стоимостью. Моделирование и создание таких устройств может представлять значительные трудности, так как необходимо решение целого комплекса задач математической физики (деформации твердого тела, теплопроводности, диффузии, электростатики, гидродинамики и других). Универсальные пакеты конечного элементного анализа, такие, как ANSYS, Algor, Comsol Multiphysics (Femlab) и другие, обеспечивают решение описанных выше задач [2]. Одним из таких инструментов является программный продукт компании Coventor.

Одним из важных параметров для болометра, является устойчивость к механическим напряжениям (внутренним и внешним). Для оценки механической прочности конструктивного решения болометра проведено термомеханическое

моделирование консольных балок выполняющих роль подвеса активной области. Балка состоит из трех слоев: нижний Si_3N_4 (слой 1), NiCr (слой 2), верхний Si_3N_4 (слой 3). Ширина балки равна 1 мкм. Балка опирается на алюминиевую опору квадратного сечения (1×1 мкм) высотой 3 мкм. Длина фрагмента без опоры – 15 мкм. Для исследования выбраны две конструкции, отличающиеся друг от друга толщиной слоев: для структуры № 1 толщины слоев 1–3 равны 1 мкм, для структуры № 2 – 0,15 мкм. Деформации консольных балок вдоль оси *OZ* (плоскостность) оценена с помощью термомеханического анализа в установившемся режиме, при котором конструкции нагреваются до температуры $T = 300$ K. Внутренние механические напряжения материалов составляют для Si_3N_4 200 МПа, для NiCr 1 ГПа.

По результатам моделирования установлено, что наибольшее отклонение по оси Z (почти 12 нм) соответствует конструкции №2. Происходит изменение направления изгиба с учетом внутренних механических напряжений и без него.

Для определения зависимости величины отклонения по оси Z от внутренних механических напряжений в материалах было проведено моделирование Конструкции № 2 с изменением внутреннего механического напряжения в слоях Si_3N_4 от –200 до 200 Мпа с шагом в 10 Мпа (для NiCr механическое напряжение составляет 1 ГПа). Наблюдается линейная зависимость величины отклонения консольной балки по оси Z от внутренних механических напряжений в слоях Si_3N_4 и NiCr.

Исследования выполняются при финансовой поддержке и в рамках решения задач государственной программы научных исследований «Фотоника и электроника для инноваций» (задание 3.4).

Литература

1. Hübers H.-W. Terahertz heterodyne receivers // IEEE J. Select. Topics Quant. Electron. 2008. Vol. 14. P. 378–391.

2. Коловский А.А., Левицкий А.А., Маринушкин П.С. Компьютерное моделирование компонентов МЭМС: научная статья // Проблемы разработки перспективных микро- и наноэлектронных систем. 2008. № 1. С. 398–401.

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОЛЯРНЫХ КОДОВ

С.Б. Саломатин, М.А. Алисеенко

Полярные коды достигают граничных параметров и используются в системе сотовой связи 5G [1]. Представляет интерес рассмотреть особенности полярных кодов для защиты канала передачи данных [2].

Один из возможных методов защите может быть основан на методике сокрытия порождающей матрицы полярных кодов, структура которой зависит от канала. Предполагается, что злоумышленник имеет неограниченный доступ к каналу передачи и может определить генераторную матрицу, используя параметры канала, длину и размер предполагаемого полярного кода.

Алгоритм защиты генераторной матрицы.

1. Определяются параметры Бхаттачатрия битовых каналов, и перестановка.

2 Индексы выбираются случайным образом из индексов хороших битовых каналов. Этот шаг эквивалентен случайному выбору битовых каналов из хороших битовых каналов.

3. Секретная матрица определяется как подматрица, строки которой выбираются на основе индексов замороженного набора секретов.

4. Замороженный вектор имеет криптографическую защиту.

Эффективность. Существует большого семейства эквивалентных полярных кодов, которое приводит к повышению уровня защиты от атак с исчерпывающим поиском. Матрицы полярных кодов имеют особую структуру, которая позволяет уменьшить размер ключа. Несистематичность полярных кодов, позволяет декодировать особые формы преднамеренных векторов ошибок, что обеспечивает более высокий уровень защиты от выбранных атак с открытым текстом при меньшей длине ключа.

Литература

1. Rosenqvist T., Sloof J. Implementation and evaluation of Polar Codes in 5G. Karlstad University, 2019.

2. Mahdavifar H., Vardy A. Achieving the secrecy capacity of wiretap channels using polar Codes // IEEE Trans. Inf. Theory. 2011. Vol. 57, iss. 10. P. 6428–6443.

МНОГОПУТЕВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ В СЕНСОРНОЙ СТОХАСТИЧЕСКОЙ СЕТИ

С.Б. Саломатин, А.П. Турлай

В сенсорных сетях распределение ключей обычно сочетается с начальным установлением связи, чтобы настроить безопасную коммуникационную инфраструктуру из набора развернутых сенсорных узлов [1].

Один их подходов решения задачи распределения секретных ключей предполагает использовать случайную маршрутизацию сетевой структуры.

Модель распределения ключей. В сенсорных сетях распределение ключей обычно сочетается с начальным установлением связи, чтобы настроить безопасную коммуникационную инфраструктуру из набора развернутых сенсорных узлов. В процессе настройке, узлы предварительно инициализируются секретной информацией. После настройки сети известно местоположение узлов. Предположим, что можно обмениваться достаточной маршрутной информацией, так что A знает все непересекающиеся пути к B, созданные во время начальной установки ключа.

Модель динамической стохастической сенсорной сети [2]. В модели сенсорной сети, каждый узел обновляет скалярное состояние. Узел является последовательным, если для формирования управляющего действия используется только относительный обмен информацией с соседями. Узел является лидером, если, помимо относительного обмена информацией с соседями, он также имеет доступ к собственному состоянию. Проблема идентификации лидеров сети, сводится к решению задачи минимизации среднеквадратического отклонения.

Алгоритм многопутевого ключа состоит в том, чтобы координировать обновление ключа по нескольким независимым путям, определяемыми случайно расположенными лидерами сети. Секретность ключа защищена всеми случайными значениями путей.

Литература

1. Chan H., Perrig A., Song D. Key distribution techniques for sensor networks. Norwell, MA, USA: Kluwer Academic Publishers, 2004.

2. Саломатин С.Б., Алексеенко А.Э., Турлай А.П. Сетевое кодирование кодом Рида-Соломона с учетом лидеров стохастической сети // Кодирование и цифровая обработка сигналов в инфокоммуникациях: материалы международной научно-практической конференции, Минск, 19 апреля 2021 г. С. 23–27.

ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ТПТС-НТ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ДЛЯ ЯДЕРНОЙ ЭНЕРГЕТИКИ

С.М. Сацук, С.С. Стома

Одним из элементов практико-ориентированной подготовки специалистов для Белорусской АЭС в рамках специальности 1-39 03 03 «Электронные и информационно-управляющие системы физических установок» является практическое обучение на базе программно-технических средств ТПТС-НТ, серийно выпускаемых «ВНИИА им. Н.Л. Духова».

Оборудование ТПТС-НТ используется в составе АСУ ТП Белорусской АЭС в части систем нормальной эксплуатации для выполнения задач, возлагаемых на низовую автоматику, и объединяется в отдельные программно-технические комплексы по технологическим и компоновочным признакам. В состав комплекса ТПТС-НТ входят базовые средства автоматизации в виде стандартных крейтов с установленными в них модулями, средства коммуникации, конфигурирования и сервисные устройства.

Модули связи с процессом выполняют базовые стандартные функции, такие как измерение, фильтрация, диагностика модуля и канала, индивидуальное управление исполнительным механизмом и т.п. Центральное устройство ТПТС-НТ – программируемый процессор автоматизации, в котором реализуются прикладные алгоритмы, функции защиты, блокировки, функционально-групповое управление.

Для реализации практико-ориентированной подготовки специалистов на базе аппаратуры ТПТС-НТ разработан комплекс лабораторных работ по специальным дисциплинам, который предполагает широкий спектр практических задач: создание тестового алгоритма приема и первичной обработки дискретного сигнала; составление алгоритма обработки аналогового унифицированного сигнала тока и напряжения средствами стандартных функциональных блоков в редакторе GET-R1; реализация алгоритмов контроля и управления регулирующим клапаном; создание алгоритма индивидуального управления электродвигателем и запорной арматурой.

Совместно с ТПТС-НТ при проведении лабораторных занятий студентами используются имитаторы аналоговых и дискретных сигналов, исполнительных механизмов: задвижек, двигателей, регулирующих и соленоидных клапанов. Созданные алгоритмы проверяются на ошибки аппаратными средствами САПР GET-R1.

Предлагаемый комплекс лабораторных работ позволяет студентам освоить основные методы и типовые алгоритмы измерения, управления, диагностики и защиты от несанкционированного доступа на базе оборудования ТПТС-НТ для систем управления, используемых на Белорусской АЭС.

ТЕСТИРОВАНИЕ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ XSS-АТАК

Д.С. Сацукевич

XSS (Cross-Site Scripting) – уязвимость веб-сайта, при которой совершается внедрение злоумышленником вредоносного скрипта в структуры веб-приложения, в результате чего может быть установлено вредоносное программное обеспечение (ПО) в клиентское приложение. Используя XSS-атаки, злоумышленники не нацеливаются на конкретных пользователей, а распространяют свой вредоносный код. В рейтинге OWASP «Топ 10 главных угроз WEB-приложениям» за 2020 год данная атака занимает 7 место. В результате реализации данной атаки может быть получен доступ к Cookie, хранимым браузером пользователя, в которых хранится различная персональная

информация. Выделяют два вида XSS: отраженная (непостоянная) и хранимая (постоянная) XSS атаки.

Для реализации отраженной атаки не обязательно хранить вредоносный скрипт на сервере, но необходимо, чтобы пользователь совершил какое-то действие, к примеру, перешел по ссылке вида http://Сайт.com/search.php?q=<script> Функция</script>. В ситуации, если на сайте не реализовано экранирование символов, данный GET-запрос будет исполнен как скрипт, в результате которого злоумышленник получит себе данные, хранимые в Cookie пользователя. При реализации хранимой XSS атаки вредоносный скрипт уже хранится на сервере и автоматически исполняется.

В рамках данного исследования было проведено тестирования системы электронного обучения учреждения образования на возможность реализации XXS-атак.

Изначально необходимо было произвести аутентификацию в тестируемой системе электронного обучения по известной учетной записи и изучить содержание Cookie пользователя. Было обнаружено, что значения Cookies хранятся в поле MoodleSession. Если предположить, что злоумышленник может реализовать перехват значений Cookies, то он получит доступ к профилю пользователя, что было и протестировано в данной работе. Для этого с другого компьютера был осуществлена попытка доступ к тестируемой системе электронного обучения, при реализации которой значения поля MoodleSession было вручную изменено на значения другого пользователя, которые предположительно ранее были перехвачены злоумышленником. В результате доступ к системе электронного обучения был успешно получен злоумышленником.

Необходимо отметить, что в тестируемой системе использован метод защиты от XSS-атак, суть которого в том, что все Cookie, необходимые для авторизации, имеют флаг HttpOnly, из-за чего JavaScript не имеет доступа к данным, содержащимся в данных полях [1–4].

Литература

1. OWASP Top Ten [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/ – Дата доступа: 20.04.2021.

2. Cross-Site Scripting (XSS) [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS). – Дата доступа: 20.04.2021.

3. XSS атака – межсайтовый скриптинг [Электронный ресурс]. – Режим доступа: https://insafety.org/xss.php – Дата доступа: 20.04.2021.

4. JavaScript и куки (cookie) [Электронный ресурс]. – Режим доступа: https://ruseller.com/lessons.php?id=593 – Дата доступа: 20.04.2021.

К ВОПРОСУ О МЕТОДИКЕ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

А.И. Серый

В учебном плане некоторых физико-математических специальностей предусмотрено, в частности, изучение дисциплины «Технические средства и методы защиты информации». Независимо от того, являются ли сведения по отдельным темам данной дисциплины относительно устойчивыми или быстро устаревающими, в образовательном процессе следует более широко использовать принцип «все познается в сравнении» (что особенно важно при обобщении и закреплении материала).

При этом вопросы классификационного характера удобно оформлять в виде схем, а сравнительный анализ осуществлять в виде таблиц.

В качестве примеров заданий первого типа можно назвать составление классификационной схемы разновидностей: а) информационных сигналов; б) микрофонов. В качестве примеров заданий второго типа можно назвать сравнительный анализ: а) технических каналов утечки акустической информации (с точки зрения передающей среды, принципов перехвата, передачи и приема сигнала и т.д.); б) систем охраны периметров (с точки зрения основных элементов конструкции, особенностей расположения по отношению к земной поверхности и охраняемым сооружениям, особенностей реакции на человека, задействованных физических эффектов, степени защиты от помех и т. д.). В качестве источника информации, содержащего сведения, необходимые для составления подобных таблиц и схем, можно назвать [1]. При указанном подходе работа с учебными пособиями превращается в творческий процесс, при котором происходит переработка и реструктуризация имеющейся информации.

Можно выделить следующие уровни использования схем и таблиц в образовательном процессе. 1. Заучивание студентами готовых таблиц и схем, составленных преподавателем. 2. Самостоятельное заполнение таблиц и схем нужным содержанием (преподаватель предоставляет только «основу»). 3. Полностью самостоятельное составление таблиц и схем (на заданную тему или с самостоятельной формулировкой темы).

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.

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ МОБИЛЬНОГО РОБОТА

А.В. Сидоренко, К.А. Акула

В современных условиях для решения задач различного функционального назначения получают распространение роботизированные системы. При использовании программируемых команд с управляемого сервера, а также при обмене данными между роботами критически важным условием является безопасность передаваемой информации.

При внедрении же мобильных роботов одной из актуальных является проблема определения местоположения робота и мониторинг его движения. Подобные задачи решаются путем применения при моделировании нейросетевых алгоритмов, а также алгоритмов обучения с подкреплением. Критерием оптимизации при этом является определение вознаграждения в зависимости от числа производимых итераций.

В данной работе рассматривается модель управления движением мобильного робота в некоторой среде при известном начальном местоположении, расположения целевых точек с учетом огибания встречающихся на пути движения препятствий. При моделировании используемая нами модель входит в состав блоков пакета Mobile Robotics Toolbox. В модели движения группы роботов применяется пакет Mobile Robotics Simulation Toolbox на операционной системе Linux при использовании пакета визуализации Gazebo. Взаимодействие обеспечивается через пакет для Matlab ROS Toolbox. Robotics System Toolbox поддерживает генерацию соответствующего кода, что позволяет создавать узлы ROS непосредственно из Simulink-моделей.

Анализ данных, полученных при верификации предложенной нами модели, и данных, полученных при реализации известных алгоритмов обучения с подкреплением, включая алгоритм SARSA, алгоритм Q-learning, алгоритм Deep Q-learning, показал, что производительность разработанной нами модели при расчете значения вознаграждения в зависимости от количества итераций превышает результаты использования других алгоритмов более, чем в 20 раз при одинаковом числе итераций.

ИССЛЕДОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ASTRA LINUX СМОЛЕНСК

В.С. Сляднев, Д.Е. Белов, Е.А. Сляднева

Операционная система специального назначения Astra Linux Special Edition (ОС СН Смоленск) основана на дистрибутиве Astra Linux Common Edition (ОС ОН Орел), который в свою очередь основан на операционной системе Debian (универсальсальная система с открытым исходным кодом) и, кроме того, включает в себя ряд принципиальных доработок для обеспечения соответствия требованиям руководящих документов Российской Федерации по защите информации. Например, из двух СУБД MySQL и PostgreSQL, входящих в состав Astra Linux Common Edition, в дистрибутив операционной системы Astra Linux Special Edition включена СУБД PostgreSQL, доработанная по требованиям безопасности информации. Также к основным отличиям AstraLinux можно отнести реализацию «мандатного доступа» в соответствии с патентом на изобретение «Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом» (№ 2525481; патентообладатели: АО «НПО РусБИТех», Девянин П.Н.; автор: Девянин П.Н.; заявка № 2012146550; приоритет изобретения: 01.11.2012; опубликовано: 10.05.2014; бюл. № 13, 12 с.; МПК G06F21/62). ОС СН соответствует требованиям руководящего документа «Средства вычислительной техники. ОС СН может использоваться в составе автоматизированных систем класса защищенности до 1Б включительно, обрабатывающих информацию до степени секретности «совершенно секретно» включительно [1–6].

Литература

1. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2014. 640 с.

2. Степанов Е.А. Информационная безопасность и защита информации. М.: ИНФР-М, 2014. 353 с.

3. Северин В.А. Правовое обеспечение информационной безопасности предприятия. М.: Городец, 2014. 352с.

4. Дунаев С. Доступ к базам данных и техника работы в сети. М.: Диалог МИФИ, 2014. 444 с.

5. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. СПб.: Университет МВД РФ, 2015. 226 с.

6. Штребе М. Безопасность сетей NT4. М.: Мир, 2011. 344 с.

ИССЛЕДОВАНИЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «МАГПРО КРИПТОПАКЕТ»

В.С. Сляднев, Д.Е. Белов, Е.А. Сляднева

Средство криптографической защиты информации (СКЗИ) «МагПро КриптоПакет» основана на программных продуктах с открытым исходным кодом

OpenSSL и OpenVPN. Разработчикам удалось заменить алгоритмы шифрования с RSA на ГОСТ, в соответствии с руководящими документами ФСБ в Российской Федерации. «OpenVPN-ГОСТ» предлагает масштабируемый режим клиент/сервер, позволяет нескольким клиентам подключаться к одному и тому же серверному процессу «OpenVPN-ГОСТ» через один TCP-порт. «OpenVPN-ГОСТ» – это составная часть СКЗИ «МагПро КриптоПакет» 3.0, а именно исполнение 7 (соответствует классу КС1) и исполнение 8 (соответствует классу КС2) указанного СКЗИ. При выявлении нарушений целостности модулей СКЗИ или операционной системы необходимо выявить и устранить причины искажения модулей. Восстановление целостности СКЗИ осуществляется с помощью средств установки СКЗИ или программного комплекса, использующего СКЗИ: для Windows путем повторной установки СКЗИ; для UNIX-подобных ОС – путем повторной установки пакета в режиме «reinstall». Перед установкой СКЗИ необходимо проверить целостность дистрибутивных пакетов СКЗИ (перечень дистрибутивных пакетов и значения хэш-векторов для них приведены в формуляре на СКЗИ). По завершении процедур восстановления целостности модулей СКЗИ и/или операционной системы должна быть проведена проверка корректности восстановления путем вычисления хэшвекторов модулей и их сравнения с ранее зафиксированными эталонными значениями [1–10].

Литература

1. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2014. 640 с.
2. Степанов Е.А. Информационная безопасность и защита информации. М.: ИНФР-М, 2014. 353 с.
3. Северин В.А. Правовое обеспечение информационной безопасности предприятия. М.: Городец, 2014. 352с.
4. Дунаев С. Доступ к базам данных и техника работы в сети. М.: Диалог МИФИ, 2014. 444 с.
5. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. СПб.: Университет МВД РФ, 2015. 226 с.
6. Штребе М. Безопасность сетей NT4. М.: Мир, 2011. 344 с.
7. Назаров С.В. Администрирование локальных сетей. М.: Финансы и статистика, 2015. 355 с.
8. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. СПб.: Питер, 2008. С. 86–87.
9. Семененко В.А. Информационная безопасность. М.: МГИУ, 2010. 277 с.
10. Сычев Ю.Н. Основы информационной безопасности. М.: ЕАОИ, 2007. 300 с.

ОСНОВНЫЕ ФУНКЦИИ БЕЗОПАСНОСТИ SALESFORCE

М.В. Стержанов

Функции безопасности Salesforce дают пользователям возможность безопасно и эффективно проводить работу в системе, разграничив доступ к данным для разных групп пользователей. Рассмотрим основные способы защиты данных от несанкционированного доступа внутри организации и от ненадлежащего использования пользователями.

Salesforce отображает информацию о производительности и безопасности системы в режиме реального времени на сайте http://trust.salesforce.com. Ресурс http://trust.salesforce.com/security предоставляет оперативные данные о производительности

системы, предупреждения о текущих и недавних попытках фишинга и вредоносного ПО, а также советы по передовым методам обеспечения безопасности.

Администратор может использовать механизм Health Check для выявления и устранения потенциальных уязвимостей в настройках безопасности. Сводная оценка показывает степень соответствия с базовыми показателями и стандартами безопасности. Имеется возможность загрузить до пяти настраиваемых базовых показателей вместо стандартного базового плана Salesforce.

Функции аудита Salesforce непосредственно не защищают организацию, однако предоставляют важную информацию об использовании системы, которая может иметь решающее значение для диагностики потенциальных или реальных проблем безопасности.

Salesforce Shield – это три инструмента безопасности, которые помогают создавать дополнительные уровни доверия, соответствия и управления прямо в критически важных для бизнеса приложениях. Он включает в себя шифрование платформы Shield, мониторинг событий и журнал аудита [1].

Литература

1. Salesforce Security Basics [Электронный ресурс]. – Режим доступа: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/overview_security. htm. – Дата доступа: 10.04.2021.

ВИЗУАЛИЗАЦИЯ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СРЕДСТВАМИ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

В.А. Столер

В ходе рассмотрения технологий виртуальной и дополненной реальности, были выявлены особенности их использования, которые нужно учитывать, например, при изучении воздействия электромагнитного излучения (ЭМИ). Перспектива визуализировать процесс воздействия ЭМИ, который можно рассмотреть со всех сторон, увидеть результат этого воздействия, представляется интересным.

Виртуальная реальность – это созданный техническими средствами мир, передаваемый человеку через органы чувств. Дополненная реальность – это среда, дополняющая в реальном времени физический мир цифровыми и графическими данными с помощью технических и программных средств [1].

Использование средств виртуальной и дополненной реальности позволяет, не находясь непосредственно в зоне воздействия, интерактивно наблюдать и оценивать ситуацию. В этом случае дополненная реальность предлагает широкий функционал и множество сценариев для оптимизации различных факторов воздействия и защиты от ЭМИ. Например, можно применить приложения дополненной реальности для отображения цифровых данных, графических изображений, статистики и любой другой информации, относящейся к текущей задаче. При рассмотрении экранов ЭМИ или других компонентов оборудования, можно виртуально видеть, например, температуру объектов взаимодействия, их поглощательную способность, рабочий диапазон частот, другие технические характеристики.

Вместе с тем, использование виртуальной и дополненной реальности в настоящее время достаточно затруднительно. В первую очередь это относится к дополненной реальности, так как связано со значительными финансовыми затратами, с отсутствием качественных приложений и небольшим опытом использования данной технологии.

Литература

1. AR – Дополненная Реальность (статья плюс ролик) [Электронный ресурс] // Национальный форум Российской Федерации. – Режим доступа: https://habr.com/ru/post/419437/. – Дата доступа: 06.08.2018.

ВЛИЯНИЕ ВРЕМЕНИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ВЕРОЯТНОСТЬ ОШИБОЧНОЙ РЕГИСТРАЦИИ ДАННЫХ В КВАНТОВО- КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

А.М. Тимофеев

Для обеспечения абсолютной скрытности и конфиденциальности информации целесообразно использовать системы квантово-криптографической связи [1, 2]. Одной из основных задач при этом является обеспечение достаточно высокой надежности приемных модулей таких систем – счетчиков фотонов [2]. Поскольку известные методы оценки показателей надежности не применимы для систем квантово-криптографической связи, целью данной работы являлось выполнить оценку влияния среднего времени передачи информации на вероятность ошибочной регистрации данных в квантово-криптографическом канале связи, содержащем в качестве приемного модуля счетчик фотонов. Объект исследования – квантово-криптографический канал связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа. Получены выражения для расчета вероятностей ошибочной регистрации двоичных данных, передаваемых в каналах квантово-криптографической связи. Определены зависимости вероятностей ошибочной регистрации двоичных данных от среднего времени однофотонной передачи информации, что позволило обосновать время однофотонной передачи, обеспечивающее наименьшие потери информации. Установлено, что с ростом средней длительности мертвого времени продлевающегося типа наименьшие значения вероятностей ошибочной регистрации символов «0» и символов «1» имеют место при более высоких значениях среднего времени однофотонной передачи символов «0» и «1» соответственно.

Литература

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Мн., Белоруская наука, 2007. 378 с.

2. Тимофеев А.М. Методика снижения потерь информации в асинхронном двоичном однофотонном канале связи с приемником на основе счетчика фотонов // Приборы и методы измерений. 2020. Т. 11. № 1. С. 70–81.

ПРИЕМО-ПЕРЕДАЮЩЕЕ УСТРОЙСТВО НА ОСНОВЕ КАНАЛОВ ОДНОФОТОННОЙ СВЯЗИ ДЛЯ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

А.М. Тимофеев

В настоящее время при реализации систем защиты информации достаточно часто применяют каналы однофотонной передачи информации, например, в системах квантово-криптографической связи [1–3]. Эти каналы позволяют обеспечивать абсолютную скрытность и конфиденциальной передаваемой информации за счет использования маломощных оптических импульсов, содержащих в среднем от одного

до десяти фотонов на каждый передаваемый бит (символ). Одной из основных задач при этом является регистрация столь слабых оптических импульсов, для чего используют высокочувствительные приемные модули – счетчики фотонов. Однако счетчики фотонов ввиду неидеальности своих технико-эксплуатационных характеристик могут снижать достоверность зарегистрированных данных. В частности, при увеличении мертвого времени счетчика фотонов достоверность зарегистрированных данных уменьшается при прочих равных параметрах приема [2]. В свою очередь, это может снизить уровень информационной безопасности системы связи в целом и уменьшить пропускную способность каналов однофотонной связи [3]. Для достижения наибольшей достоверности зарегистрированных данных необходимо получить статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации двоичных данных [2]. Поскольку до настоящего времени отсутствуют устройства, позволяющие сформировать указанные выше распределения, целью данной работы является разработка такого устройства. Объектом исследования являлся асинхронный двоичный несимметричный однородный однофотонный канал связи без памяти и со стиранием [2, 3]. Разработано приемо-передающее устройство на основе каналов однофотонной связи для передачи конфиденциальных данных. Устройство позволяет сформировать массив данных, содержащий статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов, не требует использования для передачи данных поляризационного оптического излучения, что, в сравнении с известными, упрощает его, ускоряет процесс обмена информацией за счет устранения процедуры согласования базисов, в которых переданы и приняты двоичные символы, а также уменьшает ошибку передачи данных, связанную с деполяризацией оптического излучения.

Литература

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Мн., Белоруская наука, 2007. 378 с.

2. Тимофеев А.М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов // Информатика. 2019. Т. 16, № 2. С. 90–98.

3. Тимофеев А.М. Скорость передачи информации однофотонного канала связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа // Труды БГТУ. Сер. 3. Физико-математические науки и информатика. 2019. № 2. С. 79–86.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ РАДИОПОМЕХ НА РАБОТУ СЧЕТНЫХ СХЕМ

Н.А. Титович

Путем выбора менее восприимчивых к воздействию электромагнитных помех (ЭМП) элементов, рациональной защиты их наиболее уязвимых цепей можно значительно снизить затраты на обеспечение электромагнитной совместимости. В связи с этим при проведении исследований необходимо расширить номенклатуру интегральных микросхем (ИМС). Для повышения достоверности оценки восприимчивости многовыходовых микросхем целесообразно осуществлять одновременный контроль состояния всех их выходов [1].

Проведены исследования влияние гармонических ВЧ помех с частотой 100–400 МГц на работоспособность четырехразрядного двоичного счетчика ИЕ5, который

представляет собой последовательное соединения четырех JK-триггеров (A, B, C, D). Осуществлялся одновременный контроль сигналов на всех выходах Q1–Q4 исследуемой ИМС. Помехи подавались последовательно на вход C1, выход Q4, шину питания.

При воздействии радиопомех на вход C1 происходит нарушение в работе первого JK-триггера (A), который начинает работать как инвертор входного сигнала, происходят нарушения в работе последующих триггеров, коэффициент счета счетчика уменьшается на два. При воздействии ЭМП на выход нарушения работоспособности происходят по причине сбоя в работе четвертого JK-триггера (D), на выходе Q4 устанавливается постоянный уровень логического нуля. При подаче ЭМП на шину питания сначала отказывает триггер D. Состояния выходов Q1, Q2, Q3 при этом не нарушаются. При дальнейшем увеличении уровня помехи происходят сбои в работе триггеров A и C. Алгоритм работы триггера B не нарушается. И только при дальнейшем возрастании уровня ЭМП он сбивается. В конечном итоге все четыре триггера работают как инверторы. Таким образом, наиболее восприимчивым к действию ВЧ помех оказался триггер D, а самым устойчивым – триггер B.

Информацию о более уязвимых к воздействию ЭМП элементах ИМС можно учитывать при разработке мер их защиты и построении схем с высокой алгоритмической устойчивостью. Так, например, при определенных условиях для деления на 2 целесообразнее использовать более устойчивый триггер B микросхемы ИЕ5 вместо триггера A.

Литература

1. Патент RU 2069865. Устройство для контроля параметров цифровых интегральных схем при воздействии электромагнитных помех / Н.А. Титович, Е.А. Буевич. – Опубл. 27.11.1996.

АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОГО ХЕШИРОВАНИЯ ДАННЫХ

П.И. Удалой, М.С. Коротыгин, Е.С. Белоусова

В настоящее время хеш-функции распространены в системах проверки целостности и подлинности сообщений, аутентификации пользователей, для формирования и передачи электронно-цифровой подписи. Также хеш-функции используются при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных.

Хеш-функции – это функции, предназначенные для «сжатия» произвольного сообщения или набора данных в некоторую битовую комбинацию фиксированной длины, называемую сверткой. Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргумента.

Криптографические хеш-функции – это выделенный класс хеш-функций, который имеет определенные свойства, делающие его пригодным для использования в криптографии, то есть, делающие его криптостойким.

В рамках данного доклада будет представлен сравнительный анализ наиболее распространенных алгоритмов криптографического хеширования, проведенный на основе углубленного изучения различных видов хеширования, их статистических свойств и требований, предъявляемых к таким алгоритмам, а также будут выделены проблемы, возникающие при их использовании.

В ходе сравнительного анализа установлено, что разработчики в нынешнее время при выборе алгоритма хеширования, учитывая настолько большое количество различных хеш-функций, сталкиваются с компромиссом. Компромиссом между скоростью хеширования и криптостойкостью свертки – если, например, разработчику нужен в первую очередь быстрый, а не надежный, алгоритм он выбирает MD5. А если же ситуация противоположная, когда на первом месте стоит степень криптостойкости функции, а не ее скорость, разработчик выбирает SHA-384 или SHA-512. Если ситуация более сложная, когда разработчику одновременно важна скорость алгоритма и ее криптостойкость, он выбирает SHA-1 или SHA-256 [1–5].

Литература

1. Хеш-алгоритмы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/93226/. – Дата доступа: 25.04.2021.

2. Криптографические хеш-функции [Электронный ресурс]. – Режим доступа: https://utmagazine.ru/posts/21195-kriptograficheskaya-hesh-funkciya. – Дата доступа: 25.04.2021.

3. Hashing algorithm [Электронный ресурс]. – Режим доступа: https://www.sciencedirect.com/topics/computer-science/hashing-algorithm. – Дата доступа: 25.04.2021.

4. MD5 Problems [Электронный ресурс]. – Режим доступа: https://www.avira.com/en/blog/md5-the-broken-algorithm/. – Дата доступа: 25.04.2021.

5. Cryptography Hash functions [Электронный ресурс]. – Режим доступа: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm. – Дата доступа: 25.04.2021.

ОПЫТ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В КОМПЛЕКСАХ «СОЛДАТ – БОЕВЫЕ СИСТЕМЫ»

Л.Л. Утин, Е.Л. Остромухов

В настоящее время по инициативе Государственного военно-промышленного комитета Республики Беларусь предприятиями оборонного сектора ведутся разработки по созданию информационно-технического комплекса «Солдат – боевые системы» [1]. Разработкой подобных систем занимаются многие ведущие государства, что обусловлено возросшими требованиями к современному общевойсковому бою. Основными подсистемами комплекса являются: подсистема управления, подсистема поражения, подсистемы энерго- и жизнеобеспечения и ряд других.

Одним из элементов комплекса является карманный персональный компьютер ВМ2306, разработанный ОАО «НИИ ЭВМ», предназначенный для решения различных задач по обработке поступающей информации, проведению тактических расчетов и отображению требуемой информации на мониторе [2]. При разработке данной вычислительной машины необходимо было учесть, что она должна обеспечивать исправное, непрерывное, круглосуточное функционирование в самых экстремальных климатических условиях. Кроме того, изделие должно сохранять свою работоспособность при воздействии дождя и пыли, а также одиночных и многократных ударов повышенной мощности. Не маловажным фактором, являлось обеспечение защита от несанкционированного доступа к информации. Опыт решения вышеуказанных проблем предлагается к обсуждению.

Литература

1. Синявский В.К., Солдат XXI века: на пути создания / В.К. Синявский, С.И. Верещагин [Электронный ресурс]. – Режим доступа: https://agat.by/upload/statii_files/files/Soldat%20XXI%20veka%202013. – Дата доступа: 20.04.2021

2. Машина вычислительная электронная персональная карманная – ВМ2306.М – Защищенные и промышленные компьютеры [Электронный ресурс]. – Режим доступа: https://niievm.by/produktsiya/kompyutery-i-komplektuyushchie/karmannyy-personalnyy-kompyuter-kpk-vm2306. – Дата доступа: 20.04.2021.

ХИМИЧЕСКОЕ ОСАЖДЕНИЕ СУЛЬФИДА ОЛОВА И КЕСТЕРИТА НА НАНОСТРУКТУРОВАННЫЕ ТЕМПЛАТ-ПОДЛОЖКИ ДЛЯ УСТРОЙСТВ ОПТОЭЛЕКТРОНИКИ

Е.А. Уткина, А.И. Воробьева, М.В. Меледина, А.А. Ходин

Полупроводниковые тонкие пленки сульфида олова SnS_x и кестерита перспективны для создания эффективных тонкопленочных солнечных элементов и фотодетекторов с учетом широкой распространенности, низкой стоимости и экологичности исходных составляющих материалов – серы и олова, процессов изготовления и готовых изделий, в том числе их утилизации [1, 2], а также при создании двумерных (2D) слоистых материалов для приложений в оптоэлектронных сенсорах и других устройствах оптической обработки информации [3]. Однако, до сих пор не разработаны достаточно надежные и эффективные процессы получения тонких слоев SnS_x с требуемой микроморфологией и электрофизическими характеристиками, особенно с учетом слоистой структуры данного соединения с ван-дер-ваальсовыми связями между слоями.

В данной работе исследуется химический метод послойного (SILAR) осаждения тонких 2D-слоев сульфида олова и кестерита Cu_2ZnSnS_4 с использованием наноструктурированных темплат-подложек алюминия и его анодного оксида. Использование подслоя титана и тантала обеспечивает улучшение адгезии к подложке, улучшение границы раздела с 2D слоем поглотителя на основе кестерита. СЭМ изображения демонстрируют изменение морфологии от наноразмерных кристаллов CZTS в зерна CZTS почти микронного размера в результате сульфидизации при температуре 450 °C. Анализ процесса осаждения 2D слоев сульфида олова и кестерита на темплат-подложку алюминия показывает, что использование нанопрофилированной подложки обеспечивает ориентированное осаждение полупроводника, увеличение эффективной площади осаждения, а также усиление поглощения оптического излучения в активном слое полупроводника.

Литература

1. Kawanishi S., Suzuki I., Bauers S.R., Zakutayev A., Shibata H., Yanagi H., Omata T. SnS homojunction solar cell with n-type single crystal and p-type thin film // RRL Solar. 2021. Vol. 5 (4). P. 2000708.

2. Cho J-Y., Kim S-Y., Nandi R., Jang J., Yun H-S., Enkhbayar E., Kim J-H., Lee D-K., Chung C-H., Kim J-H., Heo J. Achieving over 4 % efficiency for SnS/CdS thin-film solar cells by improving the heterojunction interface quality // J. Mater. Chem. 2020. Vol. A8. P. 20658–20665.

3.Tan T., Jiang X., Wang C., Yao B., Zhang H. 2D Material Optoelectronics for information functional device applications: Status and challenges // Adv. Sci. 2020. Vol. 7. P.2000058-25.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЦИФРОВЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ ВОЕННОГО НАЗНАЧЕНИЯ

В.А. Федоренко, М.Н. Лешкевич

Любая система имеет ряд уязвимостей. Рассмотрим основные способы воздействия нарушителя на цифровую систему передачи информации на примере цифровой радиорелейной системе связи. Данная система включает в себя: автоматизированное рабочее место (АРМ), модуль доступа, приемо-передающее устройство, антенну и, соединяющие это оборудование между собой, кабели.

Местами воздействия нарушителя и возможный результат его действий будут следующими:

а) получение доступа к АРМ, незащищенной операционной системе:

- изменение конфигурации управляемой системы;
- получение данных об характеристиках и установленных параметров аппаратуры;
- заражение вредоносным программным обеспечением;

б) место между модулем доступа и автоматизированным рабочим местом:

- ведение разведывательной работы за действиями системы;
- подставив модуль приема и анализатор принятого сигнала вводить пользователя АРМ в заблуждение и управлять модулем доступа;

в) имея выход к самому модулю доступа:

- подключить свое оборудование управления для действий, описанных выше;
- управление потоками, ввод/вывод их из эксплуатации;
- выведения из строя модуля для прекращения связи;

г) место посредника между внутренним и внешним блоком:

- получить мультиплексированную информацию потребителей сети;
- оборвать линию передачи между внутренним и внешним блоком;

д) получение доступа к месту соединения антенны и приемо-передающего устройства:

- оборвать линию передачи между антенной и приемо-передающим устройством;
- вести прослушивание [1, 2].

Литература

1. Утин Л.Л., Федоренко В.А., Масейчик Е.А. Военные системы радиорелейной связи. Минск: БГУИР, 2020. 160 с.

2. Эриксон Д. Хакинг: искусство эксплойта. СПб.: Питер, 2018. 496 с.

ИСПОЛЬЗОВАНИЕ ОБФУСКАЦИИ ПАКЕТОВ ДЛЯ СОКРЫТИЯ МЕТАДАННЫХ ТРАФИКА

П.С. Федорцов

Обфускация типа трафика – сокрытие сетевого протокола, используемого при обмене между двумя или более конечными узлами. Интерес к технологии маскировки метаданных трафика при помощи обфускации стал проявляться в ответ на широкое распространение технологии глубокого анализа пакетов (DPI) для активного мониторинга трафика, отправляемого приложениями. DPI, в отличие от традиционных брандмауэров, позволяет анализировать не только заголовки, но и содержимое пакетов. Также для фильтрации трафика при помощи DPI учитываются косвенные признаки, присущие каким-то определенным сетевым программам и протоколам. Для этого может использоваться статистический анализ (например, статистический анализ частоты встречи определенных символов, длины пакета и т. д.).

Обфускация направлена на разрушение этих статистических характеристик. Известны два подхода к обфускации: рандомизация характеристик и маскировка под известные сетевые протоколы. Рандомизация характеристик обычно заключается разбиении данных на пакеты случайного размера и отправки их со случайными интервалами. Такой подход проще в реализации и требует меньше вычислительных ресурсов. В результате невозможно установить принадлежность соединения какому-либо известному протоколу. При маскировке под известный сетевой протокол передаваемая информация таким образом, что ее сложно отличить от той, что обычно передается с использованием выбранного протокола. Также имитируются его статистические характеристики. Такой подход требует больших вычислительных ресурсов, но при этом сложнее обнаружить факт использования обфускации.

ЗАЩИТА ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ С ПОМОЩЬЮ ONLINE ПЕНТЕСТОВ

О.А. Хацкевич, А.Д. Михейчик

Защита информации на корпоративных сетях Республики Беларусь всегда являлась актуальной задачей. В настоящее время наблюдается непрерывное совершенствование механизмов реализации сетевых атак. В связи с этим системные администраторы должны периодически проверять на эффективность применяемые в их сети средства обеспечения сетевой безопасности. На рынке сетевых услуг существует большое количество программных и программно-аппаратных средств, предназначенных для мониторинга безопасности сетей. К недостаткам таких средств можно отнести высокую стоимость и сложность в реализации самостоятельной настройки. По этой причине в некоторых ситуациях имеет смысл прибегнуть к бесплатным online-инструментам, которые дают возможность оценить защищенность сети от актуальных сетевых атак владельцам даже небольших сетей. К таким online инструментам относятся пентесты. Под пентестом понимается мониторинг безопасности сети с помощью проведения испытаний на проникновения. Испытания основаны на сетевых атаках, реализуемых с целью обнаружения уязвимостей и недосатков. В работе исследовалась эффективности работы online-пентестов, направленных на межсетевые экраны, антивирусные программы и веб-сайты. Для проверки защищенности межсетевого экрана применялся сервис Check Point CheckMe . Представленный сервис включает в себя несколько тестов, с помощью которых выполняется анализ компьютера пользователя и сети на предмет наличия уязвимостей, связанных с вредоносными программами, удаленным доступом, утечкой данных, кражей конфиденциальной информации, эксплойтами и использованием анонимайзеров. Для мониторинга безопасности межсетевых экранов, антивирусных программных средств, веб-сайтов был использован дистрибутив Linux – Kali Linux, который непосредственно используется для осуществления пентестинга, благодаря большому количеству встроенных в данный дистрибутив инструментов. В качестве объекта исследования использовалась сеть БГУИР. Результат показал эффективность метода и достаточно высокую степень защищенности сети.

БАЗОВЫЕ ПРИНЦИПЫ РЕАЛИЗАЦИИ ПЛАГИНА ДЛЯ СИСТЕМЫ ОНЛАЙН-ПРОКТОРИНГА

А.А. Хомбак, Г.В. Юдин

В связи с пандемией COVID-19 резко вырос интерес к технологиям удаленной работы. Одновременно появилась стала задача удаленной проверки знаний учащихся

и компетенций работников, основной технологией проведения которой является прокторинг. Прокторинг рассматривается как способ удостовериться в соблюдении всех правил удаленного экзамена.

Цель работы – рассмотреть реализацию системы прокторинга с использованием браузера и технологии распознавания лиц. Система имеет вид веб-приложения или плагина для браузера. Особое внимание уделяется вопросам конфиденциальности и безопасности данных пользователей. Объект исследования – системы дистанционного обучения. Методы исследования – анализ, обобщение, формализация, эксперимент.

Онлайн-прокторинг может быть реализован в двух режимах – синхронном и асинхронном. При синхронном прокторинге за процедурой сдачи экзамена наблюдает человек-проктор. При асинхронном прокторинге все сдающие проходят проверку самостоятельно, используя систему прокторинга. Процесс сдачи записывается и отправляется прокторам на проверку.

В ходе исследования мы решили уделить повышенное внимание автоматизированной системе прокторинга. При использовании данной системы до начала экзамена сдающий устанавливает расширение (плагин) для браузера, такое расширение получает все нужные разрешения (доступ к микрофону, камере и т.д.), проверяет качество связи у сдающего экзамен. После проверки качества связи система верифицирует сдающего. При незначительных нарушения система будет оповещать сдающего о нарушениях. После завершения экзамена система обрабатывает полученные данные и отправляет их проктору, после чего он может провести дополнительную верификацию.

Очевидно, что в связи с удобством прокторинга и необходимостью проведения проверок в удаленной форме, технологии прокторинга будут развиваться. В дальнейшем мы планируем рассмотреть внедрение систем прокторинга в другие сферы деятельности, а также способы улучшения технологий применения существующих методов контроля и поиск их уязвимостей [1, 2].

Литература

1. Kryterion Online Proctoring Service / Kryterion Global Testing Solutions [Electronic resource]. – Access mode: http://www.kryteriononline.com/Delivery-Options/Online-Proctoring. Date of access: 20.03.2021

2. ProctorEdu. Сопровождение онлайн-экзаменов / ProctorEdu [Электронный ресурс]. – Режим доступа: http://proctoredu.ru. – Дата доступа: 20.03.2021.

БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ

Д.В. Хомельянский, Н.В. Ермакович, Е.А. Криштопова

Микросервисная архитектура – сервис-ориентированная архитектура программного обеспечения, направленный на взаимодействие насколько это возможно небольших, слабо связанных и легко изменяемых модулей – микросервисов [1].

Для обеспечения защиты микросервисной архитектуры используются такие сервисы, как: smart endpoints и dumb pipes (клиентские приложения), принцип децентрализованного управления, а также организация управления данными. Как и в традиционных системах функции, обеспечивающие безопасность должны быть встроены в шаблоны архитектуры, дизайна, и интегрирована во весь жизненный цикл разработки, чтобы приложения и данные оставались защищенными.

При использовании платформы облачных вычислений Amazon web services (AWS) предоставляет сервис Amazon Macie, который помогает защитить данные, аккаунты и рабочие нагрузки от несанкционированного доступа. Сервисы защиты данных обеспечивают возможности для шифрования, управления ключами и обнаружения угроз, среди их числа AWS Key Management Service (KMS), AWS CloudHSM (аппаратное хранилище ключей для соответствия нормативным требованиям).

Для идентификации угроз для микросервисных архитектур используются сервисы Security Hub, Network Firewall и Shield, которые непрерывно отслеживают активность в сети и поведение в аккаунтах вашей облачной среды [2]. Каждый микросервис отвечает за конкретно сформированную задачу, при этом является взаимозаменяемым, что позволяет не зависеть от конкретной технологии и полностью соответствует принципам построения микросервисной архитектуры.

Литература

1. Фаулер М., Льюис Д. Микросервисы [Электронный ресурс]. – Режим доступа: https://martinfowler.com/articles/microservices.html. – Дата доступа: 23.03.2021.

2. Amazon веб-сервисы [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ – Дата доступа: 23.03.2021.

РАЗРАБОТКА СИСТЕМЫ СИНТЕЗА РЕЧЕПОДОБНОГО СИГНАЛА

К.П. Шакин, О.Б. Зельманский

Защита акустической речевой информации является одной из важнейших задач по обеспечению информационной безопасности и осуществляется с использованием пассивных и активных методов защиты информации. Для реализации устройства активного метода защиты речевой информации, генерирующего речеподобную помеху, предлагается применить систему синтеза речеподобных сигналов на основе компиляционного метода, основная идея которого заключается в соединении готовых минимальных акустических единиц. При использовании этой модели составляется база данных звуковых фрагментов, из которых в дальнейшем будет синтезироваться речь. Размер элементов синтеза, как правило, не меньше слова. В качестве показателя эффективности защиты речевой информации используется словесная разборчивость речи W_c. Предлагаемая система синтеза речеподобных сигналов включает в себя следующие функции: анализ и обработка входного текста, формирование фонем и аллофонов, компиляция и генерация речевого сигнала. В целях реализации системы синтеза речеподобных сигналов разработан программный модуль синтеза речеподобных сигналов, который предполагает формирование фонемного текста и компиляцию баз аллофонов. В качестве минимальной акустической единицы используется аллофон Структура программного модуля включает: генератор псевдотекста, базу аллофонов, компиляционный синтезатор речи, акустическую система. В качестве основы компиляционного синтезатора речи целесообразно использовать два больших бока: обработки естественного языка и обработки цифрового сигнала. В результате на выходе компиляционного синтезатора речи формируется речеподобная помеха, которая в дальнейшем поступает на вход акустической системы. Предлагаемая система синтеза речеподобных сигналов обеспечивает защиту информации с помощью заранее сформированных баз аллофонов, однако ее можно адаптировать и к формированию баз аллофонов из речи диктора в режиме реального времени.

В заключении стоит отметить, что данный способ обеспечивает высокое качество синтезируемой речи, т. к. позволяет воспроизводить форму естественного речевого сигнала. Еще одно достоинство данного подхода: не требуется никаких знаний об устройстве речевого тракта и структуре языка [1–5].

Литература

1. Хорев А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты // Специальная техника. 2013. № 4. С. 31–63.

2. Фролов А., Фролов Г. Синтез и распознавание речи. М., 2008.

3. Рыбин С.В. Синтез речи. СПб: Университет ИТМО, 2014. 92 с.

4. Киселев В.В, Лобанов Б.М. Система синтеза русской речи на основе компиляционного метода // Доклады БГУИР. 2004. № 4 (8). С. 138–142.

5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – Телеком, 2005. 416 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ПРИЗНАКОВ СЕТЕВОЙ РАЗВЕДКИ

Н.П. Шараев, С.Н. Петров

В настоящее время около 15 % крупнейших организаций детектируют таргетированные или APT атаки на сетевую инфраструктуру. Указанные атаки крайне опасны для организаций, что связано с созданием киберпреступниками вредоносного программного обеспечения с учетом специфики работы информационных систем и сетевой инфраструктуры организаций. Исследование проводимых APT атак показал, что в общем случае таргетированные атаки состоят из четырех этапов: подготовка, проникновение, распространение (закрепление) и достижение цели. На каждом из представленных этапов дополнительно проводится процедура сокрытия (очистки), что позволяет злоумышленникам оставаться в сетевой инфраструктуре незамеченными. Обнаружить подобный тип атак на последней стадии крайне сложно, а в отдельных случаях невозможно. По данной причине целесообразно провести обнаружение и анализ таргетированной атаки на этапе подготовки. На указанном этапе злоумышленники проводят процедуру сетевой разведки инфраструктуры организации, которую можно выявить с помощью методов машинного обучения.

В качестве перспективных и быстродейственных алгоритмов машинного обучения, позволяющих провести обнаружения признаков сетевой разведки, выбраны: логистическая регрессия, квадратичный дискриминантный анализ, метод опорных векторов, метод ближайших соседей (K-ближайших соседей), «наивный» байесовский классификатор, дерево принятия решений и многослойный персептрон (нейронная сеть прямого распределения). Для всех представленных методов проведено обучение и тестирование с использованием различных гиперпараметров. Обучение алгоритмов проводилось на основе сгенерированного датасета, состоящего из 1000 уникальных событий (250 событий сетевой разведки и 750 легитимных событий). Наилучшие результаты эффективности и быстродействия показал метод дерева принятия решений с параметрами criterion = «gini» и splitter = «random». Дополнительно проведено улучшение отдельных алгоритмов с помощью процедур бэггинга и бустинга, а также представление алгоритма с наилучшими параметрами в виде программного кода, что позволило увеличить скорость работы приблизительно в 2 раза.

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЧЕСКИХ ПРИЕМОВ УЛУЧШЕНИЯ ЭЛЕКТРОИЗОЛЯЦИОННОЙ ПРОЧНОСТИ В ПЕРЕХОДНЫХ ОТВЕРСТИЯХ ДВУХСТОРОННИХ АЛЮМООКСИДНЫХ ОСНОВАНИЙ ДЛЯ СИЛОВЫХ МОДУЛЕЙ

Д.Л. Шиманович, Е.Д. Беспрозванный, Е.Е. Алясова

Целью исследований являлась разработка методов и приемов с применением оптимизированных технологических режимов для улучшения электроизоляционной прочности анодного Al_2O_3 в переходных отверстиях двухсторонних алюмооксидных оснований для перспективного использования в силовых многокристальных модулях [1], в частности, в области аппаратных средств защиты информации. Предварительные экспериментальные исследования изготовленных алюмооксидных оснований с матрицами переходных отверстий показали, что в процессе электрохимического анодирования на стыке горизонтальной и вертикальной поверхностей в переходных отверстиях неизбежно появлялись микротрещины из-за конкурирующих в разных направлениях фронтов анодирования, перестройки пористой структуры и возникающих механических напряжений, даже если на сплошной поверхности алюмооксидных оснований микротрещины полностью отсутствовали.

Было показано, что электрическая прочность анодного оксида алюминия в переходных отверстиях повышалась за счет минимизации количества микротрещин, если на исходных образцах алюминиевых оснований механическим обработкой формировались варианты тестовых переходных отверстий с фасками (под углом до 45°), плавным профилем на входах с удовлетворительными показателемя шероховатости и за счет залечивания микротрещин при реанодировании. Были разработаны и исследованы различные методы и методики, заключающиеся в выборе составов одно- и многокомпонентных электролитов и электрохимических условий для выгодной (с точки зрения увеличения пробивных напряжений в переходных отверстиях) структурной перестройки Al_2O_3 и формирования эластичных и гибких покрытий с минимизацией количества микротрещин и внутренних механических напряжений. Было установлено, что для обеспечения высоких пробивных напряжений необходимо выполнять грунтовку (заполнение пор) пористого анодного оксида алюминия и залечивание дефектных микротрещин Al_2O_3 в переходных отверстиях кремнийорганическим лаком в ультразвуковой ванне при частоте ~20–40 кГц при максимальной мощности ~0,5 кВт при температуре ~30 °С в течение ~ 20 мин. Причем этот технологический прием необходимо проводить в два цикла, а после заполнения излишки лака в переходных отверстиях необходимо выдувать сжатым воздухом, а с поверхностей снимать ракелем и обрабатывать раствором толуола, после чего осуществлять многостадийную процедуру термообработки до максимальной температуры ~280 °С.

Таким образом, было показано, что после применения соответствующих технологических приемов значения пробивных напряжений изготовленных тестовых образцов составляли до ~6 кВ на рабочих поверхностях без отверстий и до ~ 2,5 кВ в переходных отверстиях.

Литература

1. Шиманович Д.Л., Яковцева В.А. Электрохимическая алюмооксидная технология для приборов силовой электроники // Доклады БГУИР. 2019. № 3 (121). С. 5–11.

БЕЗОПАСНОСТЬ ПРИ АУТЕНТИФИКАЦИИ ФИЗИЧЕСКИХ ЛИЦ ПОСРЕДСТВОМ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

Д.И. Шуманский

Единая система идентификации физических и юридических лиц (ЕС ИФЮЛ) является компонентом Белорусской интегрированной сервисно-расчетной системы (БИСРС) и предназначена для предоставления гражданам Республики Беларусь сервисов строгой цифровой аутентификации для получения электронных услуг в информационных системах электронного правительства. Взаимодействие ЕС ИФЮЛ с внешними информационными системами построено на базе спецификации Open ID connect, расширенной криптографическими алгоритмами, стандартизированными в Республике Беларусь.

Защита данных, передаваемых от ЕСИФЮЛ до внешней информационной системы достигается использованием средств выработки ЭЦП и средств предварительного шифрования, сертифицированных на соответствие требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY). Защита данных, передаваемых от идентификационной карты до ЕС ИФЮЛ, достигается передачей информации в зашифрованном виде на общем ключе, сформированном в результате выполнения протокола BAUTH (п. 8.4 СТБ 34.101.78). Защита данных, передаваемых от клиентской программы до ЕС ИФЮЛ, достигается путем применения алгоритма предварительного шифрования BELT-CFB256 (п. 6.4 СТБ 34.101.31). Защита данных, передаваемых от клиентской программы до информационной системы, достигается путем применения протокола защиты транспортного уровня TLS (СТБ 34.101.65).

Идентификационная карта гражданина Республики Беларусь содержит два криптографических приложения eID и eSign. Приложение eID предназначено для хранения и предоставления персональных данных. Приложение eSign содержит личный ключ ЭЦП и предназначено для выработки электронной цифровой подписи. Идентификационная карта является пропуском гражданина в мир электронного правительства Республики Беларусь.

МОДИФИКАЦИЯ МЕТОДА LSB НА ОСНОВЕ ПОПИКСЕЛЬНОГО ИЗМЕНЕНИЯ ЦВЕТА СИМВОЛОВ ТЕКСТА-КОНТЕЙНЕРА

Н.П. Шутько

Как известно, формирование любого изображения (в том числе – текста) в растровой графике происходит по битовой карте (bitmap). Битовой картой называется структура данных, которая содержит информацию о растровом изображении в виде таблицы. С помощью такой таблицы можно описывать операции, базирующиеся на изменении цветовых параметров символов текстового документа. В основе предлагаемого метода лежит классический метод LSB (наименьшего значащего бита). В докладе приводится дальнейшее усовершенствование данного метода. В предлагаемом стеганографическом методе в качестве основного параметра символа текста, с помощью которого будет встраиваться секретное сообщение, выступает цвет [1].

Цвет символов в документах текстового процессора MS Word представлен в цветовой модели RGB, поэтому можно изменять значения лишь трех цветовых каналов – красного, зеленого и синего. Отклонение цвета должно быть незначительным

для эффективного скрытия секретного сообщения. Это связано с ограниченными возможностями человеческого глаза, в силу чего люди не способны различать незначительные вариации цветов. Кроме того, предлагается встраивать тайную информацию за счет изменения координат в модели HSL. HSL (от англ. hue, saturation, lightness (intensity)) – цветовая модель, в которой цветовыми координатами являются оттенок, насыщенность и яркость.

Таким образом, основной постулат рассматриваемого метода можно сформулировать так: цвет отдельных пикселей, формирующих символы текста-контейнера, можно изменить так, что это остается незаметным для других лиц в силу специфики человеческого зрения.

Литература

1. Шутько Н.П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста // Труды БГТУ. 2016. № 6 (188). С. 160–165.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИИ ПАРАМЕТРОВ АПРОША В МЕТОДАХ ТЕКСТОВОЙ СТЕГАНОГРАФИИ

Н.П. Шутько, П.П. Урбанович

Одним из направлений в области синтаксической стеганографии является использование параметров текста. К таким параметрам, в частности, относится апрош. Апрош – расстояние между символами текста. Авторами предложен и исследуется новый метод текстовой стеганографии, основанный на использовании данного пространственно-геометрического параметра текста. Контейнером в данном случае выступают текстовые документы, созданные с помощью текстового процессора MS Word. В основе описываемого метода лежит неспособность человеческого глаза различать незначительное изменение расстояния между символами в тексте.

Особенностью рассматриваемого метода является возможность одноразового размещения (в апроше одного символа) числа бит, определяемого дискретной разницей между минимальным и максимальным значением изучаемого пространственного параметра шрифта. За счет этого можно встроить необходимую секретную информацию. Межбуквенный интервал (апрош) может принимать значение от 0 до 1584 пт, однако следует принимать во внимание, что интервал может быть, как разреженным, так и уплотненным, что дает возможность встроить больший объем секретной (авторской) информации. При реализации данного метода внедрение секретного сообщения производится путем встраивания определенного числа бит (от 1 до нескольких – в зависимости от того, с каким шагом изменяется апрош) тайного сообщения, переведенного в двоичный вид, в апрош каждого символа файла-контейнера.

Дальнейшая работа предполагает проведение исследования, суть которого заключается в определении того, какое количество информации и при каких условиях сохранится после печати и последующего сканирования текстового документа-контейнера [1, 2].

Литература

1. Шутько Н.П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста // Труды БГТУ. 2016. № 6 (188). С. 160–165.

2. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh // Przegląd elektrotechniczny. 2018. R. 94, NR 6. P. 82–85.

ОПРЕДЕЛЕНИЕ ВРЕМЕНИ ТЕСТИРОВАНИЯ ПЛАНИРУЕМЫХ К РАЗРАБОТКЕ УЧЕБНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.В. Юреня, А.В. Будник

При разработчике учебных компьютерных программ, в том числе предназначенных для подготовки специалистов в области информационной безопасности, возникает вопрос о длительности этапа тестирования программ. Специалисты хотели бы также знать ожидаемые трудозатраты (в человеко-днях) на процедуру тестирования еще до написания кода компьютерных программ. Цель работы – получить модель для определения требуемого процессорного времени тестирования планируемых к разработке компьютерных программ.

В статье [1] была предложена модель надежности планируемых к разработке компьютерных программ, в том числе предназначенных для моделирования и обучения. Эта модель включает коэффициент тестирования, определяющий эксплуатационный уровень надежности компьютерной программы и зависящий от процессорного времени ее тестирования. На основе экспериментальных данных о тестировании и эксплуатационной надежности компьютерных программ, используемых для моделирования и обучения [2], получена модель расчета процессорного времени тестирования (с учетом требуемого коэффициента тестирования) для планируемых к разработке новых компьютерных программ. По значению полученного этого времени можно определить требуемые трудозатраты в человеко-днях на процедуру тестирования.

Литература

1. Боровиков С.М., Казючиц В.О., Хорошко В.В., Дик С.С., Клинов К.И. Оценка ожидаемой надежности прикладных программных средств для компьютерных информационных систем // Информатика. 2021. Т. 18, № 1. С. 84–95.

2. Software Reliability, Measurement, and Testing Guidebook for Software Reliability Measurement and Testing [Electronic resource]. Access mode: https://apps.dtic.mil/dtic/tr/fulltext/u2/a256164.pdf. Date of access: 03.05.2021.

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XVIII Белорусско-российской научно–технической конференции
(Минск, 8 июня 2021 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 21.05.2021. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 12,56. Уч.-изд. л. 9,2. Тираж 100 экз. Заказ 64.

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