Министерство образования Республики Беларусь
Белорусский государственный университет информатики и радиоэлектроники
Оперативно-аналитический центр при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь
Белорусское инженерное общество

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XVII Белорусско-российской научно–технической конференции
(Минск, 11 июня 2019 г.)

Минск БГУИР 2019

УДК 004.56 (043.2)
ББК 32.972.5
Т38

Технические средства защиты информации: Тез. докл. XVII Белорусско-российской
Т-38 науч.-техн. конф. (Республика Беларусь, Минск, 11 июня 2019 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2019. – 84 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 004.56 (043.2)
ББК 32.972.5

ISBN 978-985-543-513-7

ОГЛАВЛЕНИЕ

MICROWAVE SHIELDS MADE OF NON-VOWEN FABRICS CONTAINING CARBON ADDITIVES AND GEOMETRIC SHAPES FORMED WITH ALUMINIUM FOIL

H.D.A. Abdulhadi, A.M. Prudnik

The materials on the basis of non-vowen yarn to ensure shielding properties in a wide range of frequencies are praiseful if they are outlined by a high level of protection from the effects of external microwave fields, biological compatibility with biological objects [1].

Today there is a strong need for the materials that can be used to make protective shields from the microwave radiation produced by various electronic appliances. The most actual problem is to produce soft, breathable and cheap materials to ensure a sufficient degree of suppression of microwave radiation [2].

The experimental pieces of the needle-punched non-vowen fabrics containing carbon additives were produced of polyester with linear mass density 0.33 tex and 0.44 tex, polypropylene with linear mass density 0.33 tex, and wool with linear mass density 76 tex. As carbon additives we used carbon cellulose-hydrate filaments. The carbon cellulose-hydrate filaments were 65 mm long, with diameter of the fiber of 7–10 μm, with linear electrical resistance less than 20 Ohm·cm and electrical resistance about 0.024 Ohm·cm [3]. To ensure better reflective properties we attached geometric shapes formed with aluminium foil to the surface of the non-vowen fabrics.

To study the shielding peculiarities, we used a scalar network analyzer to measure transmission and reflection coefficients. The transmission and reflection coefficients of the experimental pieces were studied in the range of 0.3 to 17 GHz using scalar network analyzer. The microwave radiation transmission coefficient provided by the experimental pieces varies in the range of –7.0 to –15 dB and the reflection peculiarities vary in the range of –3 to –15 dB.

The main superiority of non-vowen fabrics containing carbon additives is a possibility to add it as a protective layer for the protective enclosures and clothing.

References

1. Wideband electromagnetic shields and absorbers / L. Lynkov [et al.] // Korean-Belarusian joint workshop on nanocomposite technology. Daejeon, 4–7 April 2009. P. 52–86.

2. Mahmud M.Sh., Belousova E.S., Kazeka A.A., Prudnik A.M. Otdelochnyj material na osnove shungita dlja zashhity biologicheskih ob'ektov ot jelektromagnitnyh polej / M.Sh. Mahmud [i dr.] // Doklady BGUIR. 2014. № 1 (79). S. 89–92. (in Russ.)

3. Production technology and shielding properties of the needle-punched non-vowen fabrics with carbon additives / A. Prudnik [et al.] // Proceedings of the 24th International conference «Electromagnetic disturbances EMD 2017». Białystok, 20–22 September 2017. P. 108–111.

HISTOGRAM-BASED ALGORITHMS OF LOW-CONTRAST IMAGE ENHANCEMENT

M.A. Abdulwahid, Y. Alhashimi, I. Baryskievich

Enhancement of image quality is an important task for the security systems based on image processing. Currently, there are a large number of methods for processing the noisy grayscale images, both in the spatial and in the frequency domain. Spatial image enhancement techniques are a basis of simple and more complex image processing techniques [1].

Three algorithms for processing the noisy grayscale images in the spatial domain were developed. The first algorithm for enhancement of low-contrast images is based on calculation of the normalized and cumulative histograms of grayscale images and the formation of the output image with a uniform histogram in a given dynamic range. The second algorithm is based on selecting the histogram of the output image, calculating the cumulative histogram of the output image, calculating the normalized and cumulative histograms of the input image and comparing the values of the cumulative histograms of the input and output images, forming the output image with the specified histogram. An iterative contrast optimization algorithm is based on the procedure of grouping low-contrast image histogram components into a specific number of bins according

to a selected criterion, redistributing these bins evenly according to the gray levels and the ungrouping procedure of previously grouped gray levels.

The simulation of the algorithms was performed in Matlab programming environment. The proposed algorithms have low computational complexity and can enhance the quality in 1.5–2.5 times. A comparative analysis of the results of processing the low-contrast noisy images and an efficiency evaluation of the algorithms were conducted. It has been found that the iterative contrast optimization algorithm is the most efficient algorithm for contrast enhancement.

References

1. Gonzalez R., Woods R. Digital Image Processing: International Edition. Pearson Education, 2011. 976 p.

ACTIVE LEARNING FOR TRAINING SPECIALISTS IN THE FIELD OF WEB TECHNOLOGIES PROTECTION

E.S. Belousova, O.V. Boiprav

From a technical view-point, the web is a highly programmable environment that allows mass customization through the immediate deployment of a large and diverse range of applications, to millions of global users. Two important components of a modern website are flexible web browsers and web applications; both available to all and sundry at no expense.

Security assessment is the key for identifying issues with protection of components and spotting potential attack vectors. Penetration testing by modeling what a real attacker would do against the target system offers a powerful way to obtain such information. This approach provides an unbiased look at the true level of protection against attacks and shows whether a company's security solutions are effective in practice. Therefore, it is important to train specialists in the field of web technologies protection. The discipline «Protecting web resources from unauthorized access» is an integral part of master's training in the specialty 1-98 80 01 «Methods and systems of information protection, information security» and refers to the state component of the cycle of special education disciplines. The experts in the field of web resources protection should possess the skills to find vulnerabilities in web system and eliminate them. For example, laboratory work plan on the topic «Vulnerability of connection Client-Server» should include the active learning methods that the teacher can use to develop students' thinking. Methods «Five minute paper» is used for test of the student preparation to perform laboratory work. The teacher can use methods «Ten-Two Strategy» and «Brainstorm» for developing skills of working in a team, showing initiative and creativity in non-standard situations, proposing directions for improving and developing the used technical means and solutions. The main technology, which should use teacher, is virtualization. Virtualization makes it possible to deploy virtual labs without high-end equipment and resources. Thus, the use of all these active teaching methods will improve the quality of training specialists in the field of information systems protection.

FEATURES OF TEACHING THE SUBJECT «INTRODUCTION TO INFORMATION SECURITY» TO INTERNATIONAL STUDENTS

O.V. Boiprav, E.S. Belousova

The subject «Introduction to information security» refers to the component of the higher education institution «Belarusian state university of informatics and radioelectronics», to the cycle of general professional and special subjects. Subject is taught for freshmen students of the specialty 1-98 01 02 Information security in telecommunications.

As a result of studying the subject, the students should obtain the theoretical knowledge about:

– legal support of information security;

– potential and real vulnerabilities of information systems and networks;

– information security threats classification;

– organizational and technical methods to ensure information security;

The authors propose to use the following approaches to organize for freshmen international students the possibility of these knowledge obtaining.

1. Describe the principles of legal support of information security on the base international standards (the main of them are ISO 15408, ISO 17799).

2. Use peer-to-peer method to organize the study of principles of information security threats classification and modeling. This method could be used both on the lecture and seminar, because as a rule the group of international students is no more then 15 persons.

3. Explain organizational methods for information security ensuring by the discussing with students the content of the standard ISO 27001, standards about the information security audit realization (COBIT, SAC, COSO), features of social engineering methods.

4. Use theoretical modeling method to organize discussion of technical methods to ensure information security. These discussion should be build on the knowledge about information security threats classification and modeling.

5. Explain technical methods for information security ensuring

6. Use the problem based learning method and brainstorm method to organize the final seminar of the subject. The theme of this seminar is «Information security vulnerabilities». The main task of this seminar could be connected with development the measures for protection defined information network of organization from impact of different attacks. These measures have to correspond the studied standards.

CLOUD SECURITY FOR FINANCIAL ORGANIZATIONS

S.N. Petrov, Anas Moftah Elbuaishi

Financial institutions are particularly exposed to cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected networks. By 2016, more than 60 % of transactions in the banking sector worldwide carried out on the basis of cloud technologies, according to Gartner . Banks are among the most advanced IT users, so they are still at the forefront in terms of developing private clouds. Cloud infrastructure technologies provide a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. The cloud requires few provisions while delivering rapid results.

Among the systems that banks are ready to place in private clouds: information systems such as CORE, ERP, CRM, that is critical for the existence of the entire banking business it solutions, while the least critical, for example, e-mail servers, can be placed in the public cloud.

Therefore, despite the fact that the banking sector is dominated by private clouds, cloud service providers are working to create highly secure public cloud solutions, «sharpened» for banking requirements and problems. In particular, new advances in encryption technology allow an organization to retain control over data even when it is on a remote server. In this case, even if the information is leaked, the key to decryption will remain in the hands of the company.

However the usage of a physically shared infrastructure also introduces new potential vulnerabilities unless the system is tightly monitored and controlled. An effective cloud security and privacy solution requires both the inclusion of key security features in the technology as well as a properly designed governance organization and processes.

Successful attacks on a financial institution could result in significant disruptions, although to date attacks have not caused large damages, based on publicly available information. A common method to disrupt firm business operations is to launch a DDoS attack on the targeted firms' servers. Cyber-attacks can also be used to undermine customers' confidence in an institution. For example, on June 27, 2014, Bulgaria's largest domestic bank FIB experienced a depositor run, amid heightened uncertainty due to the resolution of another bank – following phishing emails indicating that FIB was experiencing a liquidity shortage. Deposits outflows on that day amounted to 10 percent of the banks' total deposits and the bank had to use a liquidity assistance scheme provided by the authorities.

Banks should perform an internal/external risk assessment including PenetrationTesting, Vulnerability Scanning, Social Engineering and business process analysis related to data security. They should also develop a cloud computing roadmap based on business risk exposure (low-high), Cost of Ownership and opportunity of Return on Investment towards moving to the cloud.

ANALYSIS OF USERS WORK IN CLOUD COMPUTING ENVIRONMENT

U.A. Vishniakou, Z.R. Al-Attar Abdulraouf

Cloud computing (CC) have many advantages, but it is very important to ensure the safety of users and their recognition. Selected classes of threats in the CC environment related to the attacks: on the software; on cloud elements; on hypervisor, in the control system; threats of virtualization, migrate the virtual machines. The class of threats of users authority abuse, including due to the mutual influence of user tasks on computing nodes leading to unauthorized user access to data. Analysis of security mechanisms in CC systems showed that protection against joining unauthorized components is provided by means of mutual authentication mechanisms users and providers using digital certificates, encryption and digital signature of information transmitted between nodes of CC environments.

The main aspects of user security in CC. 1. Privacy, to achieve it, there are two main methods: physical separation and encryption. 2. Integrity: two main approaches to achieving it – message authentication code and digital signature. 3. Availability: make sure that users can access in Internet anytime and anywhere.

We consider the use of a new technology − Data-Centric Networking − DCS, which provides data owners with full control of their security throughout the life cycle of data in CC.

ANALYSIS OF USERS WORK IN CORPORATE MANAGEMENT SYSTEM AND E-SHOP

U.A. Vishniakou, H.J. Al-Musawi Hani, I.K. Nvosu

Traditional security paradigms in corporate management systems (CMS) provide security levels along the security perimeter: firewalls, intrusion prevention systems, encrypted network tunneling. Information-oriented network (ICN) is considered as a promising paradigm for the next generation of CMS working on Internet. In ICN content is more important than the host, which gives advantages such as reduced network load, low propagation delay, scalability, etc. Named Data Networking (NDN) represent the ICN architecture. The report presents four issues most important for security in NDN for information protection: from new forms of unknown attacks, privacy, blocking malicious network traffic, anomaly detection and DoS / DDoS attacks.

The following areas of protection in e-shops are highlighted: encryption method with digital signature, use of firewall, secure sockets layer (SSL), access permission. Encryption method: MD5 algorithm and password cache are used. Cache contains random data that are used as an additional login. A hash function hashes the password. The main function of cache is to protect against symbolic attacks against the list of hash passwords and against pre-computed attacks in the table. Firewall: creates an additional layer of security throughout the online store. With a firewall rule it will block attackers or blacklist them and deny access to the site. It has a scanner to provide installation recommendations in our e-shop. SSL protocol uses a 128-bit encryption key.

ANALYSIS OF THE BLOCK CHAIN USE

U.A. Vishniakou, R.Kh. Khudier

The functioning of the block chain and its security is provided by miners and other block chain participants. Access to the block chain takes place using special keys that guarantee the reliability of the entire network. Every user has it. A key is a set of cryptographic records. It is absolutely unique, which guarantees the impossibility of data substitution and hacker attacks. To do this, hackers need to access all the computers on the network. Mechanisms that ensure the efficiency and reliability of the block chain are algorithms of Proof of Work (PoW) – the work done, and Proof of Stake (PoS) – confirmation of the share. PoW in the block chain checks the calculations generated during the creation of a new block. The block is recognized as true and closed, provided that the value of its hash is less than the signature sought by miners. That is, a certain cryptographic cipher shows the authenticity of the block.

Examples of block chain application in various spheres of life, in addition to finance. Personal identification - services in the field of identification and confirmation of access rights work, which

create a digital equivalent of an identity card. Such startups include HYRP, BlockVerify, OneName and others. Copyright – the Ascribe platform uses the register in which artists, musicians, inventors can store the copyright of the encrypted identifiers. Management and law – already now there are projects like Borderless, which combine legal and economic services.

УГЛЕСОДЕРЖАЩИЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Х.А.Э. Айад, О.В. Бойправ, Л.М. Лыньков

Авторами обоснована перспективность использования порошкообразных материалов на основе активированного, древесного и кокосового углей для создания электромагнитных экранов. Установлено, что значения коэффициента передачи электромагнитного излучения (ЭМИ) в диапазоне частот 0,7–17 ГГц экранов на основе порошкообразных углесодержащих материалов – не более –7 дБ (толщина экранов – 8 мм). Значения коэффициента отражения, измеренные в режиме короткого замыкания, достигают величины –10 дБ. Определено, что в результате пропитывания до насыщения порошкообразных углесодержащих материалов водным раствором хлорида кальция можно обеспечить снижение с –7 до –35 дБ значений коэффициента передачи и с –10 до –14 дБ коэффициента отражения ЭМИ электромагнитных экранов на их основе, что связано с увеличением с $4{,}6\cdot10^{-8}$–0,45 См/м до 0,1–70 См/м удельной проводимости таких порошков.

Таким образом, электромагнитные экраны на основе порошкообразных углесодержащих материалов могут быть использованы для обеспечения защиты информации от утечки по каналу побочного электромагнитного излучения, а также в целях снижения радиолокационной заметности наземных объектов.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

В.М. Алефиренко

Подготовка специалистов по специальности «Техническое обеспечение безопасности», специализации «Технические средства защиты информации» осуществлялась в Белорусском государственном университете информатики и радиоэлектроники с 2002 по 2017 годы. Образовательная программа подготовки специалиста предусматривала изучение циклов социально-гуманитарных, естественнонаучных, общепрофессиональных и специальных дисциплин, дисциплин специализации, факультативные дисциплины, экзаменационные сессии, три вида практик, дипломное проектирование и итоговую государственную аттестацию [1]. Цикл общепрофессиональных и специальных дисциплин включал в себя обязательный компонент, вузовский компонент и дисциплины по выбору. Цикл дисциплин специализации включал в себя такие дисциплины как: «Первичные измерительные преобразователи и их применение в системах обеспечения безопасности», «Физические и аппаратные средства защиты информации», «Техническая защита информации в каналах утечки и вычислительных системах и сетях», «Технические и программные средства защиты информации в офисных и банковских системах» и «Проектирование электронных средств и систем обеспечения безопасности». Обучение студентов по специальности «Техническое обеспечение безопасности» предусматривало как очную (дневную), так и заочную формы обучения. При дневной форме обучения срок подготовки специалиста составлял 5 лет, а по заочной форме обучения увеличивался на 1 год. В университете осуществлялась также подготовка специалистов по заочной форме обучения для получения высшего образования, интегрированного со средним специальным образованием, что сокращало время подготовки до 4 лет. Подготовка специалистов проводилась как на бюджетной, так и на платной основе. Выпускающей кафедрой являлась кафедра «Проектирование ннформационно-компьютерных систем». При подготовке специалистов по специальности «Техническое обеспечение безопасности» использовались различные виды инновационных технологий, включая собственные разработки университета. За весь период подготовки по всем формам обучения по специальности «Техническое обеспечение безопасности» в Белорусском государственном

университете информатики и радиоэлектроники было выпущено более 1000 специалистов, работающих в настоящее время в различных областях, связанных с обеспечением защиты информации и безопасности объектов.

Список литературы

1. Образовательный стандарт республики Беларусь ОСРБ 1-38 02 03-2007. – Минск: МО РБ, 2007. – 36 с.

ИССЛЕДОВАНИЕ ЭКРАНИРОВАНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ

В.М. Алефиренко, В.Е. Галузо

При установке радиозакладных устройств, передающих информацию по радиоканалу (радиомикрофонов), злоумышленник должен обеспечить максимальную визуальную скрытность установки, оптимальное место установки с точки зрения съема акустической информации, максимальную дальность приема информации по радиоканалу и минимальную возможность его обнаружения. Последнее условие теоретически может быть обеспечено путем экранирования радиомикрофона со стороны прослушиваемого помещения. Такой экран, установленный на определенном расстоянии от радиомикрофона, не будет являться серьезным препятствием для акустических волн, но будет экранировать радиосигнал в сторону помещения и не экранировать его в противоположном направлении – в сторону радиоприемника, установленного в соседнем помещении или снаружи здания, в котором находится прослушиваемое помещение. Для проведения исследований были выбраны следующие приборы: индикатор электромагнитного поля, интерсептор, портативный частотомер ROGER RFM-31, сканирующий приемник IC-R5. В качестве закладного устройства использовался камуфлированный имитатор радиомикрофона, работающий на частоте 509,5 МГц, выполненный в виде деревянного бруска размером 160×25×15 мм [1]. В качестве экранирующего материала использовался жесткий металлический экран размером 200×300 мм, толщиной 0,5 мм и гибкая металлическая лента тонкой фольги толщиной 0,1 мм, позволяющая создавать различную форму экрана. Жесткий экран располагался перед микрофоном на различных расстояниях, на которых проводились измерения соответствующими приборами. С помощью фольги проводилось экранирование различных поверхностей самого корпуса радиомикрофона (деревянного бруска) и также проводились измерения соответствующими приборами: индикатором электромагнитного поля и интерсептором (метод акустической завязки), частотомером (измерение частоты), сканирующим приемником (захват и прослушивание сигналов в помещении). Исследования показали, что когда экран (фольга) располагался вплотную только на одной тыльной стороне бруска, сигнал экранировался на расстоянии 100 мм и менее, на одной тыльной и одной торцевой стороне – на расстоянии 80 мм и менее, на одной тыльной и двух торцевых – на расстоянии 20–30 мм и менее. При этом экранирующий эффект наблюдался со всех сторон, вне зависимости от того, какая сторона экранировалась. Если брусок экранировался со всех сторон, то сигнал вообще не обнаруживался. Таким образом, проведенные исследования показали, что вне зависимости от расстояния, на котором находился экран, достичь одностороннего экранирования сигнала не удается.

Список литературы

1. Алефиренко В.М., Андрушкевич В.С. Поиск закладных устройств комбинационным методом // Тез. докл. XVI Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 12.

АНАЛИЗ СЕТЕВОГО ТРАФИКА В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ ВООРУЖЕННЫХ СИЛ

М.А. Бабич

Корпоративная информационная сеть Вооруженных Сил (далее – КИС), объединяющая локальные информационные сети структурных подразделений Министерства обороны и Генерального штаба Вооруженных Сил, командований, учреждений и воинских частей Вооруженных Сил создана 27 октября 2017 года. В настоящее время КИС используется как для организации взаимодействия автоматизированных рабочих мест должностных лиц Вооруженных Сил между собой, так и для организации функционирования ведомственных информационных и автоматизированных систем.

Среднее количество сетевого трафика, проходящее через центральный сегмент КИС, в сутки составляет около 10 Гб. Анализ используемых в центральном сегменте КИС протоколов (DNS – 55,6 %, HTTP – 28,6 %, SSL – 9,8 %, SMTP – 2,7 %, NFS – 2 %, FTP – 1,3 %) свидетельствует о преобладании сетевого обмена с предварительным установлением соединения.

Наиболее активно системами мониторинга фиксируются DNS-запросы для обновления прикладного (31 %) и системного (28 %) программного обеспечения, установления соединения с ведомственными сетевыми ресурсами (21 %) и синхронизации времени (19 %).

Анализ данных систем управления событиями информационной безопасности позволяет прийти к выводу, что основные сообщения в КИС (классов notice – 36,4 %, info – 26,7 % и debug – 24,1 %) создает сетевой трафик запросов к DNS-серверам и ответов от них (для сегмента № 1 – 55,6 %, сегмента № 2 – 84,1 %). Следовательно, оптимизация конфигурации DNS-серверов в КИС позволит:

– снизить нагрузку на коммутационное и серверное оборудование;

– уменьшить количество ложных срабатываний сетевых систем обнаружения вторжений;

– уменьшить количество сообщений, поступающих в системы управления событиями информационной безопасности;

– повысить эффективность сетевой инфраструктуры.

ИНТЕГРАЛЫ ДВИЖЕНИЯ ЗАРЯЖЕННЫХ ЧАСТИЦ В ЭЛЕКТРОМАГНИТНОМ ПОЛЕ, ОБЛАДАЮЩЕМ СИММЕТРИЕЙ

И.В. Баженова

Во многих случаях электромагнитное поле в электронных приборах и устройствах СВЧ обладает симметрией в пространстве или имеет простые связи координат и времени (вращающееся поле, бегущая волна, поляризованная по кругу волна) [1, 2]. В этих случаях легко определяются первые интегралы движения электронов, которые носят название законов сохранения. Законы сохранения играют важную роль в теории электронных приборов по следующим причинам.

1. Они позволяют получить ценную информацию о специфике процессов взаимодействия электрона с электромагнитными полями и произвести анализ этих процессов, не прибегая к численному решению задач. При этом могут быть получены весьма общие и далеко идущие выводы; в частности, во многих случаях, еще до решения задачи, может быть решен вопрос о возможности или невозможности полезного эффекта, при том или другом новом механизме взаимодействия в приборе (если закон сохранения противоречит условиям получения полезного эффекта, то этого эффекта, естественно, не будет).

2. Законы сохранения позволяют контролировать точность численных расчетов. Кроме того, они позволяют эффективно контролировать и правильность формулировки приближенных математических моделей процессов взаимодействия в различных схемах приборов (в этих моделях неизбежны те или иные приближения, т. е. некоторые эффекты

и явления игнорируются). Действительно, если интегралы, следующие из приближенных уравнений, противоречат точным, то очевидно, что приближенная модель ошибочна.

3. Законы сохранения могут быть использованы и непосредственно для понижения порядка системы нелинейных уравнений, описывающих процесс взаимодействия электронов с электромагнитными полями.

Наиболее важными являются интегралы движения, не содержащие полевых составляющих. Эти интегралы связывают не только параметры движения электрона, но и позволяют получить достаточно глубокие и определенные выводы о характере этого движения.

Список литературы

1. Ландау Л.Д., Лифшиц Е.М. Теория поля. М.: Наука, 1967. 422 с.

2. Морозов А.И., Соловьев Л.С. Движение заряженных частиц в электромагнитных полях // Вопросы теории плазмы. 1963. Вып. 2. С. 177–241.

МЕТОДЫ РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ЭЛЕКТРОННЫХ ПОТОКОВ С ЭЛЕКТРОМАГНИТНЫМИ ПОЛЯМИ

И.В. Баженова

В теории оптимального управления широкое распространение получили вариационные методы решения возникающих в этой области задач, основанные на необходимых условиях стационарности функционала, выражающего цель конкретной задачи оптимального управления (целевой функции) [1, 2]. Если математическая модель динамического процесса задается в форме дифференциальных уравнений состояния, то необходимые условия стационарности формулируются в виде краевой (двухточечной) задачи для переменных состояний и множителей Лагранжа (сопряженных переменных). Эта задача имеет аналитическое решение лишь в исключительных случаях; в общем случае приходится использовать те или иные численные методы решения краевой задачи. Однако, эти методы могут привести к неустойчивым решениям, и необходимы специальные приемы (например, использование метода направленной ортогонализации), чтобы обеспечить сходимость решения. При высоком порядке уравнений состояния возможность численного решения задачи становится весьма проблематичной. Математические модели процессов взаимодействия электронных потоков с электромагнитными полями отличаются именно тем, что порядок уравнений состояния, описывающих поведение «крупных частиц», моделирующих электронный поток, весьма высок.

Таким образом, использование необходимых условий в задачах электроники СВЧ практически исключается и следует остановиться на прямых методах решения, т. е. на непосредственной минимизации (или максимизации) целевой функции, определенной на решениях уравнений состояния. На этом пути не следует пренебрегать некоторыми общими следствиями теории вариационного исчисления, которые, в частности, позволяют определять составляющие градиента целевой функции аналитически, не прибегая к шаговым численным методам. В сущности, необходимые условия в случае многопараметрической оптимизации сводятся к тому, что градиент целевой функции в экстремальной точке должен быть равен нулю. Построение первой вариации функционала и введение некоторых дополнительных условий позволяют получить формулу для градиента целевой функции и в любой текущей точке в пространстве параметров.

Список литературы

1. Болтянский В.Г. Математические методы оптимального управления. М.: Наука, 1969. 408 с.

2. Моисеев Н.Н. Численные методы в теории оптимальных систем. М.: Наука, 1971. 424 с.

АНТИФЕРРОМАГНИТНЫЕ СПИНОВЫЕ ВЕНТИЛИ

Г.Б. Байман, А.Л. Данилюк

В настоящее время спинтроника антиферромагнетиков (АФМ) является быстро развивающейся областью физики магнетизма. Несмотря на отсутствие макроскопической намагниченности, антиферромагнетики испытывают воздействие спин-поляризованного тока. В основе этого явления лежит спин-зависимое взаимодействие между локализованными и свободными электронами. Особенностями АФМ материалов как потенциальных носителей информации является сложная магнитная структура, существенная роль обменных взаимодействий, отсутствие макроскопической намагниченности. Эти факторы требуют непосредственного учета и ведут к усложнению моделирования электрических параметров спинтронных устройств [1]. С прикладной точки зрения АФМ имеют ряд преимуществ перед ферромагнетиками. Во-первых, обладая магнитной структурой и высокой восприимчивостью к внешним полям, АФМ частицы имеют нулевую или малую намагниченность, т. е. не создают внешних магнитных полей и поэтому слабо взаимодействуют друг с другом. Во-вторых, характерные частоты АФМ и, следовательно, частоты переключения между различными АФМ состояниями на несколько порядков превышают аналогичные значения для типичных ферромагнитных материалов. Это дает возможность создания высокоскоростных устройств, работающих в терагерцовом диапазоне. АФМ порядок в полупроводниках наблюдается гораздо чаще и при гораздо более мягких условиях, чем ферромагнитное упорядочение, что позволяет сочетать в одном устройстве преимущества как электроники (быстродействие, легкую управляемость), так и спинтроники (высокую чувствительность, малую энергоемкость). АФМ могут обладать и свойствами полуметаллов, т. е. проявлять свойства проводника для одной спиновой поляризации и изолятора для другой, что делает их весьма привлекательными спинронными материалами. Впервые идея о возможности использования АФМ материалов в качестве активных составляющих типичных спинтронных устройств (спиновых вентилей) была высказана в работах [2, 3].

В настоящей работе приведены результаты моделирования параметров спиновых вентилей, содержащих антиферромагнитные слои. Рассмотрен эффект обменного смещения намагниченности и его влияние на магнитосопротивление спинового вентиля. Показана возможность усиления магнитосопротивления спинового вентиля за счет обменного смещения в несколько раз.

Список литературы

1. Гомонай Е.В., Локтев В.М. Low Temperature Physics 40, 22 (2014).
2. Nunez A., Duine R., Haney P., MacDonald A. Phys. Rev. B 73, 214426 (2006).
3. Duine R.A., Haney P.M., Nunez A.S., MacDonald A.H. Phys. Rev. B 75, 014433 (2007).

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПАРАМЕТРИЧЕСКОЙ НАДЕЖНОСТИ ТРАНЗИСТОРОВ

А.И. Бересневич

Одним из подходов к оценке параметрической надежности изделий электронной техники (ИЭТ) является использование метода имитационных воздействий [1]. Метод позволяет по реакции функционального параметра ИЭТ (конкретного экземпляра) на имитационное воздействие в начальный момент времени спрогнозировать значение этого параметра на заданный будущий момент времени и сделать заключение о параметрической надежности экземпляра. Уровень имитационного воздействия, соответствующий заданной наработке, определяют с помощью имитационной модели, представляющей собой выражение, показывающее, какое значение имитационного фактора (тока или напряжения) соответствует той или иной заданной наработке.

Имитационную модель получают один раз с помощью предварительных экспериментальных исследований обучающей выборки. Обучающая выборка – это некая выборка, случайным образом сформированная из более крупной выборки или партии ИЭТ, параметрической надежностью экземпляров которой интересуются специалисты. Экспериментальные исследования включают получение математических выражений (моделей), показывающих, как выбранный функциональный параметр ИЭТ рассматриваемого типа изменяется от уровня имитационного фактора и от значения наработки.

Индивидуальное прогнозирование выполняют применительно к той выборке или партии ИЭТ, из которой была взята обучающая выборка. Причем прогноз получают для тех экземпляров, которые не принимали участия в обучающем эксперименте.

Рассмотренный метод имитационных воздействий был положен в основу разработки методики индивидуального прогнозирования параметрической надежности биполярных транзисторов. В качестве имитационного фактора рассматривалось напряжение, прикладываемое к *p*-*n*-переходу транзисторов. С методикой можно ознакомиться на кафедре ПИКС БГУИР (обращаться в ауд. 37 1-го учебного корпуса университета).

Список литературы

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

ДИФФЕРЕНЦИАЛЬНЫЙ МЕТОД АНАЛИЗА АНАЛОГОВОЙ СХЕМОТЕХНИКИ

И.А. Богод

В работе исследованы свойства дифференциального метода анализа аналоговой схемотехники. Данный метод отличается от классического тем, что с его помощью за счет использования дифференциальных параметров можно добиться гораздо меньшей погрешности по сравнению с результатами расчетов классическим методом. В работе исследованы несколько относительно простых схем, и в результате сравнения их расчетных погрешностей было установлено, что дифференциальный метод обладает наибольшей точностью в схемах с цепями отрицательной обратной связи. Данный метод позволяет получить более точные результаты и может оказать положительное влияние на способности и возможности нынешних и будущих специалистов в области криптографии и защиты информации.

Список литературы

1. Свирид В.Л. Аналоговая микросхемотехника. В 3 ч. Ч. 1: Интегральные микросхемы. Системотехническое проектирование радиоэлектронной аппаратуры. Минск: БГУИР, 2003. 232 с.

2. Свирид В. Л. Дифференциальный метод анализа аналоговой схемотехники // Доклады БГУИР. 2016. № 8 (102). С. 39–45.

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ ИНДИВИДУАЛЬНОГО ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

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

Для аппаратных частей технических систем, в том числе систем обеспечения информационной безопасности, во многих случаях предъявляются повышенные требования к надежности. Для обеспечения требуемого уровня надежности необходимо при изготовлении аппаратных частей использовать комплектующие элементы повышенного уровня качества. Полупроводниковые приборы (ППП) составляют заметную часть в составе устройств, используемых в электронных системах безопасности. Совершенствование технологии изготовления ППП привело к снижению доли внезапных отказов. Постепенные отказы, отражающие внутренне присущие материалам ППП свойства, в частности старение, в принципе исключить невозможно. Примерно в 80 % случаев отказы ППП проявляются в виде

постепенных (деградационных) отказов. Этим вызван растущий интерес к постепенным отказам ППП. В работе [1] приведена методика индивидуального прогнозирования надежности ППП по постепенным отказам, позволяющая из партий однотипных приборов отобрать экземпляры, отвечающие требованию по надежности. Для повышения эффективности процедуры индивидуального прогнозирования актуальна ее автоматизация. При участии авторов разработано программное средство, включенное в систему автоматизированного расчета надежности электронных устройств АРИОН-плюс [2]. С программным средством автоматизации индивидуального прогнозирования надежности ППП по постепенным отказам и системой АРИОН-плюс можно ознакомиться на кафедре ПИКС БГУИР, обращаться по e-mail: bsm@bsuir.by или в ауд. 37 1-го учебного корпуса университета.

Список литературы

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

2. Разработка программного комплекса автоматизированной оценки надежности электронных устройств и систем: отчет о НИР (заключительный). Рук. С.М. Боровиков. Минск, 2016. 46 с. № госрегистрации 20121425.

ОБ ИЗУЧЕНИИ ВИДОВ И ОСОБЕННОСТЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛИСТОВ

Е.В. Валаханович, Л.В. Михайловская

В настоящее время военному специалисту необходимо соответствовать современным профессиональным требованиям в области защиты информации. Вследствие этого на кафедре высшей математики учреждения образования «Военная академия Республики Беларусь» разработаны и внедрены факультативный курс «Защита информации» и дисциплина «Прикладная математика». Одной из начальных тем вышеназванных курсов является тема «Классификация угроз информационной безопасности».

Авторы считают необходимым уточнение разработанной ранее, например, в [1], классификации угроз. Угрозы информационной безопасности в зависимости от характера ущерба, который они могут нанести, целесообразно систематизировать исходя из двух основополагающих критериев: происхождения и категорий безопасности. Предлагается угрозы по происхождению подразделить на два направления: стихийные (природного характера) и созданные людьми. Источники угроз информационной безопасности, созданные людьми, можно разделить на три типа: преднамеренные, техногенные и случайные. Угрозы по категориям безопасности соответственно делятся на три направления: угрозы нарушения целостности, конфиденциальности и доступности.

Так как средства и методы обработки, передачи и защиты информации постоянно совершенствуются, то перечень и классификация угроз информационной безопасности могут изменяться и приводить к появлению принципиально новых видов угроз и способов преодоления систем безопасности.

Таким образом, непрерывная и надежная работа по защите информации в сфере военной деятельности обусловлена разработкой классификации угроз информационной безопасности, как первого шага в алгоритме работы по их предотвращению и предупреждению.

Список литературы

1. Mehrhoff M. IT-Grundschutzhandbuch. Standard – Sicherheitsmapnahmen. Bundesamt fur Sicherheit in der Informationstechnik. DBUS-Jahrestagung, 2004.

АСПЕКТЫ ПРЕПОДАВАНИЯ ТЕХНИЧЕСКИХ ДИСЦИПЛИН ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г.А. Власова

Стремительное развитие информационных технологий и их внедрение во все сферы жизнедеятельности человека требует подготовки все большего количества технических специалистов. В то же время рост потребности рынка труда не должен приводить к снижению качества подготовки кадров.

Базовыми навыками при подготовке специалистов по информационной безопасности являются умение представлять в аналитическом виде модели сигналов, осуществлять расчет временных и спектральных характеристик сигналов, знание математических моделей сигналов и принципов передачи сигналов по каналам связи и умение применять эти знания для решения теоретических и практических задач. Однако классические учебники, содержащие монохромные статические зависимости, тяжелы для усвоения современными студентами. Информация, содержащаяся в таких учебниках, воспринимается учащимися как устаревшая и сложная для восприятия. Поэтому для изучения математических моделей сигналов разработаны и используются в учебном процессе компьютерные программы для вуализации базисных функций, исследования их свойств и особенностей разложения различных сигналов в базисе данных функций. Рассматриваются следующие негармонические ортогональные нормированные полиномы: полиномы Чебышева 1-го рода; полиномы Лагерра, Лежандра и Эрмита. Программы позволяют: выбрать число базисных функций, увидеть значение каждой функции при произвольном значении аргумента на интервале определения, задать сигнал в виде функции и увидеть его представление во временной области и в виде спектра в выбранном базисе.

Использование в учебном процессе данных программ вызывает интерес у студентов, помогает изучить вопрос множественности спектров, формирует способность анализировать и оценивать собранные данные, навыки работы с компьютерной техникой, системного и сравнительного анализа, оптимизации параметров элементов и систем защиты информации.

АСПЕКТЫ ПРОЕКТИРОВАНИЯ УСТРОЙСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ДАТЧИКОВ И ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ IoT

Г.А. Власова

Интернет вещей (Internet of Things, IoT), рассматриваемый Советом Европы как основной путь развития информационных технологий, постепенно становится производственной системой. В том числе и на критически важных объектах информатизации: атомных станциях, нефтеперерабатывающих заводах, газопроводах, системах электроснабжения и т.д. Однако многочисленные примеры успешных атак на системы IoT говорят об их уязвимости. Значительная потенциальная опасность последствий, которые могут возникнуть в результате сбоев в работе системы, делают актуальной проблему обеспечения информационной безопасности IoT. Эффективным методом обеспечения защиты является применение криптографии. Однако не существует универсального решения для различных областей применения криптографических методов.

Для датчиков и исполнительных устройств в системе IoT характерны малые объемы передаваемой информации, низкое быстродействие (во многих случаях до 30 с). При этом требуются низкая стоимость (меньше стоимости датчиков), что влечет низкий объем доступной памяти, низкую потребляемую энергию (небольшая экономия на одном устройстве оборачивается большой для сети таких устройств). Однако надежность (криптостойкость) должна снижаться незначительно. Согласно рекомендациям американского Национального института стандартов и технологий (NIST) гарантированно обеспечивают высокий уровень безопасности симметричные алгоритмы с длиной ключа не менее 128 бит и асимметричные алгоритмы с длиной ключа не менее 3072 бит. Проведенные измерения для алгоритмов RSA-3072 , AES-128 и ECIES-256 на симуляторе микроконтроллера показали следующие

результаты. Алгоритмы RSA-3072 и AES-128 значительно (примерно в 3 раза) меньше используют память программ по сравнению с ECIES-256. Однако для памяти данных AES-128 уже не имеет такого значительного преимущества по сравнению с ECIES-256 (выигрыш приблизительно в полтора раза). RSA-3072 требует в 3,5 раз больше памяти данных по сравнению с ECIES-256 и в 5,4 раза больше по сравнению с AES-128. Для успешного запуска RSA-3072 требуются микроконтроллеры с минимум 32 КБ памяти.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНАХ И ПОДРАЗДЕЛЕНИЯХ ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ БЕЛАРУСЬ

С.Ю. Воробьёв, В.А. Русак

В XXI веке трудно найти какую-либо область из жизни общества, где бы не использовались способы обработки и передачи информации [1]. Информационная сфера Республики Беларусь стремительно развивается. По мере совершенствования и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых информационных технологий [2]. Наибольшую общественную опасность представляют правонарушения, связанные с неправомерным доступом к компьютерной информации. Требования к обеспечению технической защиты информации в органах и подразделениях по чрезвычайным ситуациям Республики Беларусь изложены в приказе МЧС от 11.03.2016 № 64 «Об информационной безопасности». Необходимо отметить усиление опасности несанкционированного доступа к компьютерной информации в связи с ростом различного способа использования компьютерных систем и сетей в органах государственного управления и государственных организациях.

Список литературы

1. Лемешевский О.О. Актуальные вопросы информационной безопасности на факультете внутренних войск МВД Республики Беларусь // Матер. междунар. науч.-практ. конф. «Теоретические и прикладные проблемы информационной безопасности». Минск, 18 мая 2018 г. С. 36–38.

2. Чижиков Э.Н. Защита информации в информационных системах МЧС России // Темат. сб. «Информационные технологии, связь и защита информации МВД России». Москва, 2012. С. 14–17.

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ

А.А. Гавришев, А.П. Жук

Авторами в работе [1] разработан обобщенный алгоритм защищенного информационного обмена в беспроводных системах безопасности. В работе [2] на основании работы [1] разработан усовершенствованный алгоритм защищенного информационного обмена с усложненной имитовставкой, состоящий из следующих шагов. 1. Инициализация генератора ПСП-1 управляющего блока. 2. Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока, и его отправка на генератор ПСП-2 блока контроля и в блок логической операции XOR. 3. Выбор из таблицы уникальных идентификационных данных (УИД) одного уникального значения, присвоенного каждому контролируемому объекту. 4. Сложение по правилу XOR значений первой ПСП-1 блока контроля и УИД выбранного контролируемого объекта. 5. Отправка полученного значения в накопитель хаотической последовательности (НХП), где оно перемножается с хаотическим сигналом (ХС), и передача полученного произведения на контролируемый объект. 6. Декодирование в контролируемом объекте полученного сигнала с помощью накопителя копии хаотической последовательности (НКХП), идентичного НХП в управляющем блоке. 7. Поступление декодированного сигнала в блок логической операции XOR контролируемого объекта, в который одновременно с этим приходит индивидуальное

значение УИД контролируемого объекта. 8. Получение в блоке логической операции XOR контролируемого объекта значения ПСП-1 блока контроля и его поступление в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока. 9. Выработка в генераторе ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока, последовательности ПСП-2. 10. Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок. 11. Декодирование в управляющем блоке полученного сигнала с помощью НКХП, идентичного НХП в контролируемом объекте. 12. Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в УС. 13. Выработка ПСП-2 управляющего блока и ее поступление в УС. 14. Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта. 15. Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма. 16. Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 17 алгоритма. 17. Вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

Список литературы

1. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена // Вестник СибГУТИ. 2018. № 1. С. 33–40.

2. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена для беспроводных систем безопасности с усложненной имитовставкой // Вестник НГУ. 2019. Т. 17, № 1. С. 18–27.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ УСТАНОВОК ДЫМОУДАЛЕНИЯ

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

При проектировании в соответствии с [1] установок дымоудаления (ДУ) в составе систем противодымной защиты (ПДЗ) в первую очередь определяется весовой, а затем объемный расход удаляемой газодымомвой смеси $L_Д$. Значение последнего определяется при нормированном [1] значении температуры удаляемых газов (более 300 °С) для подбора вентилятора. Кроме $L_Д$ для подбора вентилятора необходимо значение падения давления в сети $P_С$ установки ДУ. Давление $P_С$ рассчитывается в соответствии с [1] с учетом естественного давления газов $P_{ЕС}$, определяемого разностью удельных весов наружного воздуха и дыма (при температуре более 300 °С) и высотой шахты. При высоте шахты (здания) 50 м $P_{ЕС} \approx 300$ Па. Это давление вычитается из расчетного давления $P_С$ установки ДУ. Аэродинамические испытания установок ДУ проводятся при нормальной температуре в помещении (менее 30 °С) и параметрах Б [2] для теплого периода года для данного региона (26 °С для г. Минска). При таких температурах удельные веса удаляемого из помещения и наружного воздуха отличаются незначительно и давление $P_{ЕС}$ составляет единицы Па, и им можно пренебречь. То есть измерения объемного расхода газа, удаляемого установкой ДУ проводятся при давлении в сети отличающегося от проектного значения, а значит производительность вентилятора и объемные расходы будут отличаться, что может привести к тому, что измеренное значение объемного расхода воздуха $L_В$ будет существенно отличаться от проектного $L_Д$ (более 20 % [3]), что может быть причиной принятия решения о непригодности установки ДУ для эксплуатации.

Предлагается при проектировании установок ДУ выбор вентилятора осуществлять с учетом давления газов $P_{ЕС}$ при нормируемой температуре дыма (более 300 °С). Затем по аэродинамической характеристике выбранного вентилятора определять объемный расход удаляемого установкой воздуха при давлении в сети без учета давления $P_{ЕС}$ газов (воздуха). На основании чего определять объемный расход удаляемого через клапан ДУ воздуха $L_В$.

Список литературы

1. ТКП 45-4.02-273-2012. ПДЗ зданий и сооружений при пожаре. Системы вентиляции.
2. СНБ 4.02.01. Отопление, вентиляция и кондиционирование воздуха.
3. НПБ 23-2010. ПДЗ зданий и сооружений. Методы испытаний.

МЕТОДИКА НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СЕТИ

А.А. Горелик, Н.В. Журавский

В работе [1] для оценки защищенности узлов информационной сети предложено использовать программное средство «Сканер». В настоящей работе определен порядок настройки и эксплуатации указанного средства. Он включает в себя следующие этапы.

1. Вход в веб-интерфейс ПС «Сканер». Для этого необходимо открыть веб-обозреватель и перейти по адресу https://<IP-адрес сервера ПС «Сканер»>/. В результате будет открыто окно авторизации, в котором необходимо ввести имя пользователя и пароль.

2. В случае успешной авторизации – выбор ссылки «Задачи» в разделе «Сканирование» главного меню.

3. Запуск процесса сканирования. Для запуска стандартного сканирования следует выбрать «Мастер задач» и в открывшемся диалоговом окне указать IP-адрес или DNS-имя целевой системы (устройства). Для запуска расширенного сканирования в окне «Продвинутый мастер задач» необходимо выбрать дополнительные параметры сканирования, основными из которых являются следующие:

– «Конфигурация сканирования» – выбор предустановленной конфигурации сканирования;

– «Время запуска:» – время запуска задачи сканирования (немедленно или по расписанию);

– «Отправить отчет по электронной почте» – адрес электронной почты для отправки отчета.

4. Формирование отчета, содержащего результаты сканирования.

На основе данных, представленных в отчете, составляются рекомендации по совершенствованию механизмов защиты данных в исследованном объекте (информационной системе или информационной сети).

Список литературы

1. Горелик А.А., Бойправ О.В., Журавский Н.В. Методика анализа защищенности узлов вычислительной сети // Материалы XV Международной науч.-практ. конф. «Управление информационными ресурсами», Минск, 7 декабря 2018 г. С. 210–212.

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ ТЕХНОЛОГИИ HONEYPOT

В.И. Грицкевич, С.Н. Петров

В современном информатизированном мире для любой организации очень важно защитить свои активы от нападения злоумышленников. Чтобы приблизиться к обеспечению наиболее полной информационной безопасности, нужно быть на шаг впереди злоумышленников, таким образом, необходимо отражать атаки до наступления негативных последствий от их выполнения. Одним из таких инструментов для мониторинга поведения злоумышленников является технология Honeypot (далее – ханипот).

В ходе анализа существующих ханипотов был сделан вывод, что хорошим вариантом построения данной технологии является комбинирование автоматического подхода к решению задачи обнаружения атак и человеческих возможностей принятия решения. Архитектура такой системы может состоять из четырех различных компонентов, а именно: внешний брандмауэр, ханипот (виртуальная машина), база знаний и специальная группа SOC (Security operations center, центр реагирования на инциденты в сфере информационной безопасности) для ручного анализа журналов событий. В ней присутствуют различные модули для определения наиболее точных результатов, которые помогут администратору принимать решения на основе

автоматически генерируемых журналов событий. В рассматриваемом подходе задачей группы центра оперативного реагирования на инциденты в сфере информационной безопасности является ручной анализ данных из различных источников и принятие решения для какого-либо действия в зависимости от уровня критичности.

Ханипоты не могут полностью заменить такие средства защиты информации, как средства обнаружения вторжений или межсетевые экраны. Однако ханипоты являются прекрасным средством для изучения инструментария и методологии злоумышленников и улучшения систем защиты информации с помощью полученной информации. Помимо этого, благодаря возможности использования человеческих способностей для принятия решении о критичности события, ханипоты могут стать прекрасным дополнением функционирования центра оперативного реагирования на инциденты в сфере информационной безопасности (SOC).

Список литературы

1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.

2. Назначение технологии Honeypot. [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/275420.php?R=1 (дата обращения: 02.05.2019).

ОСОБЕННОСТИ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

М.В. Губич

Развитие информационного общества обусловило рост количества информации в электронном виде, подлежащей защите, и регистрируемых киберпреступлений, что в свою очередь повлекло необходимость подготовки квалифицированных кадров, обученных общим вопросам обеспечения информационной безопасности, и отдельной категории сотрудников, способных эффективно противодействовать преступлениям в сфере высоких технологий.

В связи с этим одной из основных целей профессиональной подготовки специалиста юридического профиля для правоохранительной сферы становится непрерывная компьютерная подготовка, в рамках которой должна быть сформирована готовность к использованию информационно-коммуникационных технологий (ИКТ), являющаяся базовой основой для развития компетенций в области информационной безопасности. К составляющим готовности к использованию ИКТ мы относим теоретические знания, технологические умения, навыки и профессиональные качества, личностные и мотивационные качества.

Соответственно, концепция формирования готовности к использованию ИКТ, на наш взгляд, должна быть основана на принципах обучения, способствующих овладению умениями решать профессиональные задачи и проблемы правоохранительной сферы на базовом (на уровне пользователя на основе выполнения установленных требований по информационной безопасности), углубленном (на уровне продвинутого пользователя, осуществляющего мероприятия по обеспечению информационной безопасности собственного рабочего места пользователя на основе выполнения требований технических и иных нормативных правовых актов) и специальном уровнях (умение решать служебные задачи на основе внедрения в служебную деятельность новых ИКТ, разработки собственных систем и средств обеспечения информационной безопасности рабочих мест пользователей ИКТ организации, а также противодействовать компьютерной преступности).

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ПОМОЩЬЮ ПОИСКОВОЙ СИСТЕМЫ SHODAN

Ш.Р. Давлатов

Shodan – это ведущая поисковая система по Интернету вещей, существующая уже более семи лет. В отличие от популярных поисковых движков (Google, Yandex, Bing и др.), которые ищут в сети информацию из обычных сайтов, система Shodan работает с теневыми каналами

Интернета. Она позволяет искать серверы, веб-камеры, принтеры, роутеры и самую разную технику, которая подключена к глобальной сети и составляет его часть. Shodan работает 24 часа в сутки, 7 дней в неделю, собирая информацию о 500 млн подключенных устройствах к сети Интернет ежемесячно. К основным фильтрам поисковой системы относятся: City/Country (фильтрация устройств, расположенных в пределах заданного города/страны, например, city:minsk); Port (вывод устройств с заданным открытым портом, например, port:443); OS (фильтрация устройств, которые работают на заданной операционной системе, например, os:linux); Geo (применяется для точного задания координат расположения устройства в формате долгота-широта, например, geo:42.9693,-74.1224); Net (используется для поиска устройств из заданного диапазона ip-адресов, например, net:216.0.0.0/16);

В данной работе представлены результаты интеграции системы Shodan с метапоисковой платформой Maltego, которая широко применяется для построения и анализа связей между различными интернет инфраструктурами (веб-сайты, dns-имена, ip-адреса и др.). Особенностями данного подхода являются визуализирование, обработка и комбинирование информации для более детального анализа данных, полученных из поискового движка Shodan. Результаты исследования могут быть использованы специалистами по информационной безопасности на начальных этапах проведения аудита автоматизированных систем (сбор первичной информации, автоматизация процесса анализа данных, тестирование объекта защиты на проникновение).

ИДЕНТИФИКАЦИЯ АКУСТИЧЕСКИХ СИГНАЛОВ МЕТКАМИ С КОДОМ БАРКЕРА

Г.В. Давыдов, В.А. Попов

Проверка защищенности речевой информации включает элемент оценки звукоизоляции помещений. Для этих целей используются как тональные сигналы, так и «белый» шум. Однако при приеме акустического сигнала за пределами помещений трудно выделить тестируемый сигнал на фоне производственных шумов.

Проанализированы методы встраивания меток в акустические сигналы, включающие тональные сигналы, «белый» шум, речевые и речеподобные сигналы, для целей определения способности акустических сигналов проходить через ограждающие элементы конструкций помещений. При этом в качестве меток широко используются коды Баркера. Коды Баркера являются оптимальными кодами, что заключается в том, что амплитуда автокорреляционной функции равна числу элементов кода, а значение боковых лепестков равно 1. Такие методы применяются для автоматического обнаружения акустических сигналов и их аутентификации [1]. Применение методов стеганографии не представляется возможным из-за того, что зондирование выполняется акустическим сигналом, а метод стеганографии предусматривает введение информации в цифровой сигнал за счет использования последних разрядов акустического цифрового сигнала.

На основании проведенного анализа разработан алгоритм встраивания меток с кодом Баркера в акустические сигналы, который включает формирование и излучение в акустическом виде в проверяемом помещении тестовых сигналов с амплитудно-импульсной модуляцией с использованием кодов Баркера для подтверждения присутствия зондирующего акустического сигнала. Предлагается использовать коды Баркера с числом разрядов 11.

Большое влияние на выбор кода и алгоритма кодирования тестового сигнала оказывает канал связи. В связи с тем, что канал связи обладает неравномерной амплитудно-частотной характеристикой, обусловленной резонансными свойствами ограждающих элементов конструкций помещений, наиболее приемлемым видом модуляции будет амплитудно-импульсная или частотная. Рассматриваются наиболее распространенные методы декодирования и обнаружения меток в тестируемом сигнале и вопросы выбора оптимальных требований для решения поставленной задачи.

Список литературы

1. Воробьев В.И., Давыдов Г.В., Лещенко Д.В. Обнаружение акустических сигналов на фоне речи // Доклады БГУИР. 2003. Т.1, №2/1. С. 48.

ПОЛУЧЕНИЕ СТАТИСТИЧЕСКИХ ДАННЫХ ОБ УМЕНЬШЕНИИ ЧИСЛА ОШИБОК В ПРИКЛАДНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММАХ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.С. Дик, В.Т. Лэ, С.М. Боровиков

Прикладное программное обеспечение является составной частью систем обеспечения информационной безопасности и его надежность во многом определяет эффективность функционирования этих систем. Актуальным является оценка надежности прикладного программного обеспечения на ранних этапах его разработки. Определив ожидаемые показателями надежности программного обеспечения, и зная состав используемых аппаратных частей в системе обеспечения информационной безопасности, можно спрогнозировать эффективность функционирования системы. Авторами предлагается подход к оценке надежности прикладного программного обеспечения на ранних этапах его разработки. Подход основан на статистических моделях определения ожидаемого числа ошибок в компьютерной программе и, следовательно, ее надежности. Статистические модели должны помочь проектировщикам определять значения коэффициентов, показывающих степень уменьшения числа возможных ошибок в компьютерной программе в зависимости от таких факторов как область применения прикладного ПО (телекоммуникационные системы, мобильные электронные устройства, автоматизированные системы управления и т.д.), квалификация и опыт программистов, среда разработки ПО (язык программирования, операционная система, компьютерная сеть), степень использования стандартных модулей, используемые технологии и условия проведения тестирования программы. Указанный подход был изложен в работах [1, 2]. Для получения статистических моделей подготовлена анкета опроса специалистов и получены первые результаты. Для ознакомления с этими материалами можно обращаться по e-mail: bsm@bsuir.by или на кафедру ПИКС БГУИР (ауд. 37 1-го учебного корпуса).

Список литературы

1. Боровиков С.М., Дик С.К. Прогнозирование ожидаемой надежности прикладных программных средств с использованием статистических моделей их безотказности // Сб. материалов IV Междунар. науч.-практ. конф. «BIG DATA Advanced Analytics». Минск, 3–4 мая 2018 г. С. 348–354.

2. Боровиков С.М., Лэ В.Т., Дик С.С. Возможный подход к оценке надежности прикладных программных средств для технологий big data // Сб. материалов V Междунар. науч.-практ. конф. «BIG DATA and Advanced Analytics» Минск, 13–14 марта 2019 г. В 2 ч. Ч. 2. С. 77–83.

ОПТИЧЕСКОЕ ИНИЦИИРОВАНИЕ РЕАКЦИЙ БЫСТРОГО ОКИСЛЕНИЯ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ

А.В. Долбик, А.С. Лазарук, В.А. Лабунов

Пористый кремний широко исследуется из-за его высокой удельной площади поверхности, уникальных оптических свойств и совместимости с процессами изготовления микросистем. Это делает его привлекательным материалом для ряда применений, включая оптические биосенсоры, солнечные элементы, энергетические материалы. Пористый наноструктурированный кремний, пропитанный твердотельным окислителем, демонстрирует процессы горения и взрыва, приводящие даже к полному разрушению подложки, на которой он был сформирован. В работе исследовалась возможность оптического инициирования экзотермической реакции окисления пористого кремния, пропитанного раствором окислителя.

Изготовление пористого кремния проводили на кремниевых подложках *p*-типа с удельным сопротивлением 10 Ом·см путем электрохимического анодирования. Анодирование проводили при плотности тока 50 мА/см^2 в 33 % растворе плавиковой кислоты. В таком режиме на пластинах образуется нанопористый кремний с диаметром пор от 2 до 5 нм, а площадь их удельной внутренней поверхности достигает величины более 200 м^2/см^3. В качестве окислителя использовали раствор нитрата калия. Оптическое инициирование экзотермической

реакции окисления пористого кремния производилось инфракрасным и ультрафиолетовым лазерами. Так оптическое инициирование осуществляли излучением Nd^{3+}:$YAlO_3$ лазера с модулированной добротностью ($\lambda = 1080$ нм, $\tau = 15$ нс) или излучением его третьей гармоники ($\lambda = 360$ нм). Плотность мощности светового потока варьировалась от 20 до 150 МВт/см^2. Проведенные исследования показали, что процессы быстрого окисления в пористом кремнии могут быть инициированы одиночным световым импульсом лазера. Пороговая плотность мощности лазера необходимая для этого составляла 38 МВт/см^2.

Оптическое инициирование предоставляет возможность дистанционного инициирования реакции окисления пористого кремния находящегося, например, на кремниевой подложке микросистемы. Возникающая реакция окисления может приводить к разрушению микросистемы и, следовательно, невозможности несанкционированного копирования информации, хранимой в микросистеме.

ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ ГОЛОСОВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

А.О. Дударенков, О.Б. Зельманский

Речевые сигналы представляют собой наиболее уязвимый тип данных и очень часто остаются открытыми и легкодоступными. Несанкционированный доступ к каналу передачи речевой информации может привести к утечке конфиденциальных данных. Проведенный анализ действующих стандартов мобильной связи показал, что в них содержится большое количество уязвимостей [1, 2].

Предлагается программный модуль обеспечения безопасности речевой информации в сетях мобильной передачи данных [3]. Данный модуль может быть использован для дополнительного и независимого шифрования информации в мобильных сетях различных стандартов. В основу предлагаемого модуля положен алгоритм шифрования AES. Модуль написан на языке программирования Java. Для его работы потребовался дополнительный кодек: Apache Commons Codec 1.11. Пакет кодека содержит простой кодер и декодер для различных форматов данных, а также большую коллекцию утилит для фонетического кодирования. Модуль состоит из блоков записи речи в аудиофайл, подачи ключа и шифрования, ввода ключа для расшифрования.

В процессе тестирования модуля был создан аудиофайл, содержащий речь. Файл подавался на вход приложения, далее происходило его преобразование в массив значений амплитуд для последующего шифрования и вывод зашифрованного файла для анализа. Далее осуществлялось дешифрование. На каждом этапе выполнялся анализ получаемых файлов посредством вывода их спектрограмм.

Список литературы

1. Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm / K. Merit [et al.] // IJDPS. 2012. № 3.

2. Real-Time End-To-End Secure Voice Communications Over GSM Voice Channel / N.N. Katugampala [et al.] // Signal Processing Conference. 2005. № 13.

3. Khomo K.B., Ogorodnikov E.A., Zelmanski O.B. Protecttion of speech information during transmission via mobile networks // Тез. докл. XVI Белоруско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 10.

МОДЕЛЬ РАСЧЕТА ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ТРАНСФОРМАТОРОВ ЭЛЕКТРОПИТАНИЯ ЭЛЕКТРОННОЙ АППАРАТУРЫ

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

В настоящее время ведущие страны мира используют свои методики расчета эксплуатационной надежности трансформаторов электропитания электронной аппаратуры. Методики основаны на моделях надежности, которые отличаются номенклатурой и числом

параметров трансформаторов, принимаемых во внимание при расчете. Поэтому разные методики расчета надежности одного и того же трансформатора дают разные результаты. Актуальным является вопрос о выборе (или разработке) модели, которая обеспечивала бы результаты расчета, подтверждаемые практикой. Для этого был проведен обзор методик, используемых в США, России, Китае и Франции для расчета эксплуатационной надежности трансформаторов. Акцент был сделан на параметры трансформаторов, учитываемые при расчете. В качестве примера отметим, что в справочнике Китая «Reliability Prediction Calculation Model For Electronic Equipment in GB/z 299B» [1] приводится модель, учитывающая назначение трансформатора, температурный режим и условия его работы, уровень качества при изготовлении в условиях производства. Однако эта модель не учитывает особенности электрических и конструктивных различий трансформаторов. К таким особенностям можно отнести входные и выходные рабочие напряжения, материал и тип магнитопровода, количество обмоток. Подобные недостатки характерны и для моделей других стран. В работе предлагается модель надежности трансформаторов, которая учитывает (кроме традиционных факторов) тип и материал магнитопровода, число обмоток, диаметр обмоточных проводов.

Список литературы

1. Reliability Prediction Model for Electronic Equipment : The Chinese Military / Commercial Standard GJB/z 299B. Yuntong Forever Sci.-тек. Co. Ltd. China 299B.

ТРЕБОВАНИЯ К ДИКТОРАМ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

Б.Б. Ергалиева, А.В. Потапович

Основные требования к дикторам – эта способность обладать хорошо поставленным голосом, четко читать связный текст со скоростью 70–80 слов в минуту при разности между средней амплитудой 10 максимальных значений речевого сигнала в течении прочтения 200 слов связного текста и среднеквадратичного значения речевого сигнала за этот период не менее 18 дБ. При отборе дикторов необходимо уделять внимание на произношение ими трудных по артикуляции согласных звуков р, л, с, з, ш, ж, ч, щ (не иметь дефектов речи). Если при артикуляции гласных звуков речевой аппарат открыт и свободно пропускает воздух и при этом возбуждаются колебания голосовых связок то, при артикуляции согласных речевой аппарат образует скоординированное положение языка, губ, полости рта и носа и имеет достаточно сильное мускульное напряжение. Следует заметить, что артикуляционный аппарат человека формируется в детском возрасте и обучение дикторов можно проводить после отбора лиц с хорошо развитым артикуляционным аппаратом. Обучение дикторов включает постановку правильного дыхания, детальное ознакомление с текстом.

Дикторы должны быть отобраны из людей в возрасте от 18 до 30 лет с хорошей артикуляцией. Количество дикторов должно быть не менее 10 человек, 5 мужского пола и 5 женского. Предварительный отбор дикторов может включать и большее количество, потому что после записи фонограмм и их обработке некоторые записи будут отбракованы по отношению максимальных уровней звукового давления речи к среднеквадратичному значению, которое должно быть не менее 18 дБ.

Обучение диктора заключается в постановке правильного дыхания при чтении текста. При правильном дыхании речевой аппарат не переутомляется и обеспечивается сила голоса, богатство динамических оттенков и мелодичность речи.

Данная работа выполнена при поддержке грантового финансирования КН МОН РК, № AP05130293.

Список литературы

1. Попов В.А., Готовко М.А. Методы отбора аудиторов и дикторов для оценки разборчивости речевой информации // Тез. докл. XIII Белоруско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 4–5 мая 2015 г. С 16.

2. СТБ ГОСТ Р 50840-2000. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости.

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА В ОБЕСПЕЧЕНИИ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

А.В. Железняков

Для технической поддержки действий по обеспечению физической защиты объектов и размещенных на них предметов физической защиты применяются комплексы технических средств физической защиты. Комплекс выполняет задачи по сбору, обработке, анализу и контролю всей информации, получаемой от технических средств физической защиты, формирует и передает сообщения подразделениям охраны и органам управления, обеспечивает информационное взаимодействие между пунктами управления, контролирует состояние и работоспособность инженерно-технических средств физической защиты.

В связи с тем, что наиболее вероятным и опасным элементом воздействия на комплекс технических средств физической защиты является человек, то особую роль в комплексе играет система контроля и управление доступом (СКУД).

Главная задача системы контроля управления доступом – сбор полной информации о проникновении на объект.

Функции же СКУД определяются как:

– защита от проникновения на объект лиц без права доступа – благодаря установке СКУД, за ограждение попадают только сотрудники или люди, получившие пропуск.

– защита других лиц, т. е. обеспечить безопасность людей, которые могут по неосторожности попасть на территорию охранных объектов, производства или строек, где можно получить травму;

– контроль за прохождением персонала на территорию объекта, а также сбор информации о длительности пребывания;

– контроль за перемещением сотрудников – эта функция действует, если зоны внутри территории разграничены.

Повышение эффективности использования СКУД возможно наращиванием устройств, подключением интеллектуальных систем видеонаблюдения и др.

СТОХАСТИЧЕСКИЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

А.П. Жук, К.М. Сагдеев, А.А. Гавришев, А.Ю. Муравьев

Современные технологии беспроводной передачи информации (БПИ) активно внедряются и широко используются как в производственной деятельности большинства компаний, так и для построения компьютерных сетей для частного использования. Не смотря на различное назначение систем БПИ, их объединяет одно очень важное обстоятельство – значительный ущерб от нарушения безопасности передаваемой информации [1]. Существующие методы защиты информации в системах БПИ ориентированы, в том числе, на использование криптографических алгоритмов и совершенствование системы аутентификации пользователей. Дальнейшее усложнение существующих или применение более совершенных алгоритмов аутентификации и шифрования передаваемой информации неизбежно сказывается на быстродействии систем БПИ, что снижает показатели качества их функционирования. В связи с этим в докладе поставлена задача усовершенствования методов защиты информации в рассматриваемых системах [2]. Поставленную задачу предлагается решать на основе стохастического преобразования информации универсальным способом, позволяющим обеспечить эффективную защиту данных в системах БПИ [3]. Преимущество данного подхода заключается в том, что в рамках одного алгоритма обеспечивает решение задачи абсолютной секретности в постановке К. Шеннона.

Список литературы

1. Применение сложных сигналов в системах радиосвязи и управления / С.С. Кукушкин [и др.] // Современные тенденции развития науки и технологий. 2015. № 2-2. С.94–96.
2. Осмоловский С.А. Стохастические методы защиты информации. М.: Радио и связь, 2003. 320 с.
3. Жук А.П., Жук Е.П. Способ повышения помехозащищенности систем связи с ортогональными сигналами // Инфокоммуникационные технологии. 2005. Т. 3, № 4. С. 39–41.

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЫДЕЛЕННОМ ПОМЕЩЕНИИ ПРЕДПРИЯТИЯ

Е.П. Жук, М.А. Брехов, Р.Р. Партоян, Е.В. Черкашин

В настоящее время остро стоит задача обеспечения защиты речевых переговоров от скрытого протоколирования. Для этих целей на предприятиях создаются специальные выделенные помещения, которые оснащаются активными и пассивными средствами защиты информации. В зависимости от корректности предварительного обследования и поиска уязвимостей, строится система защиты информации выделенного помещения, которая имеет конкретную величину стоимости [1]. В данной работе рассматриваются проблемы организации защиты выделенного помещения от несанкционированного съема речевой информации по акустическому каналу, а так же обнаружения уязвимых мест [2].

Известные подходы к построению системы защиты акустической информации в выделенных помещениях ориентированы на достижение конечного результата, заключающегося в обеспечении требуемого уровня защищенности информации без явного учета приемлемого уровня затрат на построение системы защиты. В докладе рассматривается подход, позволяющий учитывать уровень затрат на построение системы защиты акустической информации в выделенном помещении предприятия [3], с учетом уязвимостей, степени конфиденциальности информации и некоторых особенностей вариантов достижения требуемого результата.

Список литературы

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. 436 с.
2. Зашита информации / А.П. Жук [и др.]. М.: РИОР: ИНФРА-М, 2019. 400 с.
3. Жук А.П., Гавришев А.А., Осипов Д.Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе матрицы нечетких правил // Математические структуры и моделирование. 2016. № 1 (37). С. 112–120.

ФИЛЬТРАЦИЯ СЕГМЕНТНОЙ ПРОЕКЦИИ СИМВОЛЬНОЙ СТРОКИ НА ЭТАПЕ СЕГМЕНТАЦИИ

Д.В. Заерко, В.А. Липницкий

В современную информационную эпоху хранение и передача цифровых сигналов и изображений осуществляется, как правило, в преобразованном или сжатом виде. Процесс их передачи происходит в неизбежно зашумленной среде. Поэтому не подлежит сомнению факт, что в реальных условиях является постоянной проблема восстановления и распознавания переданных изображений. На путях решения этой проблемы накоплен богатый спектр методов и подходов.

Важное место занимает класс изображений с символьной строкой, также подлежащей распознаванию. Типичным примером здесь является сюжет с идентификацией номерных знаков движущегося транспортного средства. В случае основательной зашумленности

символьной строки и невозможности ее однозначного прочтения стандартными техническими средствами производится основательная обработка этого носителя информации.

Наиболее часто на первоначальном этапе предполагается проведение посимвольной сегментации строки. Как правило, сегментация строки проводится на основе анализа ее проекции на параллельную ось, вертикальной или горизонтальной проекции [1]. С целью определения и исправления зашумленных фрагментов непосредственно на этапе сегментации проекции оправдано использование своего рода фильтра. Он позволяет преобразовать зашумленный сегмент проекции символа к его шаблону (скелету), не имеющему помех [2]. Определение и устранение шумов на начальном этапе распознавания значительно ускорит процесс распознавания в целом, а также позволит использовать менее мощные вычислительные устройства.

Модифицированный алгоритм фильтрации, совмещенный с сегментаций, основывается на идее, что значение проекции на определенном фрагменте для отдельного символа может быть четко сопоставлена с конечным набором модельных проекций. В таком случае каждый элемент набора модельной проекции характеризует только один единственный символ алфавита с некоторой допустимой погрешностью. Если этап распознавания, следующий за этапом сегментации, не дал удовлетворительных результатов, возможна повторная сегментация.

В докладе подробно рассматриваются детали и процедура фильтрации – нового этапа в распознавании символьных строк.

Список литературы

1. Sawaki M., Hagita N. Text-Line Extraction and Character Recognition of Document Headlines With Graphical Designs Using Complementary Similarity Measure // IEEE Trans. PAMI. 1998. Vol. 20, № 10. P. 1103–1109.

2. Заерко Д.В., Липницки В.А. Применение модифицированных алгоритмов JavaANPR для автоматического распознавания номеров автомобилей // Матер. междунар. науч. конф. «Информационные технологии и системы 2018». Минск, 25 октября 2018 г. С. 286–287.

АГРЕГАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ SCRIPTRUNNER В СИСТЕМЕ JIRA

А.Д. Зайков

Лучшим решением для организации безопасной работы, отличным инструментом планирования, отслеживания ошибок или этапов итеративного процесса в современной ИТ-компании является система JIRA. При разработке программного обеспечения всегда важно помнить не только о деталях, но и об общей концепции. Особенность JIRA состоит в том, что проект разбивается на задачи, работа над каждой из которых ведется обособленно. Система умело акцентирует внимание администратора на деталях проекта. В конкретном ИТ-проекте всегда следует завершить одни задачи, и затем переходить к следующим. Цикл жизни каждой задачи напоминает принцип работы каскадной модели: спецификация, разработка, улучшение, тестирование, релиз. Однако, в целом, можно отметить отход от каскадной модели к гибкой методологии разработки, и один большой каскад заменяется тысячами поменьше [1, 2].

В работе предлагается организация новых технических решений для автоматического подсчета текущего курса валюты Национального Банка Республики Беларусь, который использует REST API Национального Банка Республики Беларусь, для получения данных о курсах в момент закрытия задачи в системе JIRA (или последнего трекинга в ней). Полученные данные агрегируются с ограничением доступа; для реализации такого функционала используется плагин ScriptRunner, позволяющий встраивать Groovy-скрипты в настраиваемые поля, а также работать с событиями задач в JIRA. Данные о курсах валют используются в дальнейшем для автоматического подсчета себестоимости ИТ-проекта и оценки трудозатрат на нем. Для этого были созданы дополнительные пользовательские поля с использованием языка Groovy. Доступ к редактированию данных полей ограничен для всех пользователей. Для администраторов и группы top-management в системе JIRA настроен доступ просмотра данных полей, согласно полученному техническому заданию. В дальнейшем

в проекте будет разработан функционал для генерации дополнительных отчетов для оценки загруженности сотрудников, а также обновления текущие отчетов в eazyBI.

Список литературы

1. JIRA documentation // Atlassian [Электронный источник]. URL: https://confluence.atlassian.com/jiracoreserver071/jira-core-documentation-802172329.html/ (дата обращения: 12.04.2019).

2. JIRA Software // TOPSAAS [Электронный источник]. URL: http://topsaas.ru/jira.html/ (дата обращения: 19.04.2019).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Д.В. Зезина, А.Ю. Хохлов

В работе рассматриваются основные меры, которые необходимо учитывать при проектировании системы защиты данных на предприятии. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Популярные инструменты и технологии современной повседневной жизни, такие как мобильные телефоны, веб-почта, службы мгновенных сообщений, съемные носители и беспроводной доступ к Интернету дали каждому возможность легко переносить и обрабатывать большое количество данных. Наряду с возможностью переноса данных многие организации создали информационные системы вокруг своих продуктов и услуг на основе открытых стандартов и интерфейсов совместимых с популярными устройствами. Кроме того, организации способствуют легкому доступу к данным как для персонала, так и для широкой публики через Интернет. Но недостатком этого удобства является большая вероятность передачи конфиденциальных корпоративных данных посторонним лицам. Поэтому актуальность рассматриваемой темы в том, что в наше время остро встает вопрос о необходимости защищать информацию своего предприятия различными методами, но многие не знают, что следует делать, дабы сохранить те или иные сведения в тайне, с выгодой реализовать их и не понести убытки от их утечки или утраты. Данные являются одним из наиболее важных активов любой организации и люди обычно считаются самым слабым звеном в цепи безопасности. Крайне важно чтобы сотрудники полностью осознавали свои обязанности, их ограничения на доступ к информации и дисциплинарные меры, которые будут приняты за любое нарушение безопасности. Все это может служить движущей силой для самосовершенствования с точки зрения безопасности данных.

УПРАВЛЯЕМОЕ КОДИРОВАНИЕ КОМБИНАЦИОННЫХ СХЕМ

Л.А. Золоторевич, А.В. Павлова

В последнем десятилетии значительно возрос ущерб от пиратства и других угроз в области производства аппаратного обеспечения и составляет около 4 млрд. долларов в год, что примерно в 10 раз превышает ущерб от пиратства в области ПО. Для решения проблемы в работе [1] предлагается подход к проектированию Design for-Trust (DfTr) как развитие теории контролепригодного проектирования (Design-for-Testability – DfT), который дополнительно включает средства для контроля и предотвращения аппаратных атак при проектировании и изготовлении СБИС.

В работе [2] проанализированы различные модели процесса злонамеренного искажения проекта, описывающие условия, при которых подобное искажение может внедриться в цифровую систему. В числе возможных источников искажений рассматриваются поставщики базовых функциональных блоков интеллектуальной собственности (IP's), которые приобретаются разработчиками СнК, собственно разработчики СнК, а также кремниевые фабрики – изготовители СнК.

Основная идея защиты проектов от неавторизованного пользователя основана на кодировании комбинационных схем цифровых устройств. Защита базируется на введении дополнительных логических элементов в структуру схемы, формировании ключевого кода, применение которого вводит схему в область правильного функционирования [3]. Основная задача, которая должна быть решена для эффективной практической реализации данной общей идеи, заключается в том, чтобы определить оптимальное множество внутренних линий схемы и количество ключевых элементов для создания максимальных трудностей для злоумышленника по поиску правильного ключа.

В докладе задача кодирования сводится к поиску неисправностей константного типа кодируемой структуры, обнаруживаемых на большем количестве выходных линий и на максимальном количестве входных векторов. Для решения задачи применяются методы и средства тестового диагностирования [4, 5].

Список литературы

1. Security analysis of integrated circuit camouflaging / J. Rajendran [et al.] // ACM SIGSAC conference on Computer & communications security. Berlin. 4–8 November 2013. P. 709–720.

2. Hardware Trojans: Lessons learned after one decade of research / K. Xiao [et al.] // ACM transactions on design automation of electronic system. 2016. Vol. 22. No. 1.

3. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos [et al.] // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). 2017. P. 221–226.

4. Золоторевич Л.А. Функциональный контроль СБИС типа СнК // Сб. науч. статей «Технологии автоматизации и управления». 2017. Вып. 3. В 2 кн. Книга 2. С. 216–225.

5. Золоторевич Л.А. Модели неисправностей при верификации проектов и контроле цифровых систем // Матер. Междунар. науч. конф. «Компьютерные науки и информационные технологии». Саратов, 2018. С. 160–163.

МЕТОДЫ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ В ПОСТРОЕНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.М. Кадан

Модель вероятного нарушителя информационной безопасности важна для систематизации данных о возможностях и типах нарушителей, целях их несанкционированных воздействий и выработки адекватных организационных и технических методов противодействия. Правильно разработанная модель вероятного нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности: опираясь на построенную модель, можно строить адекватную систему информационной защиты. При разработке модели нарушителя обычно учитывают: категории лиц, к которым можно отнести нарушителя; цели, градации по степени опасности и важности; анализ его технических возможностей; предположения и ограничения о характере действий.

В докладе предлагается и демонстрируется построение модели вероятного нарушителя на основе анализа лог-файлов информационной системы. Анализ ведется с использованием методов поведенческой аналитики, среди которых выделяется метод когортного анализа [1]. Когортный анализ рассматривает данные из некоторого набора данных (например, платформы электронной коммерции, веб-приложения или онлайн-игры), и вместо того, чтобы рассматривать всех пользователей как единое целое, разбивает их на связанные группы. Идея когортного анализа состоит в том, чтобы выполнить такое разбиение по определенным признакам или похожему поведению, и отслеживать развитие этих групп во времени в течение определенных временных интервалов. Построение модели нарушителя было продемонстрировано на примере информационной системы, являющейся компьютерной игрой для социальных сетей. Использование лог-файлов такой системы позволило получить для исследования набор данных объемом более 600 ГБ, содержащий около 10^{10} записей о поведении более 35 млн. пользователей. В качестве основных характеристик рассматривалась минимизация финансовых потерь разработчика от применения целенаправленной рекламы.

Список литературы

1. Aukeman, Mark. Cohort Analysis – understanding your customers / edwblog.com | EDW+ Delivering on the Big Data promise [Электронный ресурс]. URL: http://edwblog.com/adhoc/cohort-analysis-%E2%80%94-understanding-customer-behavior/32 (дата доступа: 09.05.2019).

БЕЗОПАСНОСТЬ СИСТЕМЫ И СИСТЕМА ОТКАЗОУСТОЙЧИВОСТИ

Камил Ихаб Абдулджаббар Камил, М.Б. Абросимов

Отказоустойчивость компьютерной системы – это способность системы продолжать сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Начиная с середины 90-х годов быстрое развитие вычислительных программных приложений, работающих в режиме реального времени, особенно спроса на интеллектуальные устройства, встроенные в программное обеспечение, породило насущную проблему, связанную с отказоустойчивостью программного обеспечения. Неизбежность появления проблемы заключается в том, что синтез системы выполняется лицом, не являющимся специалистом этой системы. Большинство людей, регулярно пользующиеся компьютерами, сталкиваются с проблемой сбоя системы либо сбоев программного обеспечения, работы диска, потери питания, либо в результате ошибки шины. В некоторых случаях эти сбои не более чем мелкая неприятность; в других же случаях они приводят к значительным потерям. Второй вывод, вероятно, станет более распространенным, нежели предыдущий, поскольку зависимость общества от автоматизированных систем возрастает. Отказоустойчивая система должна быть в состоянии устранять неисправности отдельных аппаратных или программных компонентов, устранять сбои питания или другие виды неожиданных аварий и по-прежнему соответствовать своей спецификации. Отказоустойчивость необходима еще и потому, что без нее практически невозможно создать идеальную систему.Надежность системы – это вероятность того, что она будет оставаться работоспособной (потенциально, несмотря на сбои) в течение всего периода работы. Наличие у системы очень высокого уровня надежности наиболее значимо в критически важных приложениях, связанных с управлением космическими кораблями многоразового использования или промышленными объектами, в работе которых любой сбой может повлечь гибель людей [1]. Безопасность и надежность системы – это те вопросы, которые становятся все более важными в сегодняшнем развивающемся мире. Безопасность, гарантирующая выполнение системой требуемой работы, идет рука об руку с надежностью, гарантирующей правильность работы системы. Взаимодействие безопасности и надежности является краеугольным камнем бесперебойной работы функциональной системы на долгие годы. Безотказность работы системы является одним из аспектов ее надежности; однако она по своей природе более сложна, чем безопасность системы, поскольку она содержит атрибуты триады информационной безопасности (CIA) («конфиденциальность, целостность и доступность»). При этом к трем указанным атрибутам необходимо добавить три других: защищенность (безопасность), эксплуатационная технологичность и надежность. Защищенность (безопасность) системы характеризуется «отсутствием аварийных последствий для пользователей и окружающей среды». Эксплуатационная технологичность означает способность системы производить текущий ремонт, техническое обслуживание и вносить другие изменения, такие как исправления и обновления системы. Поскольку безопасность и надежность системы направлены на решение одной и той же цели, способствующей ее доступности, надежность системы тесно взаимосвязана с ее безопасностью. В большинстве случаев мы можем утверждать, что более надежная система должна быть безопасной. Меры безопасности применяются к системе с целью обеспечения ее надежности; но, если вследствие атаки будет нанесен ущерб безопасности системы, то тогда доступ к ней будет прекращен в тех случаях, когда надежность системы гарантирует ее доступность[2].

Список литературы

1. Basic Concepts and Taxonomy of Dependable Secure Computing / Avizienis Algirdas [et al.] // Process for developing common vocabulary in the information security area. 2007. № 1. P. 10–51.

2. Comparing reliability and security: Concepts, requirements, and techniques / R.S. Hanmer [et al.] // Bell Labs Technical Journal. 2007. № 3. P. 65–78.

ИСПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ МЕХАТРОННЫХ СИСТЕМ НА МНОГОКООРДИНАТНОМ КОЛЬЦЕВОМ ПРИВОДЕ

С.Е. Карпович, Г.Й. Салманзадех, М.М. Форутан

На сегодняшний день весьма актуальной является задача построения и исследования исполнительных механизмов параллельной кинематики для мехатронных систем координатных перемещений широкого спектра применений, в том числе и в технических средствах защиты информации. Они должны обеспечивать возможность структурного реконфигурирования в зависимости от требуемой реализации пространственных перемещений системы, в которую встраивается эта мехатронная система. Среди кинематических характеристик, в первую очередь, необходимо учитывать способность реализации программируемых движений с заданным числом степеней свободы, поскольку влияние данного параметра на выбор структуры, конструкции и остальные характеристики является определяющим.

Решение этой задачи нами было выполнено на структурно-топологическом уровне [1, 2], что позволило разработать концепцию построения управляемого движения в трехмерном пространстве на базе композиционного использования многокоординатного привода прямого действия и реконфигурируемых механизмов параллельной кинематики. В соответствие с этой концепцией в настоящей работе исследованы две системы перемещений, полученные нами путем реконфигурирования механизма параллельной кинематики на гибридном кольцевом приводе прямого действия.

Список литературы

1. Системы многокоординатных перемещений и исполни-тельные механизмы для прецизионного технологического оборудования / В.В. Жарский [и др.]. Минск: Бестпринт, 2013. 208 с.

2. Литвинов Е.А., Жарский В.В., Ареби М.А. Построение многокоординатной системы перемещений на базе механизма параллельной кинематики // Доклады БГУИР. 2009. № 8 (46). С. 79–84.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА DES НА БАЗЕ FPGA

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

Быстрое развитие систем связи и расширение использования Интернета привели к возросшей потребности в эффективной безопасности и надежности передачи, обработки и хранения данных. Алгоритмы шифрования являются одним из механизмов обеспечения этой безопасности, при этом выполнение этих алгоритмов для шифрования данных должно осуществляться в режиме реального времени. Кроме того, защищенным системам связи часто требуется способность шифровать сообщения несколькими различными алгоритмами с возможностью регулярной смены ключей. В докладе рассматривается модифицированный подход к формированию раундовых ключей, который можно использовать в различных конвейерных алгоритмах шифрования с закрытым ключом [1]. Подход поддерживает использование различных ключей в каждом такте, что повышает общую безопасность, поскольку пользователи не ограничены использованием одного и того же ключа во время любого сеанса передачи данных. Для иллюстрации способа формирования раундовых ключей используется алгоритм шифрования данных стандарта DES, который хорошо пригоден для конвейерной обработки.

В отличии от традиционного способа реализации генератора ключей алгоритма DES, который использует операции логического циклического сдвига на каждой ступени 16-ступенчатого конвейера для формирования раундовых ключей, рассматриваемый в докладе метод использует заранее сформированные для каждого раунда алгоритма DES перестановки входного ключа. Однако в отличии от [1], в модифицированном способе для правильного

формирования раундовых ключей по ступеням конвейера с использованием массива регистров перемещаются входные ключи, а не сами раундовые ключи. Такой подход позволяет получить более экономичную реализацию генератора ключей и конвейера алгоритма шифрования данных в целом.

Характеристики реализации процессора зашифрования с 32 конвейерами алгоритма DES после процесса MAP с использованием пакета ISE 14.7 для кристалла FPGA семейства Virtex7 XC7VX485T-1: 60027 триггеров секций, 48794 просмотровых таблиц (LUT), рабочая тактовая частота – 283 МГц.

Список литературы

1. McLoone M., McCanny J.V. High-performance FPGA implementation of DES using a novel method for implementing the key schedule // IEE Proc.-Circuits Devices Syst. 2003. Vol. 150, No. 5 URL: https://www.researchgate.net/ publication/3349437_High-performance_FPGA_ implementation_of_DES_using_a_novel_method_for_implementing_the_key_schedule (дата обращения: 03.05.2019).

НЕКОТОРЫЕ АСПЕКТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА КАФЕДРЕ ИНЖЕНЕРНОЙ ПСИХОЛОГИИ И ЭРГОНОМИКИ БГУИР

П.И. Кирвель, Д.А. Мельниченко

В соответствии с Концепцией информационной безопасности Республики Беларусь цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений устойчивого развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Для решения этой задачи первостепенное значение имеет подготовка высококвалифицированных информационно- и практико- ориентированных специалистов в области защиты информации.

На кафедре инженерной психологии и эргономики проводится планомерная работа по подготовке специалистов в данной области: начиная с первой ступени высшего образования по специальностям «Инженерно-психологическое обеспечение информационных технологий» и «Информационные системы и технологии (в обеспечении промышленной безопасности)», с последующим углубленным обучением на второй ступени высшего образования по специальности «Управление безопасностью производственных процессов».

На кафедре разработан новый электронный учебно-методический комплекс по дисциплине «Информационные системы обеспечения безопасности» для подготовки магистров. Целью изучения данной дисциплины является формирование у магистрантов системы знаний об особенностях создания, функционирования и управления информационными системами в современных условиях развития общества, а так же освоение практико-ориентированных учебных материалов по применению инновационных стратегий, технологий и методов обеспечения безопасности в условиях производства и эксплуатации современных технических и программных средств, реализующих информационные технологии. После изучения дисциплины мы получим специалиста, обладающего комплексными предметными знаниями в области создания и управления информационными системами, адаптации и использования этих систем и технологий в профессиональной деятельности, а также имеющего навыки инновационной деятельности в области защиты информационных потоков в современных условиях развития общества.

Это, безусловно, будет способствовать формированию в Республике Беларусь прогрессивного информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и передового развития.

Список литературы

1. Концепция информационной безопасности Республики Беларусь: утв. Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1.

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

Р.В. Кислинский

В силу технического прогресса все больше информации на предприятиях и в государственных учреждениях обрабатывается сегодня с использованием средств вычислительной техники. Как следствие, возникает проблема защиты обрабатываемой на средствах вычислительной техники и передаваемой информации.

При построении необходимого уровня защиты информации возникает ряд проблем, которые требуют применения методов анализа и специфических организационных методов и процедур по защите информации.

Основные проблемы защиты информации можно разделить на три группы:

– нарушение конфиденциальности информации;

– нарушение целостности информации;

– нарушение доступности информации.

При построении защиты используются программные решения в области информационной безопасности, но при использовании программных продуктов для построения системы защиты сети возникает ряд проблем:

– расширенная зона контроля;

– неизвестный периметр;

– сложность в управлении и контроле доступа к системе;

– множество точек атаки;

– использование различных программно-аппаратных комплексов защиты информации;

– скрытые каналы утечки информации.

Список литературы

1. Бормотов В.Е. Проблемы защиты информации в компьютерной сети // Молодой ученый. 2016. № 11. С. 148-150. URL https://moluch.ru/archive/115/31145/ (дата обращения: 27.09.2018).

2. Программно-аппаратная защита информации / под ред. С.К. Варлатая, М.В. Шаханова. Владивосток: ДВГТУ,2007. 243 с.

3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М.: ИНФРА-М, 2010. 592 с.

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ПОТОКОВОЕ ВИДЕО

Т.Ю. Кишкурно, М.М. Данильчик

Противодействие незаконному копированию цифровой информации всегда являлось актуальной задачей, а сегодня, в условиях полной информатизации общества, защита становится все более и более важной. Внедрение цифровых водяных знаков (ЦВЗ) в видеоданные применяется для обеспечения защиты цифровых данных и помогает предотвратить копирование, тиражирование и прочие возможные варианты коммерческого использования информации третьими лицами [1].

В работе проанализированы методы внедрения ЦВЗ в потоковое видео такие как: дискретное косинусное преобразование (ДКП, DCT), алгебраическое преобразование, дискретные вейвлет-преобразования (ДВП), алгоритм синхронизации. Разработана шкала для оценки эффективности методов внедрения цифровых водяных знаков. Основными

критериями оценки эффективности являются: вычислительная мощность и сложность алгоритма, зависимость положения ЦВЗ относительно других кадров видеоряда.

Алгоритм ДКП, основанный на дискретно-косинусном преобразовании сигнала использует относительно емкие для процессора формулы нахождения косинусов соответствующих величин. Алгоритм, основанный на вейвлет-преобразовании сигнала (ДВП, преобразование Хаара), возможно реализовать в виде самых быстрых для вычисления математических операций процессором, что значительно экономит время по сравнению с ДКП. С помощью алгоритма синхронизации внедрение и извлечение ЦВЗ проходит с большим коэффициентом корреляции (близким к единице), вследствие чего вычислительная нагрузка становится меньше.

Список литературы

1. Григорьян А.К., Аветисова Н.Г. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор // Информационно-управляющие системы. 2010. № 2. С. 38–45.

ИДЕНТИФИКАЦИЯ СООБЩЕНИЙ ОЦЕНКАМИ ЧИСЛА ВЕКТОРОВ ПЕРЕХОДОВ

И.П. Кобяк

В представляемой работе рассматривается метод синтеза оценок вероятности регистрации двоичных (01)-переходов при решении задач идентификации сообщений [1]. Получено соотношение для вероятности пропуска ошибки, соответствующее указанному алгоритму при наблюдении компьютерами априори неопределенной асимптотической выборки. Определена мода распределения и выполнен сравнительный анализ вероятностей пропуска ошибки, характеризующих предлагаемый метод и известные алгоритмы свертки в точке моды. По результатам работы сделаны следующие выводы: 1) двоичные переходы могут отождествляться с событиями АКФ некоторого заданного вида; 2) графики функций вероятностей пропуска ошибки, соответствующие наблюдению переходов и формированию линейных сигнатур не имеют в асимптотике точек пересечения; 3) из вывода два следует, что метод наблюдения переходов в вероятностных процессах является более точным методом идентификации, чем сигнатурный анализ; 4) аналогичный вывод в пользу АКФ специального вида для двух заданных событий аналитически подтвержден и при сравнении исследуемого метода с алгоритмом наблюдения бернуллиевских 0 или 1 элементарных состояний. Следует ожидать, что улучшение показателей, характеризующих методы идентификации двоичной выборки в системах идентификации сообщений, может быть достигнуто в рамках синтеза других более сложных событий на базе ряда заданных состояний исследуемого процесса. При этом должна учитываться динамика формирования отсчетов для различных сдвигов, а также возможно иные, формально не определенные на сегодняшний день свойства объектов с технической, информационной или другой дискретной природой.

Список литературы

1. Кобяк И.П. Сравнительный анализ вероятностей пропуска ошибки при синтезе сигнатур и оценок числа векторов переходов // АВТ. 2004. № 5. С. 50–57.

ФИЗИКА АТОМА В РАСЧЕТАХ КРИПТОГРАФИЧЕСКИХ КАНАЛОВ СВЯЗИ

И.П. Кобяк

На основе традиционной концепции формирования спектра атома водорода получено уравнение для энергии, излучаемой электроном при переходе с энергоуровня с номером n на энергоуровень боровского радиуса. Получены соотношения, характеризующие параметры центроаффинного пространства ядра [1], а также равенство для эквивалента массы излучаемой энергии. Решение энергетического уравнения позволило рассчитать значения всех радиусов энергоуровней «классического» атома и соответственно скорости электрона на данных

орбитах. Выполненные исследования показали, что достижение физико-математической системности в базовых соотношениях квантовой механики позволяет упростить ряд взглядов на природу явлений в атоме. Так правильное толкование известных теоретических результатов и их связь с практически измеренными величинами приводит к достаточно точному представлению о средних значениях реальных параметров. В частности, анализ классического соотношения для волнового числа показал, что использование понятия «скорость света» не всегда допустимо в вопросах описания физических процессов. Это связано с тем, что подстановка указанного значения в Лоренц-фактор неизбежно ведет к появлению математических неопределенностей в исследуемых системах или критических радиусов в центроаффинных пространствах ядра. Такой контраргумент при анализе физических задач позволил выполнить расчет скорости электрона на боровском радиусе в соответствии с несложным соотношением и, как следствие, ряд параметров данной частицы. Спин электрона в представляемой работе рассматривается как форма существования частицы в некотором собственном ПВК, слабо взаимодействующим с окружающей средой.

Список литературы

1. Соколов А.А., Тернов И.М. Квантовая механика и атомная физика. М.: Просвещение, 1970. 423 с.

ЕДИНЫЙ КОМПЛЕКС БЕЗОПАСНОСТИ ВОЕННОГО ГОРОДКА НА ОСНОВЕ ПРИМЕНЕНИЯ PSIM-СИСТЕМЫ

А.Н. Коваленко

Для противодействия угрозам безопасности, современные комплексы технических средств охраны военных городков требуют технологического развития в соответствии с современным состоянием науки и техники. В настоящее время, отсутствует интеграция существующих систем комплекса технических средств охраны. Выполнение служебно-боевых задач военнослужащими осуществляется либо непосредственно с аппаратурой, либо на базе отдельных программных продуктов для каждой из систем. Взаимосвязь между ними отсутствует, как на программном, так и на аппаратном уровне. Есть только частичная организация взаимодействия между компонентами системы охранной сигнализации.

Отсутствие единого интегрированного комплекса систем безопасности, приводит к снижению удобства эксплуатации систем, а также ведет к созданию благоприятных условий для совершения диверсий или возникновению нештатных ситуаций вследствие нарушения технологических процессов.

Для объединения всех элементов комплекса необходима единая платформа. Все системы объединяются с помощью PSIM (Physical Security Information Management) – это англоязычное название комплексной системы безопасности, которая является отдельной системой и выступает надстройкой над системами безопасности. PSIM – это программная платформа, которая собирает и обрабатывает информацию из разрозненных устройств обеспечения безопасности и информационных систем, после чего складывает ее в одну общую картинку.

Список литературы

1. Возможности современных систем управления информацией о физической безопасности (PSIM) [Электронный ресурс]. URL: https://www.aktivsb.ru/statii/sovremennye_sistem_psim.html (дата обращения: 18.04.2019).

2. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. М.: Горячая линия–Телеком, 2004. 367 с.

ПРОБЛЕМЫ КИБЕРЗАЩИТЫ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

В.Н. Корделюк

Тенденции цифровой трансформации общества (в том числе в Республике Беларусь) показывают все большее внедрение автоматизированных, автоматических систем, реализующих сетевые информационные технологии по управлению технологическими процессами. Интернет был и остается основным каналом возможного воздействия на указанные системы в связи с все большим сопряжением технологических сетей и корпоративных информационных сетей.

Повсеместное функционирование объектов вооруженных сил, промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость национальную безопасность в различных сферах жизнедеятельности от их надежности и защищенности. При этом вскрывается пропорциональная зависимость – чем глубже интеграция автоматизированных систем управления в киберпространство, тем критичнее для данных объектов результаты активного воздействия извне на их информационные ресурсы [1].

В отличие от информационных сетей, где последствия реализации угроз (утечка информации, блокирование информации, ее несанкционированное уничтожение) имеют больше нематериальный характер, ущерб в сфере управления технологическими процессами в большинстве своем имеет непосредственную физическую форму (отключение электроэнергии, прекращение подачи воды, срыв работы телекоммуникационных сетей, аварии на железнодорожном, авиационном транспорте и т.д.).

Действия в киберпространстве позволяют наносить ущерб дистанционно (анонимно), не нарушая физических границ его государства. Возрастает важность кибербезопасности критически важных объектов инфраструктуры государства.

Список литературы

1. Концепция информационной безопасности Республики Беларусь: утв. Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1.

ЗАЩИТА УДАЛЕННОЙ ПОЛЬЗОВАТЕЛЬСКОЙ СТАТИСТИКИ С ПОМОЩЬЮ МЕХАНИЗМОВ ДИФФЕРЕНЦИАЛЬНОЙ ПРИВАТНОСТИ

Е.А. Криштопова

Автоматический сбор данных с пользовательских устройств (персональных компьютеров, смартфонов, фитнес-браслетов и т.п.) дает возможность сборщикам собрать информацию о конкретном пользователе – его предпочтениях, привычках, состоянии здоровья, режиме дня и т.д.

Например, для «анонимизированного» статистики просмотров пользователями фильмов компании Netflix, исследователи показали, что информацию о конкретных пользователях можно восстановить и предсказать их политические взгляды [1].

Вышесказанное делает важным задачу анонимизации пользовательской статистики. Технически это решается использованием механизмов дифференциальной приватности.

Дифференциальная приватность (Differential privacy - DP) – это совокупность методов, которые обеспечивают максимально точные запросы в статистическую базу данных при одновременной минимизации возможности идентификации отдельных записей в ней. Дифференциальная приватность дает математическое определение потери конфиденциальных данных отдельных лиц, путем внесения случайности, описываемой переменной ε, когда их личная информация используется для создания продукта.

Наиболее известны практические реализации локальных дифференциально-приватных алгоритмов: RAPPOR от Google, решения Apple для iOS 10, Microsoft’s PINQ, Uber’s FLEX.

Что касается белорусских производителей, то, так как деанонимизация пользовательской статистики не является требованием белорусского законодательства, то и алгоритмы дифференциальной приватности и аналогичные средства ими не применяются.

Список литературы

1. Narayanan, A., Shmatikov V. Robust De-anonymization of Large Sparse Datasets // 2008 IEEE Symposium on Security and Privacy (sp 2008). URL: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (дата обращения: 03.05.2019).

ПРЕПОДАВАНИЕ ДИСЦИПЛИН В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СПЕЦИАЛЬНОСТЕЙ ПЕРВОЙ И ВТОРОЙ СТУПЕНЕЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Е.А. Криштопова, В.С. Осипович, А.М. Прудник

В настоящее время, вопросам информационной безопасности в Республике Беларусь придается очень большое значение [1, 2], кроме того, одним из государственных приоритетов нашей страны провозглашена ориентация на информационное общество и развитие рынка инфокоммуникационных технологий [3, 4].

Исходя из этого, для высших учебных заведений одной из актуальных проблем является подготовка специалистов как в области безопасности информационных технологий, так и в смежных областях с соответствующими компетенциями.

В свете стоящих задач, на кафедре инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» начато преподавание ряда дисциплин в области безопасности информационных технологий.

На 1-й ступени высшего образования по специальности 1-58 01 01 «Инженерно-психологическое обеспечение информационных технологий» преподается дисциплина «Криптографические технологии», в рамках которой изучаются базовые принципы криптографии, современные криптографические протоколы, студенты овладевают навыками применения криптографических технологий для защиты информации. На данную дисциплину для студентов дневной формы обучения отводится 32 академических часа лекций и 32 академических часа практических занятий.

Для студентов 2-й ступени высшего образования по специальности 1-59 81 01 «Управление безопасностью производственных процессов» преподается дисциплина «Безопасность информационных систем». Целью изучения дисциплины является получение знаний по вопросам обеспечения безопасности информационных систем в условиях различных по виду, происхождению и характеру возникновения угроз. На данную дисциплину для студентов дневной формы обучения отводится 10 академических часов лекций и 20 академических часов практических занятий.

Таким образом, внедрение кафедрой инженерной психологии и эргономики актуальных учебных дисциплин в области безопасности информационных технологий способствует решению задач качественной подготовки инженерных кадров в соответствии с вызовами времени.

Список литературы

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». URL:http://etalonline.by/document/?regnum=h10800455&q_id=754382 (дата обращения 02. 05.2019).

2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». URL:http://etalonline.by/document/?regnum=p219s0001&q_id=754197 (дата обращения 02. 05.2019).

3. Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы / Постановление коллегии Министерства связи и информатизации Республики Беларусь от 30.09.2015 г. № 35. URL: http://etalonline.by/document/?regnum=u215e2913&q_id=754159 (дата обращения 02. 05.2019).

4. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы / Постановление Совета Министров Республики Беларусь от 23 марта 2016 г. № 235. URL: http://etalonline.by/document/?regnum=c21600235&q_id=754193 (дата обращения 02. 05.2019).

МЕХАТРОННАЯ СИСТЕМА ПАРАЛЛЕЛЬНОЙ КИНЕМАТИКИ

В.В. Кузнецов

Для технических средств защиты информации основанных на мехатронных системах остро ставится задача повышения точности и быстродействия исполнительных механизмов и используемых мехатронных систем перемещений. Эффективным средством решения этой задачи является широкое использование мехатронных систем параллельной кинематики с многокоординатным приводом прямого действия. Для таких систем нами была предложена концепция управляемого движения в трехмерном пространстве на базе многокоординатного привода и реконфигурируемых механизмов параллельной кинематики [1].

В настоящей работе в развитие этой концепции представлены новые результаты по разработке систем многокоординатных перемещений, математических моделей и алгоритмов для их компьютерного имитационного моделирования. Предложена новая мехатронная система перемещений с шестью степенями свободы, построенная на гибридном приводе прямого действия, компонуемого из трех линейных и трех поворотных программно-управляемых координатных позиционеров кинематически связанных с исполнительным механизмом параллельной кинематики в виде раскрывающегося тетраэдра.

Такая компоновка мехатронной системы позволяется реализовывать прецизионные движения с шестью степенями свободы по шести независимым координатам в трехмерном пространстве, включая три линейных и три угловых, обеспечивая повышенные кинематические и динамические характеристики перемещений при высокой точности их реализации.

Список литературы

1. Системы многокоординатных перемещений на механизмах параллельной кинематики / С.Е. Карпович [и др.]. Минск : Бестпринт, 2017. 254 с.

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ НОСИМОЙ ЭЛЕКТРОНИКИ

В.Ф. Кулиш

Согласно прогнозам компании Gartner в 2022 г. будет продано 453,19 миллион единиц устройств носимой электроники. Наиболее распространенными устройствами такого типа являются фитнес-браслеты. Они позволяют собирать данные о физической активности пользователей (количество пройденных шагов, пройденная дистанция, сожженные калории, данные о занятиях спортом и сне, данные о пульсе). Собранная информация отправляется на удаленный сервер для дальнейшей обработки. Браслет представляет собой, как правило, следующий набор датчиков (акселерометр, оптический датчик измерения пульса), а также микропроцессоры, необходимые для обработки информации от датчиков и передачи этих данных на смартфон с помощью технологии Bluetooth. Архитектура для обработки данных состоит из следующих компонентов: браслет для сбора информации, смартфон для получения информации с браслета, отправки данных на сервер и получение обработанных результатов, сервер для обработки полученных данных. Основными рисками информационной безопасности такой системы является утечка данных о пользователе, а также подмена отправляемой информации. Риск утечки информации может быть реализован с помощью следующих атак:

– перехват коммуникаций между браслетом и смартофоном;

– обход механизма аутентификации в браслете;

– создание фантомного устройства для получения статистических данных с удаленного сервера.

Риск отправки поддельных данных может быть реализован с помощью атак на сетевой приложение на сервере, а также с помощью манипуляции данных передаваемых мобильному приложению для последующей отправки.

АУДИТ БЕЗОПАСНОСТИ ТРАФИКА В СИСТЕМЕ IP-ТЕЛЕФОНИИ

Д.В. Куприянова, Д.Н. Одинец

Протоколы SIP и RTP, используемы для передачи медиа данных, были разработаны без учета необходимости защищать передаваемую информацию, в следствии чего возможны следующие виды атак и уязвимостей: фрод звонков, вирус, попавший в сеть IP-телефонии может начать рассылать спам ее абонентам, нарушение звонков – атакующий рассылает пакеты клиентам звонка, DoS – за счет отправки большого количества сообщений «Invite» и «Registrer» нарушается работу компонентов SIP, атакующий прослушивает весь трафик в IP-телефонии, подбор паролей, Man-In-The-Middle – атакующий проникает в звонок между пользователями, и может не только прослушивать, но и изменять сообщения между клиентами.

Для защиты передаваемы данных, предлагается использовать протокол TLS – протокол защиты транспортного уровня. Данный протокол использует асимметричное шифрования для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Также для защиты данных может быть использован IPsec – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, обеспечивающих аутентификацию, проверку целостности и/или шифрование IP-пакетов. В отличие от IPSec, TLS протокол реализуется на транспортном уровне и не требует поддержки на промежуточных устройствах.

Для улучшения защиты может быть использован VPN. В случае невозможности использования VPN, необходимо использовать VLAN. Данные решения создают виртуальную сеть, что позволяет передавать данные в надежных сетях.

В данном случае лучшим выбором будет использование VPN который позволяет шифровать данные, так как в этом случае нет необходимости реализации шифрования на клиентах, отсутствует риск ошибок в реализации шифрования, VPN может быть обновлен для использования более современных методов шифрования без необходимости обновления кода клиента [1–3].

Список литературы

1. Security in a SIP network: Identifying network attacks [Электронный ресурс]. URL: https://searchunifiedcommunications.techtarget.com/feature/Security-in-a-SIP-network-Identifying-network-attacks (дата обращения: 05.04.2019).

2. How to Address WoIP Security Challenges [Электронный ресурс]. URL: http://www.centurylinkbrightideas.com/how-to-address-voip-security-challenges/ (дата обращения: 05.04.2019).

3. SIP Server Security with TLS: RPE [Электронный ресурс]. URL: https://www.researchgate.net/publication/235601569_SIP_Server_Security_with_TLS_Relative_Performance_Evaluation (дата обращения: 05.04.2019).

СПОСОБЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.В. Куприянова, Д.Ю. Перцев

Анализ ситуации, проведенный BSA Global Software Survey [1], показывает, что рынок нелицензионного ПО уменьшается, однако по состоянию на 2018 г. составляет 37 % и оценивается более чем в 46 млрд. долларов. С учетом этого проблема защиты авторских прав по-прежнему является актуальной. К основным способам защиты ПО относится: лицензионный ключ, жесткая привязка к носителю информации, USB-ключ. Лицензионный ключ является самым простым способом защиты и предполагает генерацию ключа по некоторому шаблону с привязкой к имени пользователя или аппаратной конфигурации системы. Основным

недостатком подхода является относительная простота взлома, осуществляемая путем анализа дизассемблированного кода. Развитием указанного подхода является проверка ключа через Интернет. При этом, как правило, существует сервер, через который проверяется лицензия. Данный подход более сложен для взлома и, как правило, предполагает подмену сервера на собственный. Жесткая привязка к носителю информации и USB-ключ являются схожими по принципу действия. Данные подходы предполагают постоянный опрос устройства (флеш-устройство, компакт-диск и другие), при его обнаружении считывается ключ в программе и сравнивается с ключом, записанным на устройстве. После чего принимается решение, является ли копия программы лицензионной. Современные версии USB-ключей развивают концепцию [2] и позволяют разработчику выполнить произвольный алгоритм внутри электронного ключа. В дополнение к рассмотренным методам защиты применяются запутывание кода (англ. obfuscation) и комбинирование упакованного кода с кодом, который его восстановит. На основе проведенного анализа, подтверждаемого в том числе сторонними исследованиями [3], оптимальным является комбинация из нескольких способов защиты. Например, применение USB-ключа в связке с запутыванием кода.

Список литературы

1. Software Management: Security Imperative, Business Opportunity [Электронный ресурс] URL: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (дата обращения: 05.04.2019).

2. Senselock [Электронный ресурс]. URL: http://senselock.ru/index.php (дата обращения: 05.04.2019).

3. Liutkevicius A. Assessment of Dongle-based Software Copy Protection Combined with Additional Protection Methods // Electronics and Electrical Engineering. 2011. № 6 (112). P. 111–116.

ЗАЩИТА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ РАСПРЕДЕЛЕННЫМ АКУСТИЧЕСКИМ ДАТЧИКОМ НА ОСНОВЕ КОГЕРЕНТНОГО РЕФЛЕКТОМЕТРА

Д.Н. Курбыко, В.Н. Урядов

Надежность работы системы связи, т. е. ее способность в течение длительного времени выполнять заданные функции по передаче информации с установленной нормами достоверностью – то, к чему стремится и потребитель, и поставщик услуг, и оператор сети связи. Всем известно, что аварию легче предотвратить, чем устранить. Для этого надо своевременно обнаружить признаки ее наступления. Чтобы ВОЛС функционировала без прерывания связи, службы эксплуатации должны проводить комплекс мероприятий для сведения к минимуму вероятности повреждения кабельной инфраструктуры. Помочь им в этом вопросе может распределенный акустический датчик «Дунай» на основе когерентного рефлектометра. Принцип действия распределенного акустического датчика «Дунай» схож с тем, как функционирует радар или обычный оптический рефлектометр: в тестируемую линию вводится мощный зондирующий световой импульс, и анализируются характеристики отраженного и рассеянного назад излучения. В отличие от других приборов распределенный акустический датчик на основе когерентного рефлектометра благодаря чувствительности к фазовой модуляции в волокне [2] позволяет измерять распределение акустических воздействий по всей длине волокна. Датчик акустических воздействий на основе когерентного рефлектометра (COTDR) позволяет обнаружить проведение практически любых работ вблизи ВОЛС, а тем более манипуляции с оптическим кабелем. Кабельная инфраструктура волоконно-оптических сетей связи должна быть рассчитана на многолетнюю эксплуатацию и неоднократные модернизации систем связи в течение всего срока ее эксплуатации, обычно составляющего 25 лет. При отсутствии ошибок проектирования правильная организация эксплуатации – залог успешной работы ВОЛС. Чтобы предотвратить возможные обрывы кабеля на наиболее ответственных (с точки зрения объемов трафика) и проблемных (с точки зрения случайных обрывов при строительных работах) участках ВОЛС, целесообразно использовать распределенный датчик акустических воздействий на основе когерентного рефлектометра

Список литературы

1. Компания «Т8». DWDM-системы – DWDM-оборудование Волга: разработка, проектирование, инсталляция. [Электронный ресурс]. URL: http://t8.ru/wp-content/uploads/2012/01/1.pdf (дата обращения: 07.05.2019).
2. Shatalin S., Treschikov V., Rogers A. Interferometric optical time-domain reflectometry for distributed opticalfiber sensing //Appl. Opt. 1998. № 37.

ФУНКЦИИ СОВРЕМЕННОЙ ВИДЕОАНАЛИТИКИ

В.И. Лабкович, С.Н. Петров

В настоящее время, функциональные возможности систем видеонаблюдения получают все больше средств для автоматического анализа видеоинформации. Качественная современная система видеонаблюдения должна не только производить запись и выводить изображение на экран, но и осуществлять ряд аналитических функций. Одним из главных направлений цифрового видеонаблюдения является видеоаналитика.

Видеоаналитика – это интеллектуальный анализ потока видеоданных от камеры (последовательно поступающих видеоизображений) и автоматическое выявление различного рода данных и детектирование заранее запрограммированных ситуаций. Аналитика ведется как в режиме реального времени, так и при работе с архивом. Результатами работы видеоаналитики являются события, которые могут быть переданы оператору системы видеонаблюдения в виде сообщения или записаны в архив для последующего поиска по ним и составления отчетов.

Существует перечень классических задач, с которыми видеоаналитика успешно справляется.

Наиболее распространенные задачи следующие:

– распознавание номеров (автомобильных, на денежных купюрах, документах);

– обнаружение опасных ситуаций (скопления людей, оставленные предметы, возгорания и задымления и т. п.);

– распознавание человеческих лиц и поиск их в базах данных;

– распознавание с целью подсчета людей и транспорта.

Использование видеоаналитики дает возможность в автоматическом режиме, без участия человека, в процессе видеонаблюдения решать задачи, которые обычно под силу только человеческому зрению.

У видеоаналитики пока остается немало ограничений, но появляется все больше мощных и гибких систем, позволяющих решать различные задачи. Они ориентированы на разные сегменты рынка и могут не только обеспечивать безопасность, но и быстро извлекать необходимую информацию из видеоархивов, способствуя повышению эффективности работы организаций. С совершенствованием аналитических алгоритмов и увеличением вычислительных мощностей процессоров, применяемых в серверах и камерах видеонаблюдения, возможности таких инструментов значительно расширятся, а видеоаналитика станет более доступной и удобной в применении [1, 2].

Список литературы

1. Возможности современной видеоаналитики. [Электронный ресурс]. URL: https://www.videomax-server.ru/support/articles/vozmozhnosti-sovremennoy-videoanalitiki/ (дата обращения: 02.05.2019).
2. Видеоаналитика на практике. [Электронный ресурс]. URL: https://www.osp.ru/lan/2015/03/13045265 (дата обращения: 02.05.2019).

ЛАВИННЫЕ СВЕТОДИОДЫ НА ОСНОВЕ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ ДЛЯ ОПТОЭЛЕКТРОННОЙ ОБРАБОТКИ ИНФОРМАЦИИ

С.К. Лазарук, А.А. Лешок, Ле Динь Ви, А.И. Мацкевич,
Н.А. Григорук, С.Л. Перко, А.Ю. Клюцкий

Оптоэлектронная обработка информации по сравнению с традиционной электронной позволяет значительно повысить быстродействие всей системы. Помимо высокой производительности важным моментом является высокая степень защиты передаваемой информации за счет локализации информационного потока внутри микросистемы источник света – волновод – фотоприемник. Для кремниевой оптоэлектроники главные сложности связаны с преобразованием электрического сигнала в оптический. Лавинные светодиоды на основе наноструктурированного кремния позволяют решить данную проблему. Авторами разработаны конструкция и технология изготовления лавинных светодиодов, использующих наноструктурированный кремний в качестве активного материала, преобразующего электрический сигнал в оптический на длинах волн видимого диапазона с эффективностью 0,1-1 %. Оптимизация геометрии формируемых структур обеспечила их быстродействие, позволяющее работать в гигагерцовом диапазоне частот. Высокая надежность светоизлучения (более 1000 ч непрерывного функционирования) достигается за счет эффективной защиты наноструктурированного кремния от контакта с атмосферой. Разработанная технология совместима с технологией КМОП ИС, что позволило интегрировать лавинные светодиоды площадью 100 мкм^2 на одном кристалле с КМОП транзисторами. Данная разработка открывает новые возможности для развития кремниевой оптоэлектроники, способной работать на частотах гигагерцового диапазона.

ЗАРЯДОВЫЕ СВОЙСТВА ПЛЕНОК АНОДНЫХ ОКСИДОВ ВЕНТИЛЬНЫХ МЕТАЛЛОВ, ИСПОЛЬЗУЕМЫХ В МЕМРИСТОРНЫХ УСТРОЙСТВАХ

Ле Динь Ви, В.В. Дудич, Г.Г. Рабатуев, А.С. Хиневич, С.Л. Перко, В.В. Фиалковский,
Н.А. Григорук, Н.А. Казимиров, Л.П. Томашевич, Р.С. Макаров, С.К. Лазарук

Для развития современной электроники необходима разработка новых технологий и принципов формирования устройств обработки, хранения и защиты информации. В связи с этим последние десять лет особое внимание уделяется использованию мемристорных устройств (энергонезависимых ячеек памяти) для хранения информации. Мемристоры демонстрируют эффект переключения сопротивления между высокоомным и низкоомным состояниями под действием внешнего электрического поля. На эффект переключения влияют зарядовые свойства используемых пленок.

В работе проведено исследование влияния режимов анодирования на зарядовые свойства анодных пленок вентильных металлов ряда Al, Ti, Ta. Показано, это за счет выбора электролита и электрических режимов формовки можно формировать анодные оксиды как с положительным, так и с отрицательным электрическим зарядом. При этом плотность электрического заряда может достигать от 10^{-7} до $2\cdot10^{-6}$ (Кл/см^2).

Увеличение плотности электрического заряда позволило увеличить коэффициент переключения в мемристорных устройствах более чем на порядок, это открывает новые возможности для их практического применения при хранении и защите информации.

ВРЕМЕННЫЕ ОТКАЗЫ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ СИСТЕМ БЕЗОПАСНОСТИ И ОЦЕНКА ВЕРОЯТНОСТИ ИХ ВОЗНИКНОВЕНИЯ

Л.В. Майоров, С.М. Боровиков

К временным отказам (сбоям) устройств систем безопасности на основе микропроцессоров чаще всего приводят электромагнитные воздействия внешней среды, остальные виды воздействий обычно приводят к необратимым повреждениям в структуре электронных компонентов, в связи с чем устройство полностью теряет свои функции, частично

или полностью. Временные отказы микропроцессорных устройств являются следствием проблем электромагнитной помехозащищенности как по линиям питания, так и по средам распространения полезных сигналов (провода, радиоэфир).

Источники электромагнитных помех могут быть как внешними, так и внутренними. Внутренними источниками помех являются влияющие друг на друга электронные компоненты и элементы конструкции электронного устройства. Внешние источники электромагнитных помех являются одним из видов воздействия окружающей среды и могут быть естественными (атмосферный разряды, разряды статического электричества) или искусственными (электромагнитные процессы в технических системах, работа промышленных установок) [1]. Электромагнитные помехи от внешних источников в микропроцессорное устройство могут поступать в виде наводок на линии связи и дорожки печатной платы, выступающие в роли паразитных антенн. Влияние внутренних источников учитывается производителем и считается приемлемым для устройств, прошедших соответствующую сертификацию и технический контроль в условиях производства.

Основное влияние на вероятность временного отказа микропроцессорного устройства оказывает среда. Актуальным является вопрос об оценке возможности возникновения временного отказа микропроцессорного устройства в реальной ситуации. Для оценки вероятности временного отказа предлагается вначале выполнить анализ среды и оценить вероятность появления источника воздействия, а интересующую вероятность временного отказа далее получать, используя статистические данные о влиянии источников воздействий на возникновение временных отказов микропроцессорных устройств.

Список литературы

1. Хабигер Э. Электромагнитная совместимость. Основы ее обеспечения в технике. М.: Энергоатомиздат, 1995. 304 с.

ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СПЕКТРОВ СЛОЖНЫХ СИГНАЛОВ В БАЗИСЕ ПРЕОБРАЗОВАНИЯ МЕЛЛИНА

А.М. Макаров, Е.А. Писаренко

Классическая теория обнаружения сигналов на фоне шумов хорошо разработана целым рядом российских и зарубежных ученых [1–10]. В их работах, в основном, рассматриваются сигналы, имеющие базу порядка единиц. Для сигналов с большой базой разработаны теоретические основы обнаружителей сигналов, носящих название сложных. Теория обнаружения сложных сигналов на фоне помех развита в работах В. Б. Пестрякова, Я. Д. Ширмана, Ю. С. Лезина, Д. Б. Вакмана, Г. Ван-Триса.

Все методы обнаружения сигналов на фоне шумов объединяет единая методология обнаружения – нахождение путем синтеза и анализа информативных признаков контраста, отличающих сигналы от шума. В качестве контраста может служить максимум отношения сигнал/шум или различия в автокорреляционных функциях сигналов [2, 4, 5, 6].

Наиболее широкое применение на практике нашли спектральные методы основанные на интегральном преобразовании Фурье (ПФ) анализируемых сигналов. Если структура сложного сигнала неизвестна, то ПФ малоэффективно для измерения таких излучений, но можно использовать другие базисы, например, базис интегрального преобразования Меллина (ПМ) [11, 12].

Целью работы явилось исследование свойств амплитудных спектров широкополосных сигналов (фазоманипулированных) в базисе ПМ для нахождения информативных признаков, позволяющих обнаружить фазоманипулированный сигнала на фоне шума. Доказана теорема об узкополосности амплитудного спектра фазоманипулированных сигналов в базисе ПМ. Предложена структурная схема двухбазисного обнаружения фазоманипулированных сигналов.

Список литературы

1. Обнаружение радиосигналов / П.С. Акимов [и др.]. М.: Радио и связь, 1989. 288 с.

2. Левин Б.Р. Теоретические основы статистической радиотехники. М.: Советское радио, 1974. 752 с.

3. Ван Трис Г. Теория обнаружения, оценок и модуляции. Т. 1. М.: Советское радио, 1972. 744 с.

4. Котельников В.А. Теория потенциальной помехоустойчивости. М.: Советское радио, 1956. 152 с.

5. Макаров А.М., Ермаков А.С. Оптимальный согласованный фильтр для обнаружения сигнала на фоне шума с неизвестной корреляционной функцией // Известия ЮФУ. Технические науки. 2015. № 11 (172). С. 42–54.

6. Мидлтон В. Введение в статистическую теорию связи. Т. 2. М.: Советское радио, 1962. 832 с.

7. Репин В.Г., Тартаковский Г.П. Статистический синтез при априорной неопределенности и адаптации информационных систем. М.: Советское радио, 1977. 432 с.

8. Сосулин Ю.Г. Теория обнаружения и оценивание статистических сигналов. М.: Советское радио, 1978. 447 с.

9. Френкс Л. Теория сигналов. М.: Советское радио, 1974. 344 с.

10. Bertrand J., Bertrand P., Ovarlez J. The Mellin Transform. The Transformsand Applications Handbook. Boca Raton: CRCPress LLC, 2000.

11. Ovarlez J., Bertrand P., Bertrand P. Computation of offine time – frequency distributions using the Fast Mellin transform // Proc IEEE – ICASSP. 1992.

12. Philippe Flajolet, Xavier Gourdon, Philippe Dullas. Mellin transforms and asymtotics: Harmonic sums // Theoretical Computer Science 1995. Vol. 144. P. 3–38.

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.В. Макатерчик

В настоящее время общественные и бизнес-процессы в той или иной мере осуществляются с использованием различных объектов специального назначения, выполняющих функции, характерные для какой-то одной или нескольких конкретных задач. Широкое применение в современном оборудовании различных компьютеризированных систем формирует новый, динамически изменяющийся перечень угроз. Так, в телекоммуникационном оборудовании, распространенном на рынке страны 60 % используют в качестве серверной ОС Windows, у 75 % – управляющее и клиентское ПО разработано под Windows, web-интерфейс у 65% оборудования разработан на Java.

Исследования показывают, что в отличии от объектов критически важной инфраструктуры, защита объектов специального назначения находится на значительно более низком уровне:

– на 74 % объектов не применяют эффективных мер для контроля доступа;

– 67 % респондентов не осуществляют должным образом мониторинг информационной безопасности;

– исполнительное руководство 65 % объектов не осознает важности угроз информационной безопасности в полной мере;

– 55 % объектов не проводят на достаточном уровне аудит безопасности;

– 61% объектов применяют недостаточные меры по защите конечных точек.

Анализ состояния указанной проблемы в мире показывает, что уровень ее научно-теоретической, практической реализации не соответствует современному уровню угроз [1, 2].

Список литературы

1. Макаренко Д.И., Хрусталев Е.Ю. Концептуальное моделирование военной безопасности государства. М.: Наука, 2008. 303 с.

2. Kim D., Solomon M.G. Fundamentals of information systems security. Jones & Bartlett Publishers, 2013. 258 p.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЗДАНИЯ, УПРАВЛЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, А.Н. Бойко, Д.В. Калинин

Согласно отчетным данным по работе защитного алгоритма Google Play Protect, встроенного в приложение Google Play Store на всех авторизованных устройствах на Android и проверяющего устройство при установке/обновлении приложений из каталога Google Play или стороннего источника на признаки потенциально вредоносного приложения (Potentially Harmful Applications, PHA), выявляется значительное количество таких вредоносных приложений.

Для оценки технологического уровня и степени безопасности 3 специализированных приложений КФО для Android проведено их исследование на предмет возможности реверсного инжиниринга программного обеспечения (software reverse engineering, SRE) с изучением структуры построения, алгоритмов функционирования, технологий защиты информации и др.

Для сохранения конфиденциальности: названия КФО заменены порядковыми номерами, идентификаторы приложений изменены, листинг (дизассемблер/декомпилятор) исполняемого кода (classes.dex) и алгоритмы функционирования не приводятся, согласисие владельцев получено.

По результатам исследования можно сделать следующий вывод: APK-сборки (.apk) 3 типовых КФО могут быть подвергнуты реверсному инжинирингу с получением информации по общей структуре, общему алгоритму функционирования (файл AndroidManifest.xml), листингу (дизассемблер/декомпилятор) исполняемого кода (файл classes.dex), построению функциональных графов (декомпилятор) базовых функций (файл classes.dex).

В качестве защиты APK-сборок (.apk) 2 типовых КФО использовался базовой алгоритм (включая обфускацию кода от ProGuard из комплекта Android Studio), в APK-сборке (.apk) 1 типовой КФО были обнаружены признаки дополнительной защиты (усиленная обфускация кода) инструментом, отличным от ProGuard.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЗДАНИЯ И УПРАВЛЕНИЯ СЕТЕВЫМИ РЕСУРСАМИ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, В.А. Гайшун, В.Н. Ярошевич

Исследованы технологии создания и управления сетевыми ресурсами (сайтами) на примере 24 кредитно-финансовых организаций (КФО) Республики Беларусь. Проведено тестирование уровня информационной безопасности (ИБ) библиотек «JavaScript», а также алгоритмов реализации шифрования на основе SSL-сертификатов для сайтов КФО.

Проведенное углубленное тестирование библиотек «JavaScript» сайтов основного домена КФО, позволило выявить детальный перечень уязвимостей ИБ, которые уже были внесены и описаны в базах экспертных знаний (тип потенциальных атак: Regular Expression Denial of Service, Cross-site Scripting, Cross-site Scripting in dialog close Text). Следует отметить, что только 4 сайта основного домена КФО (17 %) не имеют уязвимостей библиотек «JavaScript». Для исследования уровня ИБ сайтов основного домена КФО дополнительно были выполнены оценка наличия и типа используемого SSL-сертификата и оценка качества реализации алгоритма защищенного соединения на основе SSL-сертификата (уровни оценки безопасности: A/A+, B, C, F; где A/A+ - высший уровень, F – низший уровень).

Результаты исследования показали:

– на 2 сайтах КФО (8 %) – нет SSL-сертификата (не реализуется защищенное соединение);

– на 7 сайтах КФО (29 %) – имеются уязвимости при реализации защищенного соединения на основе SSL-сертификата (тип потенциальных атак: Forward Secrecy, Diffie-Hellman key exchange parameters).

ЗАЩИТА ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПОЛЬЗОВАТЕЛЯ ОТ АТАК ПОДМЕНЫ ИНФОРМАЦИИ

В.Ю. Мандрик

Пользователи персональных компьютеров часто эксплуатируют сервисы, обеспечивающие их упрощенную аутентификацию при доступе к электронной почте и другим аккаунтам. Такая тенденция усложняет проблему информационной безопасности. Ее решение лежит в плоскости разработки организационно-технических мероприятий, направленных на противодействие атакам подмены и снижению риска несанкционированного доступа к персональным данным.

В результате исследования была смоделирована атака ARP-spoofing. В случае данной атаки компьютер начинает считать шлюзом не маршрутизатор, а компьютер атакующего. Атакующий получает запросы от «жертвы» и передает их в пункт назначения (например, запрашивает содержимое веб-сайта в Интернете), получив ответ от сервера, он направляет его «жертве». В этой ситуации атакующий становится посредником – отсюда другое название атаки человек-посередине – «атака посредника».

Атака ARP-spoofing используется в локальной сети, построенной на коммутаторах. С ее помощью можно перенаправить поток ethernet-фреймов на другие порты, в соответствии с MAC-адресом. После чего злоумышленник может перехватывать все пакеты на своем порту. Таким образом, атака ARP-spoofing позволяет перехватывать трафик машин, расположенных на разных портах коммутатора. В ходе исследования выполнена оценка эффективности различных средств защиты информации от указанного типа атаки.

КОНЦЕПЦИЯ ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Ф. Марко

Рассматривается предложенная концепция тестирования разрабатываемого программного обеспечения для технических средств защиты информации, которая реализуется с помощью комплексной системы Team Foundation Server [1]. В качестве инструмента для осуществления процесса тестирования используется тест-трекинговая система Microsoft Test Manager, которая предназначена для организации планов тестирования, создания и управления тестовыми случаями. В этом случае также присутствует возможность связать ручные тестовые случаи с автоматическими.

Нами предлагается следующая концепция тестирования. В системе MTM создается базовый план тестирования. Тестовые случаи в базовом плане сортируются по модулям в зависимости от тестируемой функциональности ПО и виду тестирования. Сортировка тестовых случаев осуществляется с помощью таких объектов системы MTM, как статические наборы тестов, наборы тестов на основе запросов и теги. Каждой версии тестируемого ПО соответствует итерация, в которой хранится два плана тестирования: базовый и текущий. Базовый план клонируется из предыдущей итерации, а также расширяется новыми тестовыми случаями, текущий план формируется из базового путем клонирования определенных тестовых наборов с учетом поставленных задач тестирования.

Таким образом разработана гибкая концепция тестирования разрабатываемого ПО, которая позволяет эффективно выполнять тестирование и автоматизировано предоставлять результаты его выполнения.

Список литературы

1. Командная разработка с использованием Visual Studio Team Foundation Server / Д. Мейер [и др.]. Microsoft Visual Studio Team System, 2008. 564 с.

ПОЛУЧЕНИЕ И ОБРАБОТКА ДИНАМИЧЕСКИХ ПРИЗНАКОВ ОНЛАЙН-ПОДПИСИ

А.И. Митюхин

Одним из биометрических поведенческих признаков, используемых в аутентификационных системах является собственноручная подпись человеческой личности. Подписи можно считать уникальными изображениями со стабильными динамическими характеристиками. В отличие от статического (офлайнового) [1] метода получения сигнатурного эталона и образа подписи, когда верификация основывается на геометрических свойствах 2D-изображения $g(x,y), \{x,y\} \in \mathrm{Z}^+$, таких как плотности линий, скрещивания, ответвления линий и др., динамический (онлайновый) [1] способ формирования эталона и образа подписи использует значения 2D-пространственных координат $\{x,y\}$ и значения реального временного интервала написания подписи. Увеличение числа признаков распознавания усложняет фальсификацию, имитацию и подделку подписи. В работе рассматривается спектральный подход получения и обработки динамических признаков. Зная частоту дискретизации и спектральные характеристики изображения подписи, фиксируя координаты определенных критических и экстремальных точек, можно получить такие характеристики, как составляющие скорости (ускорения) электронного пера во время его движения на сенсорном экране устройства ввода (таблет-PC или др.) по осям x и y. Повышение эффективности обработки достигается применением быстрого алгоритма действительного дискретного ортогонального преобразования Хартли (ДПХ) на этапе вычисления скоростных составляющих признаков [2]. Для этого из изображения подписи формировались проекции сегментов на оси x и y в виде дискретных последовательностей $g^p(x)$ и $g^p(y)$ длиной $n = 100 - 200$ отсчетов. Диапазон значений n выбирался с учетом получения необходимых точностных характеристик системы контроля и длительности подписи 1–2 с.

Список литературы

1. Zhang H., Wang K.Y., Wang Y.A Survey of on-line signature verification // Proceedings of 6th Chinese Conference «Biometric Recognition». Beijing, 3–4 December 2011. P. 141–149.

2. Mitsiukhin A. Segmentation of dynamical images by means of discrete Hartley transform // Proceedings of 56 IWK. TU Ilmenau, DE, 12–16 September 2011. URN: urn:nbn:de:gbv:ilm1-2011iwk-011:5, id 1100. P. 1–4.

ИСПОЛЬЗОВАНИЕ РАСШИРЕНИЯ БРАУЗЕРА GHOSTERY ДЛЯ ПРОТИВОДЕЙСТВИЯ ОТСЛЕЖИВАНИЮ ПОЛЬЗОВАТЕЛЯ И КОНТЕКСТНОЙ РЕКЛАМЕ

Н.В. Михальков

В современном мире широко распространена проблема с утечкой конфиденциальной информации через веб-браузер. На многих сайтах работают трекинговые сервисы. Предназначены они для разного, например, для показа ориентированной на пользователя рекламы. И это только в лучшем случае. В худшем случае встроенный вредоносный код может похитить идентификационные данные, например номер карты, PIN-код и пр.

Для блокирования подобного рода слежки существует расширение для браузеров под названием Ghostery. Оно позволяет обеспечить анонимность пользователя в сети Интернет. Для оценки эффективности функционирования расширения проведен эксперимент. Для этого использовался персональный компьютер с операционной системой Windows, подключенный к сети интернет. Интеренет браузер Google Chrome с установленный расширением Ghostery.

На первом этапе исследования выполнялась настройка указанного расширения браузера, в частности такие параметры как аналитика, виджеты, конфиденциальность, маяки,

реклама. Расширение поддерживает технологию белых списков, позволяющих создать список исключений (доменов), для которых будет исключаться блокировка процедуры сбора информации о компьютере пользователя. На втором этапе исследования выполнялось тестирование расширения с предустановленными настройками. Необходимо отметить одно из преимуществ расширения – при блокировке процедур отслеживания со стороны интернет ресурса. Расширение демонстрирует, какие из процедур блокируются.

Таким образом, показано, что Ghostery позволяет просматривать и блокировать средства слежения на посещаемых веб-сайтах, позволяя контролировать сбор пользовательских данных. EnhancedAntiTracking (улучшенный антитрекинг) также обезличивает пользовательские данные для дополнительной конфиденциальности. Из недостатков расширения можно указать на более продолжительную загрузку веб-страниц [1, 2].

Список литературы

1. Расширение для браузеров Ghostery: отключение слежки за поведением посетителя. [Электронный ресурс]. URL: https://www.kv.by (дата обращения: 22.04.2019).

2. Ghostery – анонимность в сети Интернет. [Электронный ресурс]. URL: https://sys-team-admin.ru (дата обращения: 22.04.2019).

3. ОбзорприложенияGhostery Storage Server. [Электронный ресурс]. URL: https://geekon.media (дата обращения: 22.04.2019).

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ PARROT SECURITY OS

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день многие организации проводят мониторинг своей корпоративной сети для обнаружения уязвимостей, воспользовавшись которыми злоумышленники могут осуществить нелегитимные действия. Для проведения мониторинга сети могут закупаться специализированные программные или аппаратные средства, наниматься специалисты по информационной безопасности, использоваться online-инструменты и т.п.

В последнее время наибольшую популярность набирает тестирование на проникновение (пентестинг). Задача данной технологии заключается в осуществлении сетевых атак, которые не приводят к существенным последствиям работы сети, но с помощью которых можно обнаружить недостатки в корпоративной сети. К пентестингу можно отнести дистрибутив Linux – Parrot Security OS.

Parrot Security OS – дистрибутив Linux, основанный на операционной системе Debian. Основные задачи данного дистрибутива – проведение пентестинга, осуществление оценки уязвимостей и их устранение, анонимный просмотр веб-стариц.

Главные отличия представленного дистрибутива от известного Kali Linux следующее:

– в состав Parrot Security OS входит больше инструментов, с помощью которых можно осуществлять пентестинг;

– требует меньше ресурсов при установке, чем Kali;

– Parrot Security OS имеет более удобный графический интерфейс;

– направлен на большую анонимность при работе в сети Интернет, в отличие от дистрибутива Kali Linux.

ЦЕНТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК СОСТАВЛЯЮЩАЯ СИСТЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.В. Моженкова, А.И. Парамонов

В состав корпоративной вычислительной сети входят персональные компьютеры пользователей, и являются одним из источников угроз безопасности данных, обрабатываемых корпоративными информационными системами (КИС) [1]. Для снижения уровня угрозы безопасности на предприятиях вводятся ряд организационных и технических мер

по предотвращению несанкционированного доступа. Они позволяют нейтрализовать предполагаемую угрозу безопасности при работе с КИС. Для организации процесса обслуживания корпоративных вычислительных сетей вводятся регламенты установки, эксплуатации и обслуживания вычислительной техники. Одним из основных требований регламента является сохранение аппаратной и программной конфигурации эксплуатируемой компьютерной техники.

В докладе обсуждается эффективность применения центра программного обеспечения System Center Configuration Manager [2] в вычислительной сети крупного предприятия. На предприятии запрещено самостоятельно устанавливать программное обеспечение (ПО). Службы системной интеграции ежеквартально проводят аудит ПО, установленного на рабочих станциях с целью контроля и обеспечения функционирования средств вычислительной техники, обнаружения нелицензированного ПО и пр. Центр программного обеспечения позволил не только обеспечить контроль установки и обновления ПО, но и сократить количество обращений в службу технической поддержки на 1/3. Эффективность возросла за счет реализации возможности доступа пользователя к установке разрешенного перечня дополнительного ПО, не повышая вероятности угрозы безопасности данных.

Список литературы

1. Моженкова Е.В., Парамонов А.И. Опыт применения методики определения угроз безопасности информации в корпоративных информационных системах // Тез. докл. XVI Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 65.

2. System Center Configuration Manager Documentation [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/sccm/ (дата обращения: 18.04.2019).

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПЕРЕНОСА НОСИТЕЛЕЙ ЗАРЯДА В МНОГОСЛОЙНЫХ ПОЛУПРОВОДНИКОВЫХ СТРУКТУРАХ С ИСПОЛЬЗОВАНИЕМ ГРАФЕНА

В.В. Муравьев, В.Н. Мищенко

Рассмотрены вопросы моделирования процессов переноса носителей заряда в многослойной полупроводниковой структуре с использованием одиночного слоя графена. Высокое значение подвижности электронов, высокая теплопроводность и ряд других положительных свойств делают графен перспективным материалом для использования в полупроводниковых приборах и микросхемах. Вместе с тем, для реализации уникальных свойств и характеристик графена, учитывая двухмерный характер этого материала, весьма важен выбор сопутствующих полупроводниковых и диэлектрических материалов, обеспечивающих формирование законченного в технологическом плане полупроводникового прибора. В этом плане большое внимание привлекает внимание использование пленочного нитрида бора – BN, который может иметь гексогональную кристаллическую структуру, которая близка к структуре графена, небольшую величину толщины слоя, и небольшое значение шероховатости поверхности, величина которой заметно ниже, чем у известных аналогов этого материала. На основе известных принципов, которые лежат в основе использования метода статистического моделирования – метода Монте Карло, проведены исследования основных механизмов рассеяния при переносе носителей заряда в слоях структуры полупроводникового прибора, использующего материалы графен и нитрид бора. Для материала BN с гексогональной кристаллической структурой получены зависимости интенсивностей (частот) рассевания от энергии поля при рассеивании на полярных оптических фононах, на примесях, при акустическом рассеянии, при междолинном рассеивании, а также суммарная зависимость по всем механизмам рассеивания. Исследованы закономерности физического процесса переноса носителей заряда в материале BN. Использование многослойных полевых транзисторов, использующих материалы графен и нитрид бора, позволит создать приборы и устройства, которые найдут широкое применение в системах приема, усиления и обработки сигналов в диапазонах СВЧ и КВЧ.

ТЕПЛОВАЯ СТАБИЛЬНОСТЬ АКУСТООПТИЧЕСКИХ ФИЛЬТРОВ

Е.Н. Наумович, В.И. Журавлёв, В.С. Колбун

Одним из методов защиты информации от несанкционированного доступа к физическому каналу беспроводных интерфейсов является преобразование сигналов, обеспечивающих высокую скрытность передачи, посредством многополосных акустооптических фильтров (АОТФ). В основе таких систем лежит принцип кодирования сигналов в спектральной области, когда последовательность Уолша представляется набором спектральных линий в сигнале с определенной последовательностью спектральных интервалов между ними. При работе АОТФ необходимо обеспечить тепловую стабильность кристаллов, что достижимо с использованием адекватных тепловых моделей.

В работе предлагается использовать тепловые модели АОТФ с распределенными параметрами и различной рассеиваемой мощностью вдоль акустического канала. Кристалл представляется как анизотропное тело с несколькими тепловыми источниками. Для расчета целесообразно использовать частное решение уравнения теплопроводности численными методами. Распределение акустической мощности по траектории ее распространения в кристалле является неравномерным и сильно зависит от геометрии кристалла и частоты волны. Результаты моделирования кристаллов указывают на наличие перегрева в области преобразователя АОТФ и увеличение неравномерности распределения температуры в объеме кристалла с течением времени. Это ведет ухудшение дифракционной эффективности к расфокусировке луча. При еще больших мощностях возрастает температура нагрева, и градиент в объеме кристалла усиливается. Это связано как низкой теплопроводностью материала кристалла, так и неравномерно распределенной выделяемой мощностью вследствие работы АОТФ.

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ FIREBASE AUTHENTICATION В ANDROID-ПРИЛОЖЕНИИ

Е.В. Пендо

Основой безопасной работы приложения является система аутентификации пользователей, позволяющая осуществлять разграничение прав доступа. Помимо разграничения по правам данная система также предоставляет возможность приложению безопасно сохранять пользовательские данные в облаке и обеспечивать одинаковую персонализированную работу на всех устройствах пользователя.

Аутентификация Firebase предоставляет backend-сервисы, простые в использовании SDK и готовые библиотеки пользовательского интерфейса для аутентификации пользователей в приложении. Firebase поддерживает аутентификацию с использованием паролей, телефонных номеров, учетных записей Facebook, Twitter, и многого другого [1].

Аутентификация Firebase тесно интегрируется с другими сервисами и использует отраслевые стандарты, такие как OAuth 2.0 и OpenID Connect [2].

Для использования Firebase Authentication с целью разграничения прав доступа необходимо создать Google Account, который будет использоваться для создания проектов в Firebase Console. После чего необходимо зарегистрировать Android-приложение в проекте, используя package name в качестве идентификатора. После успешного прохождения процедуры регистрации Firebase предоставляет файл конфигурации в формате json, который помещается в приложение. Последним шагом для использования Firebase Authentication в Android-приложении является добавление зависимостей для библиотеки в модули (уровень приложения и уровень модуля) [3].

Таким образом Firebase Authentication является оптимальным сервисом для разграничения прав доступа в Android-приложении, так как в нем используются отраслевые стандарты (OAuth 2.0 и OpenID Connect), а его интеграция занимает не более 10 минут ввиду наличия простых в использовании SDK и готовых библиотек.

Список литературы

1. Firebase Authentication // Firebase [Электронный ресурс]. URL: https://firebase.google.com/docs/auth/ (дата обращения: 06.04.2019).

2. Get Started with Firebase Authentication on Android // Firebase [Электронный ресурс]. – URL: https://firebase.google.com/docs/auth/android/start (дата обращения: 06.04.2019).

3. Add Firebase to your Android project // Firebase [Электронный ресурс]. URL: https://firebase.google.com/docs/android/setup (дата обращения: 06.04.2019).

МЕТОДИКА ИЗГОТОВЛЕНИЯ ГИБКИХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ НА ОСНОВЕ ПОРИСТЫХ ПОРОШКООБРАЗНЫХ МАТЕРИАЛОВ

Д.И. Пеньялоса, М.В. Тумилович

Авторами предложена методика изготовления гибких электромагнитных экранов на основе пористых порошкообразных материалов. Она включает в себя следующие этапы.

Этап 1. Раскрой пенополиуретановых пластин и полиэтиленовой сетки на фрагменты.

Этап 2. Нарезка алюминиевой пленки на фрагменты, длина и ширина которых не превышают 1 см.

Этап 3. Изготовление водного раствора $CaCl_2$ с максимальной концентрацией.

Этап 4. Пропитывание изготовленным водным раствором порошкообразного пористого материала (активированного угля, электрокорунда, перлита т. п.).

Этап 5. Размещение фрагмента полиэтиленовой сетки на фрагменте пенополиуретановой пластины.

Этап 6. Нанесение влагосодержащего пористого порошкообразного материала на фрагмент полиэтиленовой сетки, размещенный на фрагменте пенополиуретановой пластины.

Этап 7. Размещение фрагмента полиэтиленовой сетки на слое из влагосодержащего порошкообразного древесного угля.

Этап 8. Равномерное распределение фрагментов алюминиевой пленки, полученных в результате реализации этапа 2, на фрагменте полиэтиленовой сетки, размещенном поверх слоя влагосодержащего порошкообразного древесного угля.

Этап 9. Размещение фрагмента пенополиуретановой пластины поверх фрагментов алюминиевой пленки.

Этап 10. Герметизация полученной конструкции посредством полиэтилентерефталатной пленки.

Преимущества предложенной методики заключаются в быстроте ее реализации, а также в том, что изготовленные в соответствии с ней электромагнитные экраны характеризуются пониженной массой, ввиду того, что не содержат связующих веществ, используемых для фиксирования частиц порошкообразных материалов.

Электромагнитные экраны, изготовленные в соответствии с предложенной методикой, могут быть использованы для электромагнитного экранирования помещений, в которых располагаются средства обработки информации.

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ ТРЕБОВАНИЯМ СТБ 34.101.73-2017

И.И. Печень

Деятельность по оценке соответствия средств защиты информации является одним из основных механизмов управления информационной безопасностью государства. В рамках представляемой работы выполнены испытания маршрутизатора Cisco ASR 1001, в котором предусмотрена функция межсетевого экранирования, на предмет соответствия требованиям СТБ 34.101.73-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Межсетевые экраны. Общие требования». Испытания выполнены в соответствии с предложенной методикой, включающей в себя следующие шаги.

1. Выбор оборудования для разворачивания испытательного стенда.

2. Выбор программного обеспечения для проведения испытаний.

3. Сборка испытательного стенда на основе выбранного оборудования (в том числе, установка выбранного программного обеспечения, подключение к стенду испытываемого маршрутизатора).

4. Конфигурирование испытываемого маршрутизатора.

5. Проверка следующих функций межсетевого экрана на предмет их выполнимости:

– контроль и фильтрация сетевого трафика по различным сетевым протоколам, IP-адресам и портам, протоколам уровня приложений на основе заданных правил для разграничения доступа и защиты от несанкционированного трафика;

– учет и регистрация различных событий, включая вход, выход и действия субъектов доступа, нарушений заданных правил безопасности, фильтруемых пакетов запросов сервисов, виртуальных соединений и т. д.;

– основные и дополнительные возможности по идентификации, аутентификации, авторизации пользователей, доступа к сетевым сервисам, трансляции адресов и портов, ведения отчетности и уведомления, контроля функционирования целостности и восстановления, синхронизации с иными сетевыми сервисами и службами.

На основании полученных результатов был сделан вывод о том, что исследованное устройство соответствует всем требованиям СТБ 34.101.73–2017, а, следовательно, может быть сертифицировано как средство межсетевого экранирования.

ОСОБЕННОСТИ КОНТРОЛЯ РАБОТНИКОВ ОХРАНЫ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

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

Контроль выполнения работниками охраны своих функциональных обязанностей является неотъемлемой частью мероприятий по обеспечению безопасности объектов. В первую очередь это касается крупных объектов, где охранники должны осуществлять периодический обход территории по заданному маршруту в установленное время. Обеспечение этого контроля ранее осуществлялось исключительно организационными мероприятиями в виде периодических инспекционных проверок.

В последнее время набирают популярность технические средства контроля выполнения охраной объекта своих обязанностей. Как правило, это реализуется в виде персонального электронного устройства (ПЭУ), с которым охранник осуществляет обход подведомственной территории. Контроль может обеспечиваться либо посредством обхода специально установленных электронных меток, либо по заданному маршруту. Электронные метки (контактные или бесконтактные) устанавливаются в заданных местах объекта. Специалист охраны должен произвести считывание каждой метки в установленное время и в заданной последовательности. Контроль по маршруту осуществляется посредством GPS навигатора, установленного в ПЭУ. К недостаткам первого метода относится отсутствие контроля за охранником в промежутках обхода между метками, к недостаткам второго метода – дороговизна ПЭУ, сложность программного обеспечения, невозможность контроля в зданиях и сооружениях с металлическими конструкциями.

В докладе рассмотрены методы практической реализации каждого из этих методов, способы анализа и обработки полученной информации. Особое внимание уделяется способам переноса информации с ПЭУ охранника на компьютер инспектирующих органов. Проанализированы возможности, достоинства и недостатки как непосредственного переноса информации на персональный компьютер инспектора, так и с помощью промежуточных носителей информации.

Рассмотрены вопросы антисаботажных мероприятий по обеспечению работоспособности и анализу технического состояния ПЭУ. Часто охранники пытаются вывести ПЭУ из строя путем механических, электрических воздействий или воздействием воды. В этом случае задача разработчика состоит не только в обеспечении должного качества и надежности изделий, но и возможность однозначной диагностики причин возникновения отказов.

ПОВЫШЕНИЕ СКРЫТНОСТИ И ИНФОРМАТИВНОСТИ СРЕДСТВ ОХРАННОЙ СИГНАЛИЗАЦИИ

В.В. Платон

В настоящее время в сигнализационных комплексах наиболее широко используются датчики серии РЛД-94. Изделия используют физический принцип, основанный на преобразовании в сигнал тревоги изменений параметров электромагнитного поля на входе приемного устройства при появлении нарушителя в зоне обнаружения.

РЛД-94 обеспечивает высокую вероятность обнаружения нарушителя >0,98, наработку на ложное срабатывание не менее 3000 час, наработку на отказ – 30000 ч. Устойчиво к воздействию ливневых дождей и практически не реагирует на мелких животных. Корпус антенного блока выполнен из неподверженного коррозии алюминия, что обеспечивает длительный срок службы и резко уменьшает воздействие внешних электромагнитных помех, механическую прочность при резких колебаниях температур от –50 до +65 градусов.

Разнообразие моделей РЛД-94 (УМ-50-18 – до 50 м; УМ-150-18 – до 150 м; УМ-300-18 – до 300 м) позволяет потребителю оптимизировать затраты на организацию сигнализационного блокирования рубежа различной протяженности и конфигурации за счет рационального использования возможностей моделей и разницы в их цене [1].

С точки зрения повышения информативности и электромагнитной совместимости целесообразен переход к системам просветной радиолокации, реализующих не монохроматический, а линейно-частотномодулированный сигнал. В этом случае возможно измерение дальности, получение дальномерного портрета цели, снижение влияния мешающих отражений, повышение скрытности и характеристик электромагнитной совместимости.

Также повышения скрытности можно достичь снижением спектральной плотности при заданной мощности передающего устройства, оно достигается расширением спектра зондирующего сигнала, что также повышает разрешающую способность РЛС по дальности [2–4].

Список литературы

1. Лавриненко А.В. Периметровые средства обнаружения: современное состояние // Специальная техника. 2001. № 5. С. 14–18.

2. Сальников И.И. Чернышев М.Н. Определение размера и скорости движения нарушителя в двухпозиционных охранных системах ближней радиолокации // Известия высших учебных заведений. Поволжский регион. Технические науки. 2011. № 1 (17). С. 96–105.

3. Смирнова Д.М. Обнаружение и измерение координат движущихся наземных объектов в многопозиционной просветной радиолокационной системе: автореф. дис. …к-та техн. наук. Нижний Новгород, 2014. 16 с.

4. Зубков А.Н. Радиолокационная система обнаружения наземных целей в коротковолновой части ММ диапазона // Сб. докл. НТК по миллиметровой технике. Львов, ЛНИРТИ, 1986.

ОБУЧЕНИЕ СЛУШАТЕЛЕЙ КУРСОВ ПЕРЕПОДГОТОВКИ ОСНОВАМ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Полубок, А.А. Косак

В настоящее время фраза Н. Ротшильда «Кто владеет информацией, тот владеет миром» стала как никогда актуальной. Огромный прогресс в области информационных технологий привел к тому, что компании и частные лица как никогда стали зависимыми от информационных систем и их безопасности. В настоящее время вопрос информационной безопасности становится одним из основных аспектов при разработке информационных систем.

Анализ подхода к обучению слушателей переподготовки по специальностям, связанным с информационными технологиями, свидетельствует о недостаточной подготовке в области технологий обеспечения информационной безопасности. Результаты анализа показывают, что необходима фундаментализация обучения слушателей технологиям защиты

информации, что позволит познакомить их с фундаментальными основами теории защиты информации, общей схемой обеспечения информационной безопасности, со структурой унифицированной концепции и стратегией защиты информации. Рассмотрение фундаментальных основ теории защиты информации позволит сформировать представление о подходах к защите информации, инвариантных относительно развития разных информационных технологий [1].

Обучение основам защиты информации в рамках курсов переподготовки по ИТ-специальностям можно разделить на два направления: программное и техническое. Если технические методы защиты информации рассматриваются слушателями в рамках курса «Компьютерные сети», то программные методы защиты информации в рамках специальности не рассматриваются. В настоящее время прорабатывается возможность введения в рамках курса, где слушатели изучают основы алгоритмизации и программирования, темы «Основы защиты информации», в которой будут рассматриваться как основы защиты информации на уровне программного обеспечения, так и основные алгоритмы шифрования данных (например: AES, DES, RSA, RC4), будут описываться основные преимущества и недостатки и приводится варианты их применения на практике. Для закрепления полученных знаний слушателям, в рамках практических занятий, будет предложено реализовать один из алгоритмов шифрования. Полученные теоретические и практические навыки в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Димов Е.Д. Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования: автореф. дис. ... канд. пед. наук. Москва, 2013. 25 с.

МОНИТОРИНГ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ, СОЗДАВАЕМЫХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКОЙ

В.А. Попов, А.В. Потапович, П.Л. Прудников

В условиях стремительно развивающейся современной вычислительной техники, переноса на ЭВМ большинства количества и видов анализа и обработки информации, возникла и начала развиваться киберпреступность. Одной из ее разновидностей является перехват обрабатываемой на ЭВМ информации путем внедрения в агрегаты вычислительной машины аппаратной закладки, считывающей обрабатываемые в памяти компьютера данные и передаче ее по радиоканалу с помощью встроенных в вычислительную технику недекларированных возможностей. Встроенные недекларированные возможности в вычислительную технику могут быть организованы как программным путем с использованием не основных по функциональному назначению свойств элементной базы, так и аппаратно-программным путем. Такие встроенные недекларированные возможности вычислительной техники могут эпизодически кратковременно организовывать передачу информации в сжатом виде на некоторой частоте по радиоканалу. Исходя из этого, становится очевидным один из методов обнаружения подобных устройств несанкционированного съема информации – мониторинг электромагнитного излучения вычислительной техники.

Важнейшим показателем мониторинга электромагнитного излучения является выбор необходимого диапазона частот. При выборе частотного диапазона мониторинга исходили из предпосылок наиболее простого и доступного метода организации получения информации. Частотный диапазон предлагается выбрать от 10 МГц до 10 ГГц с разбиением его на 10 октавных полос.

Устройство мониторинга может применяться на рабочих местах, в машинных залах предприятий, осуществляющих обработку конфиденциальной информации на ЭВМ. Сигнал тревоги от устройства мониторинга послужит основанием для выполнения работ с целью проверки узлов и агрегатов ЭВМ на предмет наличия недекларированных возможностей.

АНАЛИЗ УЯЗВИМОСТИ «PROTOTYPE POLLUTION» В JQUERY

М.Г. Прахоцкий, М.В. Стержанов, А.Л. Хотеев, В.Н. Теслюк

jQuery – достаточно популярная в прошлом библиотека JavaScript, фокусирующаяся на взаимодействии JavaScript и HTML [1]. Библиотека помогает легко получать доступ к любому элементу DOM, обращаться к атрибутам и содержимому элементов DOM, манипулировать ими. Также библиотека предоставляет удобный API для работы с AJAX. Хоть времена jQuery уже давно прошли, однако до сих пор существует большое количество сайтов, которые используют эту библиотеку.

Следовательно, любые недостатки, обнаруженные в библиотеке jQuery, автоматически открывают двери для атак на сотни миллионов веб-сайтов. Одной из недавно обнаруженных проблем в этой библиотеке стала уязвимость вида «Prototype Pollution». Влияние этой проблемы может быть серьезным, учитывая, что библиотека JavaScript jQuery в настоящее время используется на 74 процентах веб-сайтов в Интернете, большинство сайтов по-прежнему используют версии библиотеки 1.x и 2.x, которые подвержены уязвимости «загрязнение прототипа».

Эта уязвимость безопасности, упоминаемая и проявляющаяся как «загрязнение прототипа», позволяет злоумышленникам перезаписать прототип объекта приложения JavaScript. Когда это происходит, свойства, которыми управляет злоумышленник, могут быть внедрены в объекты, а затем либо привести к аварийной остановке приложения, либо внедриться в исходный код приложения, давая злоумышленнику полный доступ к управлению приложением [2].

Список литературы

1. Адам Фримен. jQuery для профессионалов = Pro jQuery. М.: «Вильямс», 2012. 960 с.
2. Самков Г. jQuery. Сборник рецептов. СПб.: БХВ-Петербург, 2010. 416 с.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

З.Н. Примичева

С ростом информационного обмена и в условиях необходимости защиты информационных ресурсов страны спрос на специалистов по защите информации постоянно растет. В настоящее время преподавание должно сочетать в равной степени традиционную и современную интерактивную модели обучения. Современная интерактивная образовательная модель основывается на внедрении в процесс обучения таких инновационных методов, как метод проблемного изложения, презентация, мини-исследования и др., позволяет изменить роль преподавателя и сделать его руководителем самостоятельной творческой работы студента, предполагает большую активность обучаемого, развитие личностного потенциала студента.

Квалифицированный IT-специалист должен владеть основами информационной безопасности, уметь анализировать и оценивать ее угрозы, знать в этой области нормативную базу. Для успешного применения современных методов и средств защиты информационных систем на практике специалисту необходимо иметь всестороннюю подготовку в области математики и информационных технологий, владеть навыками абстрактного математического мышления и уметь применять абстрактные математические знания при решении конкретных задач реальной действительности. Математическая подготовка IT-специалистов должна быть ориентирована на изучение дисциплин, которые непосредственно используются в формировании основ области информационных технологий и сфер их применения.

Для повышения профессиональной компетентности специалиста по защите информации необходимы знания, которые не входят в классический курс «Высшая математика», по основам линейной алгебры (по конечным полям, кольцам, группам, линейным пространствам над конечными полями), преобразованиям Фурье и их использованию при

передаче и обработке цифровых данных, теории вероятности, теории графов, основам теории множеств. Поэтому на кафедре высшей математики разработаны специальные дисциплины «Прикладная математика», «Теория норм синдромов» и «Специальные математические методы и функции».

ПРОГРАММНЫЙ МОДУЛЬ КЛАССИФИКАЦИИ РЕЧИ НА ОСНОВЕ КЕПСТРАЛЬНОГО АНАЛИЗА

А.С. Райкевич, О.Б. Зельманский

На сегодняшний день в компьютерных системах все больше внимания уделяется построению интерфейса речевого ввода-вывода, эффективность которого основана на практически неограниченных возможностях формулировки на естественном языке всевозможных задач в самых различных областях человеческой деятельности [1]. Разработка эффективных алгоритмов классификации речи является ключевым моментов в решении задач: преобразования речи в текст, понимания речи, голосового управления, автоматического перевода, детектирования речи в телефонии и т. д. [2, 3]. Предлагается программный модуль классификации речи, в основу которого положена методика вычисления мел-частотных кепстральных коэффициентов фонем языка. Коэффициенты соответствия между фонемами вычисляются при помощи алгоритма динамического программирования. Программный модуль реализован в среде MATLAB. В ходе тестирования модуля устанавливалась принадлежность неизвестной фонемы к определенному классу фонем русского языка, произнесенных одним диктором. Описаны результаты для каждого класса фонем русского языка: гласных, сонорных согласных, глухих шумных согласных, звонких шумных согласных.

Список литературы

1. Мусорин А.Ю. Основы науки о языке. Новосибирск: Новосибирское книжное издательство, 2004. 196 с.

2. Huang X., Acero A., Hon H. Spoken language processing: a guide to theory, algorithm, and system development. Prentice Hall PTR, 2001.

3. Сато Ю. Обработка сигналов. М. : Додэка-XXI, 2002. 176 с.

МЕТОДИКА ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ БАЗ ДАННЫХ»

В.Т. Ревин

В теоретическую часть дисциплины «Безопасность баз данных» входят как основные понятия теории баз данных, так и принципы функционирования и команды языка конкретной системы управления информационными ресурсами. Большое внимание в начальном этапе изучения баз данных уделяется терминам и определениям основных понятий баз данных как научного направления, поскольку в современной учебной литературе даже само определение «База данных» встречается в литературных источниках в более чем двадцати модификациях.

Поэтому определенный отрезок времени в начале теоретического курса отведен следующему алгоритму: база данных → отношение → атрибут → кортеж → домен → отображение → ассоциация. Вводится понятие информационной модели данных, определяется ее состав. Важным шагом является обязательное знакомство с реляционном подходом, его современными преимуществами. Но и не отбрасываются более сложные модели построения баз данных, например, постреляционные и многомерные базы данных.

Теоретические аспекты моделей баз данных, основные принципы их проектирования и реализации модели баз данных рассматриваются в объеме, достаточном для понимания основных принципов разработки баз данных, моделирования конкретной информационной задачи, обеспечения целостности и непротиворечивости данных.

Для достижения планируемых результатов освоения дисциплины «Безопасность баз данных» предлагается сочетание традиционных образовательных технологий в форме лекций с интерактивными практическими занятиями, компьютерными автоматизированными

информационными технологиями при выполнении лабораторных работ и проведении мероприятий по контролю успеваемости.

Значительное внимание при изучении дисциплины уделяется активным методам преподавания, которые подразумевают проведение деловых игр для моделирования поведения современного технического специалиста в реальных рабочих ситуациях, использование виртуальных компьютерных средств и других современных учебно-методических средств. Например, в процессе проведения практических занятий предлагается разработка виртуальных средств измерений (по направлениям), получение измерительной информации в виде отношений с последующим использованием ее в учебной базе данных, разрабатываемой при проведении лабораторных занятий.

Итогом изучения дисциплины «Безопасность баз данных» является самостоятельно выполненный индивидуальный проект, в котором обеспечивается многоуровневая защита разработанной базы данных, устанавливается проверку поддержки целостности данных.

СПИНТРОННЫЕ ЭЛЕМЕНТЫ РЕЗИСТИВНОЙ ПАМЯТИ

М.В. Ремизевич, А.Л. Данилюк

В настоящее время устройства резистивной памяти с произвольной выборкой (RRAM) активно разрабатываются. В перспективе они могут заменить магнитную память (MRAM). Однако еще существует ряд нерешенных проблем, связанных как с пониманием физического механизма переключения сопротивления в электрическом поле, так и с воспроизводимостью параметров элементов памяти. Наноструктуры на основе диоксида гафния перспективны для использования в энергонезависимой резистивной памяти. Оксид гафния имеет высокую диэлектрическую проницаемость, относительно высокую энергия запрещенной зоны и образует термодинамически устойчивый интерфейс с кремнием. Электрический пробой диэлектрика приводит к переключению в состояние с низким сопротивлением и созданию высокой плотности ловушек, что делает возможным долговременное хранение заряда (до 10^6–10^7 с) [1]. Практические результаты состоят в получении стабильных наноразмерных слоев диоксида гафния, переключаемых низким потенциалом. К наиболее важным задачам относится выявление особенностей, связанных с механизмом переключения диоксида гафния из состояния с высоким сопротивлением в состояние с низким сопротивлением. Одна из таких особенностей связана с наличием случайного телеграфного шума, возникающего при электроформовке диоксида гафния. Особый класс элементов памяти и логики составляют спиновые аналоги элементов резистивной памяти, в которых переключение сопротивления обусловливается наличием обратимого электрического пробоя и наблюдается усиление мемристорного эффекта [2, 3].

В данной работе, исходя из гипотезы о бистабильном характере ловушечных состояний, представлены результаты моделирования переключения бистабильных ловушечных состояний в элементах резистивной памяти при наличии поляризованного по спину тока. Приводятся результаты анализа влияния инжекции спин-поляризованного тока на время переключения сопротивления и параметры бистабильных ловушечных центров.

Список литературы

1. F. Pan [et al.] // Materials Science and Engineering R. 2014. Vol. 83. P. 1–59.
2. B.Li [et al.] // Organic Electronics. 2010. Vol. 11. P. 1149–1153.
3. M. Prezioso [et al.] // Advanced Materials. 2013. Vol. 25. P. 534–538.

ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ НА ОСНОВЕ СТОХАСТИЧЕСКОГО ГЕОМЕТРИЧЕСКОГО ПОДХОДА

С.Б. Саломатин, Аль-Эзайрджави Атир Абдулзахра Салах

Стохастическая геометрия используется для изучения показателей безопасности физического уровня беспроводных сетей с подслушивающим каналом передачи. Топология

сети предполагает, что легитимные пользователи и подслушивающие аналитики случайным образом расположены на большой географической территории в соответствии с некоторыми вероятностными распределениями.

Рассматривается децентрализованная беспроводная сеть в двумерном пространстве на основе гомогенной модели однородного точечного пуассоновского процесса PPP. Местоположения легитимных передатчиков соответствуют однородному PPP с интенсивностью λ. Каждый передатчик имеет предполагаемый приемник на фиксированном расстоянии r в случайном направлении [1, 2].

Определяются следующие основные показатели системы защиты.

Граф защищенности. Используется для изучения свойств связности среди легитимных пользователей сети и характеризует существование связи с полной защитой между любыми двумя легитимными пользователями.

Пропускная способность защищенной сети. Учитывает одновременные передачи между всеми допустимыми линиями связи и дает математически поддающийся измерению показатель достижимой пропускной способности сети с заданным требованием защиты на основе перколяционной модели.

Отключение соединения. Событие, когда пропускная способность канала от передатчика для предполагаемого приемника ниже скорости кодового слова. Вероятность этого события называется вероятностью отказа соединения, обозначается как Pco

Сбой в работе системы защиты. Событие, когда пропускная способность канала от передатчика, по крайней мере, к одному перехватчику превышает структурную избыточность. Вероятность того, что это событие произойдет, называется вероятностью отключения секретности, обозначаемой как Pso.

Список литературы

1. Franceschetti R. Random Networks for Communication: from Statistical Physics to Information Systems. Cambridge University Press, 2008.

2. Vaze R. Random Wireless Networks, Cambridge University Press, 2015.

РЕШЕТЧАТАЯ КРИПТОСИСТЕМА НА ОСНОВЕ МНОГООБРАЗИЯ БАЗИСОВ

С.Б. Саломатин, В.В. Панькова

Криптографические механизмы используют библиотеки решетчатого кодирования с масштабируемой реализации примитивов гомоморфного преобразования [1, 2].

Базовая структура решетчатых криптосистем соответствует архитектуре криптосистемы Мак-Элиса с секретной функцией на основе решеток [3]. Исходная криптосистема описывается следующим образом:

Генерация ключей. Формируется удобный с вычислительной точки зрения базис решетки R. Базис R преобразуется в трудно обратимый базис Q с помощью унимодулярного преобразования.. Базис Q используется в качестве открытого ключа (открытого базиса), а базис R – в качестве секретного ключа шифрования (закрытого базиса).

Процедура зашифрования. Выбирается любой вектор решетки **w**, используя открытый базис Q, и к нему добавляется вектор открытого текста **p**. Вектор $\mathbf{c} = \mathbf{w} + \mathbf{p}$ представляет собой зашифрованный текст.

Расшифрование. Используя закрытый базис, решается задача вычисления ближайшего вектора решетки **nw** к зашифрованному тексту **c**. Найденный ближайший вектор решетки **nw** вычитается из зашифрованного текста для получения открытого текста $\mathbf{p} = \mathbf{c}–\mathbf{nw}$.

Безопасность криптосистемы основывается на следующих трех предположениях. Легко вычислить неудобный базис Q из базиса R, но вычислительно трудно решить обратную задачу. Легко создать случайный вектор решетки даже с неудобным базисом Q. Легко найти ближайший вектор с удобным базисом R, но трудно это сделать с открытым базисом Q.

Дополнительное усиление системы состоит в использовании нормальной формы Эрмита для базиса открытого ключа, базисов генераторных матриц алгебро-геометрических структур и построения семейств PRF на основе решеток, через задачи обучения с ошибками (LWE).

Список литературы

1. Шокуров А.В., Кузюрин Н.Н., Фомин С.А. Решетки, алгоритмы и современная криптография. М.: Институт системного программирования РАН, 2011. 130 с.

2. Gentry C. Fully homomorphic encryption using ideal lattices // STOC. 2009. P. 169–178.

3. Micciancio D. Complexity of Lattice Problems. A Cryptgraphic Perspective. Kluwer Academic Publishers, 2002.

АППАРАТНЫЙ МОДУЛЬ ШИФРОВАНИЯ ПОТОКОВЫХ ДАННЫХ

Ю.И. Сапронова

Программные реализации являются более дешевыми и гибкими, однако аппаратные системы имеют выигрыш в производительности и являются гораздо более надежными, за счет использования генератора истинно случайных чисел, а также хранения ключей непосредственно на плате шифратора, а не в оперативной памяти компьютера.

Комбинированный (гибридный) алгоритм шифрования, сочетает в себе симметричный и асимметричный методы шифрования: с помощью симметричного алгоритма шифруется исходная информация, а с помощью асимметричного – сессионный ключ, используемый симметричным алгоритмом. Такой способ устраняет проблему распространения ключей для симметричных алгоритмов, помимо этого, такой способ решает проблему быстродействия асимметричных алгоритмов за счет того, что шифрованию подлежат не передаваемые сообщения, а только сессионный ключ.

Для шифрования данных выбран потоковый шифр Grain, в связи с тем, что он обладает наилучшей производительностью, при этом потребляя меньшее количество ресурсов (по сравнению с AES, MICKEY и Trivium [1]). Кроме того, производительность данного алгоритма может быть увеличена за счет использования дополнительного количества ресурсов FPGA (добавлением параллельных блоков сдвиговых регистров с линейной и нелинейной обратной связью). Для шифрования сессионного ключа выбран алгоритм RSA.

Анализ разработанной системы показал, что достижимая частота работы модуля в режиме шифрования при условии наличия одного блока сдвиговых регистров с линейной и нелинейной обратной связью составила 50 МГц. Для обеспечения достаточного уровня защиты данных синхронизация блоков и, при необходимости, смена сессионного ключа должна производиться каждый час.

Список литературы

1. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128 [Электронный ресурс]. URL: https://eprint.iacr.org/2009/218.pdf (дата обращения: 02.05.2019).

ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ КВАТЕРНИОНОВ

Ю.И. Сапронова

Алгебра кватернионов представляет собой ассоциативную четырехмерную гиперкомплексную алгебру над полем действительных чисел с уникальными законами умножения. Шифрование, основанное на кватернионах, представленное в [1], использует уникальные свойства кватернионов для поворота векторов данных в трехмерном пространстве. Как известно, вращение вектора представляется в виде результата произведения кватерниона вращения, вектора, представленного в виде кватерниона, и обратного кватерниона вращения.

Умножение кватернионов является затратной вычислительной операцией. Экспериментально было показано, что применение логарифмической системы счисления для вычисления произведения кватернионов может сократить затраты памяти на хранение коэффициентов кватернионов на 14% (при использовании логарифмического полярного

представления кватерниона в форме Кэли-Диксона), тем самым можно увеличить количество блоков обработки информации.

Процесс шифрования заключается в применении нескольких вращений к каждому из блоков шифруемой информации. При этом начальными значениями для алгоритма является порядок вращения вектора, а также кватернион вращения и синхропосылка, представленная в виде кватерниона инициализации. Рассмотренный метод шифрования можно считать симметричным потоковым алгоритмом с размером единицы шифруемой информации равной четырем машинным слова. Важно отметить, что при использовании такого алгоритма количество возможных ключей фактически безгранично из-за возможности установки порядка вращения и четырех параметров кватерниона вращения и синхропосылки. Однако, ввиду высокой сложности вычислений произведения кватернионов невозможно добиться высокой производительности данного алгоритма.

Список литературы

1. A new Quadripartite Public-Key Cryptosystem / T. Nagase [et al.] // ISCIT 2004. Sapporo, 26–29 October 2004. P.74–79.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ БЕЛОРУССКОЙ АЭС

С.М. Сацук

Подготовка высококвалифицированных кадров – один из самых важных факторов безопасной и эффективной эксплуатации атомной электростанции. Государственная программа подготовки кадров для ядерной энергетики Республики Беларусь на 2008–2020 годы была утверждена в связи с принятием решения о строительстве Белорусской атомной электростанции согласно Постановлению Совета Министров № 1329 от 10 сентября 2008 г. С 2016 года задача подготовки кадров осуществляется в рамках Государственной программы «Образование и молодежная политика» на 2016-2020 годы (Подпрограмма 10 «Подготовка кадров для ядерной энергетики»), утвержденной Постановлением Совета Министров Республики Беларусь № 250 от 28 марта 2016 г.

В соответствии с рекомендациями Международного агентства по атомной энергии (МАГАТЭ) система подготовки кадров для ядерной энергетики должна базироваться на принципах применения системного подхода к подготовке персонала, основанного на соответствующих документах МАГАТЭ, международном опыте, а также на соответствии системы подготовки персонала требованиям законодательства в области ядерной и радиационной безопасности.

В этой связи ряд стран, членов МАГАТЭ, как с развитой ядерной инфраструктурой, так и с развивающейся, выразили желание о сотрудничестве для обмена опытом в области ядерной энергетики и обеспечения стабильного развития ядерного сектора. В 2015 году была создана Региональная сеть STAR-NET.

Основной целью сети STAR-NET является улучшение качества подготовки кадров для ядерной энергетики. Основными направлениями деятельности сети являются: образовательная деятельность и учебно-методическая работа; профессиональная подготовка и взаимодействие с атомной промышленностью; исследовательская и научно-техническая деятельность; информационные системы поддержки деятельности сети.

Региональная сеть образования и подготовки кадров в области ядерных технологий STAR-NET является связующим звеном для реализации научно-образовательных проектов в области подготовки кадров для ядерной энергетики.

РАЗБОРЧИВОСТЬ РЕЧИ ПРИ ЕЕ ЗАЩИТЕ КОМБИНИРОВАННЫМИ МАСКИРУЮЩИМИ СИГНАЛАМИ

Е.Н. Сейткулов, Р.М. Оспанов, Г.В. Давыдов

Комбинированные маскирующие сигналы, предназначенные для защиты речевой информации от утечки по техническим каналам, обычно содержат шумовую компоненту в виде «белого» шума и речеподобную помеху, сформированную по базе структурных единиц речи с учетом распределения вероятностей их появления в данном языке [1–3]. Так как речеподобные сигналы по своим формальным свойствам близки к слитной речи, однако имеются временные участки, где речеподобный сигнал отсутствует (также 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 временные участки. Речеподобные сигналы могут быть сформированы и в виде диалога участников переговоров.

Разборчивость речи, маскированной комбинированными сигналами, оценить аналитически является весьма сложным процессом, 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.

Особенность речевых сигналов заключается в том, что с энергетической точки зрения они имеют формантный характер. Форманта – эта область частотного диапазона, в которой сосредоточена основная энергия при произношении определенной гласной фонемы. Для каждой из гласных фонем число формант может составлять от 3 до 5. Если согласные звуки имеют распределение энергии по диапазону частот, то для гласных звуков характерно концентрация энергии в определенных областях частотного диапазона.

Экспериментальные исследования энергетических характеристик гласных и согласных, глухих и звонких, твердых и мягких показали, что энергетические показатели гласных составляют порядка 70–78 дБ при среднеквадратичном значении звукового давления 70 дБ. При этом гласные под ударением произносятся при звуковом давлении 73–78 дБ. Для шипящих и свистящих характерно значение звукового давления в 58–63 дБ и без явно выраженных формант в спектре. Разборчивость речи будет определяться соотношением между информационным речевым сигналами и уровнем маскирующего шума с речеподобными сигналами. При этом отношение речеподобного сигнала к маскирующему «белому» шуму составляет – 6 дБ.

Работа выполнена при поддержке грантового финансирования КН МОН РК, № AP05130293.

Список литературы

1. Давыдов Г.В., Потапович А.В., Сейткулов Е.Н. Метод формирования комбинированных маскирующих речь сигналов // Матер. Междунар. науч.-техн. конф., приуроченной к 50-летию МРТИ–БГУИР. Минск, 18–19 марта 2014 г. В 2 ч. Ч. 1. 2014. С. 344–345.

2. Технические средства и методы защиты информации // А.П. Зайцев [и др.]. М.: ООО «Издательство Машиностроение», 2009 508 с.

3. Method for protecting speech information / H.V. Davydau [et al.] // Doklady BGUIR. 2015. № 8 (94). P. 107–110.

МЕТОДИКА ОПРЕДЕЛЕНИЯ СЛУХОВОЙ ЧУСТВИТЕЛЬНОСТИ АУДИТОРОВ

Е.Н. Сейткулов, Н.Н. Ташатов, Г.В. Давыдов

Слуховая чувствительностью с порогом восприятия чистых тонов не более 0–5 дБ в диапазоне частот от 500 до 2000 Гц считается хорошим показателем для аудиторов. Вместе

с тем, определение слуховой чувствительности является весьма трудоемким процессом. На результаты измерений могут оказывать ряд факторов, исключить влияние которых является весьма проблематичной задачей. Первое с чем сталкивается исследователь это весьма высокие внешние акустические шумы. Для исключения этого фактора определение порога восприятия чистых тонов необходимо проводить в акустически заглушенной камере с уровнем звукового давления фонового акустического шума в диапазоне частот 100 Гц – 10000 Гц не более 20 дБ.

Второе, это методика формирования тестовых сигналов. Наиболее удобный вариант это формирование тестовых сигналов с помощью компьютера и воспроизведение тоновых акустических сигналов с заданным уровнем звукового давления и контроль уровня звукового давления в месте расположения аудитора. Тестовый сигнал необходимо формировать на частотах 500, 1000 и 2000 Гц с повышением уровня звукового давления от 0 дБ до 10 дБ с шагом 0,25 дБ. При этом время воспроизведения акустического сигнала на каждой ступени должно составлять от 3 до 5 с. Переход от одного уровня сигнала к другому уровню сигнала необходимо выполнять при переходе синусоидального сигнала через ноль. Кроме тестового сигнала с повышением уровня звукового давления необходимо формировать тестовый сигнал, с понижением уровня звукового давления начиная с 10 дБ до 0 дБ с шагом 0,25 дБ. Изменение уровня сигнала также выполняется при переходе синусоидального сигнала через ноль. При экспериментальных исследованиях у аудитора должны быть кнопка для подтверждения слухового восприятия акустического сигнала.

Третье, измерение уровня звукового давления в месте расположения аудитора необходимо выполнять с использованием высокочувствительного микрофона с предварительным усилителем с уровнем собственных шумов не более 0 дБ в диапазоне частот от 10 до 10000 Гц. Такими характеристиками обладает микрофонный капсюль 4179 с предварительным усилителем 2660 фирмы «Bruel & Sound & Vibration Measurement A/S». Сигнал, принятый от микрофона необходимо пропустить через узкополосый полосовой фильтр для выделения чистых тонов, на которых проверяется порог восприятия.

Слуховая чувствительность аудиторов в сильной степени зависит от состояния аудитора. Если в течении последних суток перед измерением слуховой чувствительности аудитора он находился в условиях воздействия акустических шумов с уровнем звукового давления порядка 100 дБ в течении получаса или на его слуховой аппарат от наушников воздействовали повышенные уровни звукового давления, результаты проверки слуховой чувствительности дадут заниженные показатели. Это подтверждает тот факт, что слуховая чувствительность аудитора изменяется от состояния аудитора. Поэтому при оценке разборчивости маскируемой шумами речи кроме отбора аудиторов необходимо проводить их обучение и подготовку к проведению работ по распознаванию речи [1].

Работа выполнена при поддержке грантового финансирования КН МОН РК, № AP05130293.

Список литературы

1. Method for protecting speech information / H.V. Davydau [et al.] // Doklady BGUIR. 2015. № 8 (94). P. 107–110.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ РОЕВЫХ РОБОТОВ

А.В. Сидоренко, М.С. Шишко

Безопасность в информационной среде, включая роботизированные роевые системы, принципиально связана с предоставлением основных услуг, таких как конфиденциальность данных, целостность данных, аутентификация объектов и аутентификация источника данных.

В отличие от других областей, в которых активно проводятся исследования, связанные с безопасностью, роботизированные роевые системы испытывают недостаток практических решений этих проблем [1]. Тема безопасности была упущена из современных исследований в основном из-за сложных и гетерогенных характеристик роботизированных систем: автономии роботов, децентрализованного контроля, потенциально большого количества членов роя, коллективного поведения и т. д.

Технология блокчейн может обеспечить не только надежный peer-to-peer канал связи для агентов роя, но также способ преодоления потенциальных угроз, уязвимостей и атак [2]. Блокчейн – это новая технология, возникшая в поле биткоин, и демонстрирующая, что с помощью объединения одноранговой сети с криптографическими алгоритмами, группа агентов может достичь соглашения по конкретному положению дел и зафиксировать это соглашение без необходимости обращения к контролирующему органу. Комбинация блокчейна с другими распределенными системами, такими как роботизированные роевые системы, может предоставить необходимые возможности, для того, чтобы сделать операции внутри роботизированного роя более безопасными, автономными и гибкими.

Наличие распределенных данных может облегчить реализацию некоторых алгоритмов роевой робототехники и может проложить путь для новых приложений роевой робототехники (например, алгоритмам машинного обучения). Использование технологии блокчейна в качестве децентрализованной защищенной системы управления может быть полезным при решении широкого спектра задач. Распределенная система хранения данных внутри роя накладывает дополнительные требования к вычислительным ресурсам и памяти отдельных участников роя. Следовательно, данный подход может использован для отдельных задач и систем в робототехнике.

Список литературы

1. Higgins F., Tomlinson A., Martin M. Security Challenges for Swarm Robotics // Technical Report. University of London, Royal Holloway, Department of Mathematics, October 2008.

2. Strobel V., Dorigo M. Blockchain technology for robot swarms: A shared knowledge and reputation management system for collective estimation // Technical Report Series. IRIDIA, 2018.

ПРОБЛЕМЫ ВЫСШЕЙ ШКОЛЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Б. Соколов

Одной из основных проблем высшей школы при подготовке специалистов в области информационной защиты является недостаточная квалификация преподавательского состава. В основном такое положение вещей связано с практической невозможностью переподготовки преподавателей высшей школы в условиях, изменяющихся столь стремительно. Расширение информационного поля, появление новых способов защиты информации, новых информационных потоков – все это предполагает мобильность учебного процесса, его постоянное изменение и совершенствование. Но для подобных изменений, для организации мобильного учебного процесса, соответствующего реальной действительности в каждый момент времени, нет ни материально-технической, ни даже мотивационной базы, и переподготовка специалистов-преподавателей не осуществляется. Оснащенность лабораторий для занятий такова, что по большей части ознакомление студентов с современными техническими средствами защиты информации можно осуществлять лишь в теории, не переходят к практике.

Российские специалисты в области информационной защиты обращают особое внимание на недостаточность учебников – учебные пособия также отстают от действительности. Они предлагают решать данный вопрос на государственном уровне, создавая на государственные деньги в университетах творческие коллективы, которые могли бы заниматься разработкой новых учебников.

Кроме того, практически нет связи между высшей школой и потенциальными работодателями будущих специалистов в области информационной защиты, а именно такая связь может обеспечить необходимую мобильность учебного процесса и стимулирование инновационного мышления как преподавателей, так и студентов. Но в настоящее время положение вещей таково, что преподаватели неуклонно отстают от изменяющихся условий, соответственно, при этом падает уровень преподавания и подготовки специалистов.

ТРЕБОВАНИЯ К АБИТУРИЕНТАМ ПО СПЕЦИАЛЬНОСТЯМ, СВЯЗАННЫМ С ЗАЩИТОЙ ИНФОРМАЦИИ

В.Б. Соколов

Абитуриенты, поступающие на специальности, связанные с информационной защитой, должны обладать рядом качеств, причем, психологический портрет абитуриента оказывается так же важен, как и его знания. В какой-то степени даже более важен, ведь, к примеру, математике можно обучить, но обучить патриотизму, преданности, стремлению к инновационным знаниям практически невозможно – в высшую школу приходят уже сформировавшиеся личности, и возможна лишь некоторая корректировка, но не полная смена характера и убеждений, вложенных в человека с раннего детства. Более того, зачастую на специальностях, связанных с защитой информации, оказываются студенты, заинтересованные не столько в получении знаний, сколько в престижном дипломе, пусть даже не подкрепленном необходимыми знаниями, что делает их специалистами крайне низкого уровня. Именно поэтому так необходимо, чтобы еще на стадии поступления в высшую школу производился отбор по психологическим критериям – с помощью специальных тестов. Также необходимо постоянное сопровождение студентов психологами при обучении в высшей школе.

Кроме того, необходимо ужесточить требования к довузовской подготовке абитуриентов, поступающих на специальности, связанные с информационной защитой. В настоящее время этот уровень катастрофически низок. К сожалению, повышение уровня довузовской подготовки напрямую связано с реорганизацией средней школы, но по крайней мере еще на стадии поступления в высшую школу можно выявлять тех абитуриентов, которые способны нагнать упущенное, а также тех, кто не в состоянии пройти подготовку в высшей школе на должном уровне.

Если подобные меры не будут приняты, то мы рискуем в ближайшем будущем оказаться без специалистов в области информационной защиты высокого качества.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ БЫСТРОГО ПРОТОТИПИРОВАНИЯ РАДИОЭЛЕКТРОННЫХ УСТРОЙСТВ

В.А. Столер, А.Е. Олежко

На сегодняшний день для быстрого прототипирования различных изделий радиоэлектронного назначения, в том числе и экранов ЭМИ, все чаще используется трехмерная печать. Вместе с тем устройства для трехмерной печати имеют недостатки различного характера, которые в итоге отражаются на качестве изготавливаемых изделий в виде нарушений их геометрических и физических параметров.

Опыт использования 3D принтера CubeX как устройства для быстрого прототипирования показал, что важное значение при изготовлении прототипов имеет хорошее программное обеспечение с широким диапазоном варьирования режимами трехмерной печати. Промежуточным решением стало использование слайсера Kisslicer 1.6.2, который содержал больше настроек, чем фирменное программное обеспечение CubeX. Качество печати при использовании данного слайсера вместе с тем не всегда было приемлемым. В то же время это дало возможность применять принтер без дорогих фирменных картриджей [1].

После испытаний принтера со слайсером Kisslicer 1.6.2 было принято решение применить более современное программное обеспечение в виде нового слайсера Cura версии 4.0.0, что повлекло за собой замену электронной части принтера с переходом с 8-ми битной логики на 32-х битную, а также замену драйверов шаговых двигателей. Новое программное обеспечение содержит настройки печати, прямо и косвенно влияющие на ее качество, среди которых: количество и толщина стенок, шаблоны и процент заполнения модели, варианты прилипания к рабочей поверхности, управление температурой сопла экструдера, изменение скорости при печати разных частей изделия. Кроме того пользовательский интерфейс программы имеет удобную опцию предварительного просмотра процесса печати и управления принтером с компьютера, к которому он подключен.

В результате предпринятых мероприятий по совершенствованию программного обеспечения устройств для быстрого прототипирования появилась возможность получать

качественные изделия с почти идеальной геометрией со значительным уменьшением времени их изготовления.

Список литературы

1. Столер В.А. Расширение функциональных возможностей 3D-принтеров // Тез. докл. XVI Белорусско-российской научн.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 89–90.

БЕЗОПАСНОСТЬ И НАДЕЖНАЯ СРЕДА В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ

Х.Х. Судани, М.Б. Абросимов

В соответствии со стандартами IEEE надежность рассматривается как способность системы или одного из ее элементов выполнять требуемые функции в заданных условиях в течение определенного периода времени.Технологический выход (результат производственного процесса определяется как часть или процент удовлетворяющих техническим требованиям комплектующих из всего количества изготовленных [1]. Происходящий или уже имеющийся сбой системы отражает тот факт, что сервис, предоставляемый системой, отличается от нормативного или предложенного. Другими словами, система не выполняет ожидаемых от нее действий. Надежность системы – ключевое требование к отказоустойчивой системе, тогда как безопасность обеспечивается посредством модернизации межсетевой защиты и обнаружения вторжений. В терминологии безопасности термин «уязвимость» вследствие ошибок программного обеспечения или неправильных настроек сопоставим с термином «ошибки (неисправности) в отказоустойчивости». При несвоевременном обнаружении и исправлении ошибок может произойти сбой, показывающий неспособность оказания соответствующей системной услуги. Отказоустойчивость – это способность системы восстанавливаться после произошедшего сбоя или возникшей ошибки без демонстрации самого сбоя. Сбой в системе не обязательно приводит к ошибке; он может оставаться в месте его возникновения, что не приводит к ошибке. Для вызова ошибки сбой должен быть активизирован определенным состоянием системы и условиями ввода. Методы, связанные с отказоустойчивыми системами, включают в себя предотвращение сбоя, его маскирование, обнаружение ошибочной или скомпрометированной системной операции, сдерживание распространения ошибок и восстановление нормальной работы системы [2]. Отказоустойчивость, направленная на предотвращение неисправностей, осуществляется посредством обнаружения ошибок и восстановления системы. При этом отказоустойчивая система может продолжать работать в нормальном режиме.

Список литературы

1. Bushnel M.L., Agrawal W.D. Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits. Boston, MA: Springer, 2005.

2. Heidergott W. SEU tolerant device, circuit and processor design // Proc. of the 42nd Design Automation Conference (DAC). 13–17 June 2005. P. 5–10.

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТИ ОШИБОЧНОЙ РЕГИСТРАЦИИ СИМВОЛОВ «0» В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ С ПРИЕМНЫМ МОДУЛЕМ НА ОСНОВЕ СЧЕТЧИКА ФОТОНОВ

А.М. Тимофеев, И.Г. Веремейчик, В.А. Касько, И.А. Ковалев

При регистрации данных в квантово-криптографических каналах связи весьма важно обеспечивать высокую надежность приемного оборудования легитимных пользователей [1, 2]. Для этого необходимо при построении таких каналов связи использовать в качестве приемных модулей счетчики фотонов, которые являются наиболее высокочувствительными [3]. Одним

из критериев оценки надежности квантово-криптографических каналов связи является вероятность ошибочной регистрации данных [1, 3]. Поскольку до настоящего времени исследование влияния такого параметра счетчика фотонов, как мертвое время, на вероятность ошибочной регистрации данных применительно к квантово-криптографическому каналу связи не выполнялось, это являлось целью данной работы. Объектом исследования являлся асинхронный двоичный несимметричный однородный волоконно-оптический канал связи без памяти и со стиранием. Предметом исследования являлось установить влияние средней скорости счета импульсов при передаче двоичных символов «0» на выходе счетчика фотонов n_{s0} на вероятность ошибочной регистрации этих символов $P_{ош0}$. Определено, что с увеличением средней скорости счета сигнальных импульсов на выходе счетчика фотонов зависимости $P_{ош0}(n_{s0})$ вначале уменьшаются, достигая наименьшего значения, после чего растут. Это имеет место как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Установлено, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа τ_d при прочих равных параметрах приводит к росту вероятностей ошибочной регистрации символов «0». Однако в диапазонах n_{s0}, на которых зависимости $P_{ош0}(n_{s0})$ растут, увеличение τ_d, напротив, приводит к уменьшению $P_{ош0}$.

Список литературы

1. Щеглов А.Ю. Анализ и проектирование защиты информационных систем. СПб., Профессиональная литература, 2017. 415 с.

2. Румянцев К.Е. Повышение эффективности алгоритма вхождения в синхронизм системы квантового распределения ключей // Известия ЮФУ. 2015. № 8 (169). С. 6–18.

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

ОЦЕНКА ПОТЕРЬ ИНФОРМАЦИИ ОДНОФОТОННОГО КАНАЛА СВЯЗИ С ПРИЕМНЫМ МОДУЛЕМ НА ОСНОВЕ СЧЕТЧИКА ФОТОНОВ

А.М. Тимофеев, И.Г. Веремейчик, В.А. Касько, И.А. Ковалев

Одной из наиболее важных задач, решаемых при передаче двоичных данных по волоконно-оптическим каналам связи, является обеспечение скрытности и конфиденциальности передаваемой информации [1]. Для решения этой задачи применяют, как правило, комплекс мер, включая организацию квантово-криптографических каналов связи. Такие каналы характеризуются наиболее высоким уровнем информационной безопасности, что достигается за счет применения маломощных оптических сигналов и, соответственно, высокочувствительных приемных модулей – счетчиков фотонов [1, 2]. При этом весьма важно, чтобы приемное оборудование легитимных пользователей обеспечивало наименьшие потери передаваемой информации. Отметим, что потери информации в указанных каналах связи обусловлены наличием мертвого времени счетчиков фотонов – времени, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению. Поскольку до настоящего времени оценка влияния мертвого времени счетчиков фотонов на потери информации, передаваемой по квантово-криптографическим каналам связи, не выполнялась, это являлось целью данной работы. Применительно к квантово-криптографическим каналам связи получены выражения для оценки вероятностей ошибочной регистрации двоичных символов («0» и «1») и условной энтропии, которые учитывают среднюю длительность продлевающегося мертвого времени счетчика фотонов. По результатам выполненных исследований установлено, что с увеличением средней длительности мертвого времени продлевающегося типа наименьшие потери передаваемой информации наблюдаются при более высоких средних скоростях счета сигнальных импульсов на выходе счетчика фотонов как при регистрации символов «0», так и при регистрации символов «1».

Список литературы

1. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]. Минск: Белорус. наука, 2007. 391 с.

2. Тимофеев А.М. Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи // Приборы и методы измерений. 2018. Т. 9, № 1. С. 17–27.

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ НА ИНТЕГРАЛЬНЫЕ МИКРОСХЕМЫ

Н.А. Титович, В.Н. Теслюк, В.А. Тарасенко

При исследовании влияния электромагнитных помех (ЭМП) на интегральные микросхемы (ИМС), блоки и устройства радиоаппаратуры целесообразно проводить испытания с использованием ТЕМ-камеры. При этом перед экспериментом проводится предварительное расчетное моделирование влияния ЭМП на ИМС и устройства. Это позволяет значительно сократить затраты времени и средств. Используя для расчетов библиотеку ранее разработанных простых моделей, можно прибегать к проведению эксперимента только на стадии испытаний законченного изделия.

Анализ известных подходов к моделированию воздействия ЭМП на работоспособность ИМС показывает, что при расчете удобнее разбивать модель на составные части: ядро, корпус, цепи питания и входные/выходные цепи. На основе более простых моделей была создана методика для расчетной оценки восприимчивости ИМС к ЭМП. При расчетах удобно использовать фрагменты моделей электромагнитного излучения (ICEM) той же микросхемы. В основе этого довода лежит принцип взаимности, который применительно к ИМС заключается в том, что наибольшая восприимчивость микросхем к воздействию ЭМП наблюдается на частотах с максимальными уровнями паразитных излучений. Для описания входных/выходных цепей используются IBIS модели. Для контроля сбоев необходима функциональная модель, а также некоторый критерий сбоя, который зависит от конкретного приложения. Таким образом, нет необходимости в подробных данных о внутренней структуре микросхемы, что позволяет рассматривать ее как черный ящик.

По описанной выше методике проведен расчет восприимчивости микросхемы КР1533ЛА3 к воздействию ЭМП. Выделена модель входных/выходных цепей, построенная на основе IBIS модели, модель цепи питания, построенная по описанным в стандартах методикам, функциональная модель, которая представляет собой таблицу истинности и модель испытательной установки, которая построена согласно условиям эксперимента. При проведении расчетов было замечено, что подтверждаются общие тенденции, выявленные при различных исследованиях: устойчивость к помехам увеличивается с ростом частоты ЭМП. В целом расчетные данные для ИМС КР1533ЛА3 хорошо согласуются с данными проведенных ранее экспериментов.

GENERAL DATA PROTECTION REGULATION И ПРОЕКТ ЗАКОНА РЕСПУБЛИКИ БЕЛАРУСЬ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

К.И. Тишук, А.М. Прудник

General Data Protection Regulation [1] уже вступил в действие с 25 мая 2018 г., а в нашей стране в настоящее время рассматривается закон Республики Беларусь «О персональных данных» [2]. Согласно GDPR, персональными данными (ПД) является любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. В свою очередь, идентифицируемое физическое лицо определено как лицо, которое может быть идентифицировано прямо или косвенно с использованием идентификатора, например: имени, идентификационного номера, данных о его местоположении, онлайн-идентификатора, или использованием параметров, характеризующих лицо с физиологической, генетической, психологической, экономической, культурной или социальной точек зрения. Под обработкой ПД понимается любая операция или набор операций, выполняемых с ПД или набором ПД

как с использованием средств автоматизации, так без них, включая сбор, запись, структурирование, хранение, адаптацию или изменение, использование, распространение, ограничение, уничтожение, группировка или комбинирование, поиск и выборка, экспертиза.

Согласно проекта закона, ПД это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано на основании такой информации. В то время, как субъект персональных данных определен как физическое лицо, в отношении которого осуществляется сбор, обработка, распространение, предоставление персональных данных.

GDPR применяется к физическим и юридическим лицам, государственным органам, а также международным организациям, в то время как проект закона распространяется на государственные органы, физические и юридические лица, а также иные организации осуществляющие действия с ПД.

Согласно GDPR, субъекты отношений имеют следующие права: на возражение, быть забытым, на доступ, на ограничение обработки, не подвергаться автоматизированному принятию решений, подавать жалобу в надзорный орган, на эффективную защиту против решения надзорного органа и на т.н. портативность данных. В соответствии с проектом закона, субъекты имеют права соглашаться на сбор, обработку (за исключением обезличивания); распространение; отзывать согласие на сбор, обработку (за исключением обезличивания), распространение, предоставление; ознакомление со своими ПД; получать информацию о предоставлении своих ПД третьим лицам; требовать прекращения сбора, обработки (за исключением обезличивания), распространения, предоставления ПД.

GDPR кодифицировал ряд новых понятий. Например, псевдонимизация, т. е. требование раздельного хранения информации, которая позволяет сличить человека и его данные, которые к нему относятся, требуется отдельно. Также субъект наделены новыми правами, например, правом быть забытым, когда по запросу пользователя, его ПД, включая резервные копии, удаляются или право на запрет автоматизированных решений. Утечка ПД, при которой необходимо уведомить надзорный орган и пользователей не позднее 72 ч с момента ее выявления.

Установлены санкции за несоблюдение требований GDPR, которые могут быть применены в отношении юридических лиц как в ЕС, так и вне его. Могут быть наложены санкции от € 10 млн € 20 млн, либо от 2 до 4 % годового оборота.

Список литературы

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Проект Закона Республики Беларусь «О персональных данных»: принят Палатой представителей Национального собрания Республики Беларусь и одобренный Советом Республики.

МАТРИЦА БЕЗОПАСНОСТИ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

А.В. Федорцов

В настоящее время основу создаваемых в Республике Беларусь систем защиты информации, обрабатываемой в информационных сетях (ИС) различных организаций и распространение/предоставление которой ограничено, составляют программно-технические средства защиты информации (ПТСЗИ), получившие сертификат соответствия требованиям информационной безопасности технического регламента ТР 2013/027/BY [1].

По сути, единицу ПТСЗИ относительно указанного регламента следует рассматривать как оконечное программно-техническое средство, содержащее в своем составе реализующие функции защиты информации элементы, в которых программные и технические части полностью взаимозависимы и неразделимы. В свою очередь несколько ПТСЗИ – как функционально выделенную по предназначению совокупность взаимосвязанных физических компонентов, а точнее, критически важную подсистему обработки информации в ИС.

Исходя из потребностей организаций номенклатура ПТСЗИ, используемых в ИС, может включать: средства криптографической защиты информации; средства идентификации и аутентификации пользователей; средства управления доступом и т.д. Ввиду этого матрица безопасности ПТСЗИ каждой конкретной организации будет представлять собой соответственно таблицу, отображающую выполняемые функции, критические параметры и характеристики, правила и условия безопасной эксплуатации (использования), количество единиц используемых средств защиты информации определенного наименования.

Построение такой матрицы необходимо для последующей формализации связей между целями/объектами/условиями нерегламентированного воздействия и соответствующим ущербом ИС организации при решении задачи количественной оценки негативных последствий от атак на ПТСЗИ [2].

Список литературы

1. ТР 2013/027/BY. Информационные технологии. Средства защиты информации. Информационная безопасность.

2. Федорцов А.В. Последствия инсайдерских атак на программно-технические средства защиты информации в контексте оценки рисков для информационной сети // Наука и воен. безопасность. 2018. № 4 (58). С. 25–30.

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ XSS АТАК

Н.В. Харитонов, М.П. Хоронеко, М.А. Медунецкий, В.В. Шиманский

Сегодня мир веб-разработки развивается с огромной скоростью. Наблюдается тенденция перехода от десктопных приложений в сторону веба. Возможности веб-приложений впечатляют, ведь они позволяют связаться с людьми из разных стран; поиграть в игры; посмотреть новости; заказать билеты и т. д. за несколько минут и на любом устройстве, будь то ПК, смартфон или умные часы. Но наряду с данными функциями образуется ряд проблем, одной из которых является проблема защиты информации и безопасности. В данной публикации рассматриваются XSS атаки, являющиеся наиболее распространенными.

XSS атаки заставляют пользователя выполнять нежелаемые задачи на веб-сайтах (например, отправлять письма, деньги, секретные токены для авторизации на сайте), причем пользователь даже не подозревает об этом.

Сущность XSS (cross site scripting) атаки заключается во внедрении вредоносного кода в возвращаемую сервером веб-страницу, который при последующем открытии страницы будет выполнен в браузере пользователя. Такой код может быть внедрен в страницу, например, при отправке вместо привычного нам комментария, комментария вида:

```
<script>
  var img = document.createElement("img");
  img.setAttribute('src', 'http://hackers.site/?token=' + localStorage.getItem('token'));
  document.body.appendChild(img);
</script>
```
(1)

если при отображении страницы такой комментарий добавляется в html, то злоумышленники получат секретный токен приложения в качестве параметра запроса и смогут работать от имени приложения. Для защиты от такого вида атак следует фильтровать пользовательский ввод, то есть заменять все спецсимволы на escape-последовательности(например, < на &lt, & на &amp) прежде чем вставить такой комментарий в html. Современные фронтенд фреймфорки (React.js, Angular, Vue.js и т.д.) имеют встроенную защиту от XSS атак, ни один из них не позволит просто вставить код вида (1) в веб-страницу. Однако у каждого из них все же остается довольно много уязвимостей, которые позволяют обойти фильтры сайта и внедрить вредоносный код.

Таким образом, XSS атаки являются инструментом для хищения данных из cookies, sessionStorage, localStorage и т. д. Разработчики веб-сайтов не должны пренебрегать созданием защиты от атак данного типа, дабы не ставить своих пользователей под угрозу.

Список литературы

1. Shema M. Seven Deadliest Web Application Attacks (Syngrass Seven Deadlest Attacks).– Syngress Publishing, Inc. Elsevier, Inc. 30 Corporate Drive Burlington, 2010.

2. XSS Attacks – Cross Site Scripting Exploits and Defense / S. Fogie [et al.]. Syngress Publishing, Inc. Elsevier, Inc. 30 Corporate Drive Burlington, 2011. 28 p.

ГИБКИЕ МНОГОСЛОЙНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛЯ СНИЖЕНИЯ УРОВНЯ ПОМЕХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

У.М. Харма, Н.Н. Гринчик

Разработана и апробирована методика изготовления гибких многослойных электромагнитных экранов, характеризующихся значениями коэффициента передачи электромагнитного излучения в диапазоне частот 0,7…17 ГГц, изменяющимися в пределах от –30 до –40 дБ и значениями коэффициента отражения электромагнитного излучения, изменяющимися в пределах от –5 до –15 дБ. Эти экраны состоят из пяти слоев. Их первый, третий и пятый слои (относительно фронта распространения электромагнитных волн) выполнены на основе влагосодержащей плотной целлюлозы. Влагосодержание каждого следующего из указанных слоев превышает влагосодержание предыдущего. Второй и четвертый слои электромагнитных экранов, изготовленных в соответствии с предложенной методикой, выполнены на основе углеродосодержащего материала. Такие экраны могут быть использованы для изготовления изделий, предназначенных для снижения уровня побочного электромагнитного излучения средств вычислительной техники.

LDPC-КОДЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Хмелевский

Корректирующие коды получили широкое применение в задачах защиты информации. В настоящее время такие коды представлены в многочисленных технических приложениях, например, в стандартах CCSDS 101.O-B (Consultative Committee for Space Data Systems), ITU-T G.975.1 (International Telecommunication Union) и IEEE 802.16 (The Institute of Electrical and Electronics Engineers).

Одними из таких кодов являются коды с малой плотностью проверок на четность (LDPC-коды).

Целью исследования является разработка новой методики комплексной оценки помехоустойчивых кодов, применяемой на предварительном этапе построения систем, реализующих защиту информации в высокоскоростных каналах передачи данных.

В работе были получены следующие результаты.

1. Разработана новая, научно обоснованная методика комплексной оценки помехоустойчивых кодов, которая может применяться на начальном этапе разработки систем помехоустойчивого кодирования, позволяющих с заданной достоверностью гарантировать защищенность целостности данных от разрушающих воздействий в высокоскоростных каналах передачи данных, реализуя механизмы защиты информационных символов. Отличительной особенностью данной методики является то, что она оперирует комплексным набором показателей для оценки кода, учитывает различные аспекты использования данного типа кодов и предназначена для оценки возможности и способов построения систем декодирования с применением рассматриваемого типа кодов. Методика приведена на примере LDPC-кода.

2. Выявлена взаимосвязь алгоритмов декодирования LDPC-кода, которая позволяет раскрыть иерархическую вложенность данных алгоритмов и сделать вывод о том, какой алгоритм является наиболее релевантным для определенной системы передачи данных с заданными параметрами.

Список литературы

1. Gallager R.G. Low Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.
2. Jian-Bing H.A.N., Chen H.E., He Yun H.E. Research on regular LDPC codes with better performance than turbo codes // Materials of International Conference on Information Engineering ICIE '09.

ИНВАРИАНТНОСТЬ ЦИФРОВОГО ОТПЕЧАТКА УСТРОЙСТВА ПОЛЬЗОВАТЕЛЯ, ИСПОЛЬЗУЕМОГО ДЛЯ ЕГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

О.А. Хожевец, Т.В. Борботько

Идентификация пользователя информационных ресурсов предполагает использование некоторой уникальной информации, которая известна непосредственно пользователю, а также хранится в информационной системе для выполнения процедуры его аутентификации. В качестве такой информации выступает, как правило, некоторые сведения (логин, пароль и т.д.) вводимые пользователем для проверки его подлинности.

Учитывая особенности программных средств, применяемых пользователями сети интернет для доступа к информационным ресурсам, можно выделить следующие признаки таких средств, позволяющих выполнить процедуру идентификации его устройства: javascript, user agent, IP, flash, ActiveX, содержание кэша браузера, cookie, supercookie, настройки используемого программного обеспечения. Формирование из вышеперечисленных признаков массива данных и вычисление его хэш суммы позволяет получить цифровой отпечаток (фингерпринт) устройства пользователя, который будет неизменным в течение достаточно длительного времени.

Необходимо отметить, что во всех существующих браузерах есть широкий спектр переменных с большой инвариантностью, которые позволяют, даже не подготовленному пользователю, изменять цифровой отпечаток своего устройства перед подключением к информационному ресурсу. Наиболее простыми способами, являются: использование нового браузера или новой версии, изменение масштаба окна браузера, изменение часового пояса устройства, изменение языка браузера. Экспериментально установлено, что варьируя значениями указанных переменных можно получить от 1000 до 230000 уникальных цифровых отпечатков устройства, в зависимости от используемого браузера. Таким образом, для снижения ошибок первого и второго рода необходимо формировать базу цифровых отпечатков устройства пользователя, которая, в дальнейшем, может быть использована для его идентификации.

БЕЗОПАСНОСТЬ REACT-ПРИЛОЖЕНИЙ

М.П. Хоронеко, Н.В. Харитонов, М.А. Медунецкий, В.Я. Анисимов

ReactJS – самая популярная JavaScript библиотека для построения пользовательских интерфейсов по данным Google Trends на 2019 год [1]. Приложения на ее основе используют большое количество js-кода, поэтому справедливо предположить что атаки типа XSS могут принести злоумышленникам определенный результат.

Практика использования ReactJS в мире показывает, что библиотека содержит большое число компонентов поддержания безопасности приложения. Например, спецсимволы, без которых невозможно осуществить XSS атаку, автоматически заменяются управляющей последовательностью при их использовании в строчных значениях в JSX (синтаксис, подобный HTML, в основе которого лежат теги, позволяющий использовать JS-код непосредственно при построении разметки) [2]. Тем не менее, проблемы, связанные с внедрением скриптов, могут быть результатом использования неподходящих практик программирования и не всегда являются очевидными. Среди них:

– создание React-компонентов из объектов, поставляемых пользователем;
– отображение ссылок с href-атрибутом, определяемым пользователем;
– явное задание свойства dangerouslySetInnerHTML у элемента;

– передача пользовательской строки в функцию eval();
– неправильная реализация серверной отрисовки (SSR).

Несмотря на то, что ReactJS сама по себе является довольно продвинутой с точки зрения защиты от внедрения скриптов библиотекой, основная ответственность по обеспечению безопасности приложения ложится на команду разработки. Только внимательность, осведомленность и использование верных подходов, а также тщательное и регулярное тестирование безопасности продукта может гарантировать его надежность.

Список литературы

1. Thomas M. React in Action. Manning Inc., 2018. 5 p.
2. Geary D. Building React.js Applications with Redux. Syngress Publishing, 2018. 29 p.

ВЛИЯНИЕ ИСКАЖЕНИЙ ИЗОБРАЖЕНИЯ НА РЕШЕНИЕ ЗАДАЧИ РАСПОЗНАВАНИЯ

Н.В. Царенков, А.В. Сергеенко, А.Ю. Липлянин

На сегодняшний день обработка изображений является неотъемлемой частью нашей повседневной жизни. Она используется в системах охраны государственных границ и общественного порядка, медицинской техники, системах контроля за лесными ресурсами и др. К задачам обработки изображений относятся распознавание образов и объектов, восстановление изображений, фильтрация, оценка параметров изображения, сжатие изображений. Одним из наиболее активно развивающихся, но при этом наиболее трудоемких и сложных с научной точки зрения направлений является распознавание объектов. Для решения данной задачи широкое распространение получили оптоэлектронные системы распознавания.

В реальных оптоэлектронных системах изображения непременно подвергаются воздействию дестабилизирующих факторов. Такими факторами выступают [1]: помехи сенсора, движения наблюдаемого объекта, погодные условия, оптические дефекты объективов и т.д. Например, воздействие природных явлений, таких как турбулентность атмосферы, погодные условия, а также перемещение объекта наблюдения негативно сказываются на качестве изображений (вызывая расфокусировку, помехи и смазывание), и, как следствие, снижают эффективность работы системы распознавания (не зависимо от метода распознавания). Снижение эффективности работы системы распознавания влечет за собой снижение качества работы всей системы охраны в целом.

Для компенсации воздействия мешающих факторов применяется предварительное восстановление изображения. Для предварительного восстановления изображения могут использоваться различные методы, основанные на пространственной и частотной фильтрации и др [2]. Использование данных методов позволяет улучшить качество изображения, при чем критерий качество выбирается исходя из целевой функции оптической системы. Улучшения качества изображения влечет улучшение эффективности работы системы распознавания. Исходя из вышесказанного, можно сделать вывод, что внедрения этапа восстановления изображений в системы распознавания, а также совершенствование существующих методов и алгоритмов восстановления изображений, применяемых в данных системах, является сложной и важной задачей. Выполнение которой влечет за собой увеличение эффективности работы различных систем в состав которых входят системы распознавания, например, системы охраны общественного порядка.

Список литературы

1. Бейтс Р., Мак-Доннелл М. Восстановление и реконструкция изображений. М.: Мир, 1989. 336 с.
2. Анализ методов восстановления оптико-электронных изображений, смазанных при движении / А.Ю. Липлянин [и др.] // Доклады БГУИР. 2018. № 2. С. 40–46.

ФОТОЭЛЕКТРИЧЕСКИЕ СВОЙСТВА ПОВЕРХНОСТНО-БАРЬЕРНЫХ СТРУКТУР

Чан Бинь Тхан

В работе представлены результаты исследования поверхностно барьерных структур на основе монокристаллов In/ $(MnIn_2S_4)_{0,5}\cdot(AgIn_5S_8)_{0,5}$.

Для создания фоточувствительных структур из выращенных монокристаллов вырезали плоскопараллельные пластинки перпендикулярно оси роста кристаллов, которые механически шлифовали и полировали, а затем подвергали обработке в травителе состава Br_2:C_2H_5OH = 1:3. Средние размеры пластин после такой обработки составляли 1,0 × 5,0 × 5,0 мм. Структуры получали вакуумным термическим напылением металлического индия (толщина слоя ~ 1 мкм) на поверхность кристаллов, находившихся при комнатной температуре и не подвергавшихся какому-либо нагреву при напылении слоев, что позволяло не принимать в учет возможность образования на границе слоя с подложкой других фаз. Омический контакт создавался нанесением серебряной пасты.

Проведенные исследования сформированных структур In/ $(MnIn_2S_4)_{0,5}\cdot(AgIn_5S_8)_{0,5}$ показали, что при освещении их интегральным светом лампы накаливания воспроизводимо проявляется фотовольтаический эффект, знак которого согласуется с направлением выпрямления, а изменения в локализации светового зонда на фотоприемной поверхности таких структур, энергии падающих фотонов и интенсивности освещения не влияют на знак фотонапряжения. Эти результаты служат основанием для того, чтобы наблюдаемый фотовольтаический эффект приписать возникновению энергетического барьера на контакте металла с монокристаллами $(MnIn_2S_4)_{0,5}\cdot(AgIn_5S_8)_{0,5}$. Вольтовая фоточувствительность (S_U) поверхностно-барьерных структур преобладает при их освещении со стороны барьерной пленки.

Исследование вольт-амперных характеристик созданных структур показали, что они обладают выпрямлением, которое характеризуется отношением прямого тока к обратному $K \approx 5$ при напряжениях смещения $|U| \approx 10$ В, причем пропускное направление всегда реализуется при отрицательной полярности.

Фоточувствительность лучших структур достигает $U \approx 120$ В/Вт, причем знак фотонапряжения не зависит от энергии фотонов и места падения светового зонда на поверхность структур. Это обстоятельство позволяет считать, что полученные спектры относительной квантовой эффективности $\eta(\hbar\omega)$ определяются свойствами барьеров индия с поверхностями In/ $(MnIn_2S_4)_{0,5}(AgIn_5S_8)_{0,5}$.

КЛАССИФИКАЦИЯ ДАННЫХ, ЦИРКУЛИРУЮЩИХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЮРИДИЧЕСКИХ КОМПАНИЙ

Г.Д. Чурчага, А.А. Протасова, А.Р. Панфилович

Основополагающим этапом построения системы защиты информации организации является классификация данных, циркулирующих в ее информационных системах и сетях. В представляемой работе проанализированы данные, используемые сотрудниками юридических компаний для осуществления своей деятельности. Установлено, что в зависимости от содержания эти данные могут быть условно разделены на два класса. Данные первого класса – это правовая информация. Эти данные могут относиться как к категории общедоступной информации (нормативные и правовые акты, материалы учета, упорядочения, толкования и реализации правовых норм, материалы о правовом образовании), так и к категории информации, распространение которой ограничено (материалы подготовки законопроектов, сведения о разработке научных концепций развития права). Данные второго класса – информация, являющаяся объектом правоотношений (как правило, сведения, составляющие профессиональную или коммерческую тайну, т. е. относящиеся к категории информации, распространение которой ограничено).

На основе проведенного анализа установлено, что в информационные системы, используемые сотрудниками юридических организаций, относятся к классу 3-фл, 3-дсп, 4-фл

и/или 4-дсп. Система защита информации и особенности мероприятий, связанных с проведением аудита информационной безопасности в таких организациях будут зависеть от класса используемых информационных систем.

ИССЛЕДОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ

А.С. Шабуня

Программное обеспечение – это программа или какой-либо набор программ, который используется для управления и настройки устройств на которые они устанавливаются. Мобильный телефон, персональный компьютер, ноутбук, нетбук, коммуникатор и смартфон – это сложные аппаратно-программные комплексы, где корректное функционирование зависит от правильной работы как аппаратной, так и программной части. В настоящий момент больше времени и усилий выделяется на программное обеспечение для мобильных телефонов, после уже для персональных компьютеров и ноутбуков. Также следует учесть, что изготовитель не может предугадать, как будет использоваться тот или иной продукт, так же и то, в каких условиях будет использоваться устройство. Сегодня, большинство сбоев в работе технических средств, имеющих программную составляющую, связано с использованием неадаптированного под конкретное техническое средство программного контента (музыкальные и видео плееры, игровые приложения, приложения для работы). В большем это связано именно с тем, что на рынке преобладает довольно большое количество технических средств и адаптировать конкретную программную составляющую под каждое техническое устройство представляет собой довольно больших затрат и усилий. С технической точки зрения ремонт – это восстановление работоспособности устройства. Если при диагностике дефект устройства связан именно с программным обеспечением, то производится замена программного обеспечения. Чаще всего это идет перерошивка устройства либо же обновление программного обеспечения до актуальной версии. Если после данной процедуры техническое средство с программной составляющей перешло в работоспособное состояние (отмеченный дефект отсутствует) – это является ремонтом. Однако, в большом наборе программного обеспечения разрешено как редактирование, так и изменение каких-либо настроек и функций для конечного пользователя, что выявляется в сервисных центрах при диагностике. Если в программную часть вносились изменения конечным пользователем, то сервисными центрами и организациями дефект устройства, связанный с программным обеспечением не подтверждается, а для тестирования производиться смена (замена) программного обеспечения. В таких случаях устанавливается заводское программное обеспечение для устройства, что позволяет исключить какие-либо личные настройки и параметры конечного пользователя. Поэтому при возврате технического средства с программной составляющей (например, маршрутизатора) с заключением «Замена программного обеспечения» не стоит воспринимать его как устройство бывшее в ремонте, либо же отремонтированное.

Список литературы

1. Хлебников А.А. Информационные технологии. Москва: КноРус, 2015. 466 с

МЕТОДЫ СОЗДАНИЯ Al-Al_2O_3-ОСНОВАНИЙ С ТОЛСТОСЛОЙНОЙ МЕДНОЙ МЕТАЛЛИЗАЦИЕЙ ДЛЯ МИКРОПОЛОСКОВЫХ СВЧ-ЭЛЕМЕНТОВ

Д.Л. Шиманович

Использование механически прочных Al-оснований с диэлектрическим слоем Al_2O_3, полученным в результате электрохимического процесса одностороннего анодирования, является весьма перспективным, если учесть тот фактор, что вторая неокисленная сторона таких оснований служит сплошным металлизированным экраном. Толщина диэлектрического слоя и его структурно-морфологические параметры, которые влияют на величину затухания СВЧ-сигналов, могут контролироваться электрохимическими режимами анодирования [1].

Были разработаны технологические режимы формирования Al-Al_2O_3-Ni-Cu-структур, основанные на химическом осаждении Ni толщиной 1-1,5 мкм и электрохимическом осаждении Cu толщиной до 80 мкм на широкоформатные Al-основания толщиной 1,5–3,0 мм с односторонним модифицированным диэлектрическим слоем Al_2O_3 толщиной до 150 мкм, полученным в процессе электрохимического анодирования и прогрунтованным кремнийорганическим лаком. Разработанный нами технологический процесс формирования Al–Al_2O_3–Ni–Cu-структур позволил исключить операцию вакуумного напыления токопроводящих пленок в качестве подслоя с использованием дорогостоящего оборудования и основывался на использовании только химических, электрохимических и гальванических методов. Насущной проблематикой при таком подходе является улучшение электрофизических, теплофизических и механических параметров: увеличение электроизоляционной прочности анодного Al_2O_3, исключение возможных коммутационных соединений Cu-проводников с Al-основанием, снижение внутренних напряжений, улучшение термостойкости, теплопроводности и адгезионных свойств Cu в системе Al-Al_2O_3-Ni-Cu. При соблюдении оптимальных технологических режимов формирования пассивной части измеренные параметры показали следующие значения: напряжение пробоя изоляции ~ 3,5–6,0 кВ; теплопроводность ~ 41–71 Вт/м·К; термоустойчивость – до 300 ^oC; степень адгезии Cu ~7,0–8,7 кг/мм^2.

Таким образом, была показана перспективность использования полученных Al-Al_2O_3-оснований с элементами на основе толстослойной медной металлизацией в качестве микрополосковых линий пассивной части систем СВЧ-диапазона.

Список литературы

1. Шиманович Д.Л. Оптимизация методов формирования толстослойных диэлектрических покрытий на основе анодного оксида алюминия при электрохимическом анодировании широкоформатных Al-подложек и теплопроводящих оснований с радиаторами // Фундаментальные проблемы радиоэлектронного приборостроения. 2016. Т. 16, № 3. С. 116–119.

ФОРМИРОВАНИЕ АЛЮМООКСИДНЫХ СТРУКТУР СО ВСТРОЕННОЙ КОММУТАЦИОННОЙ МЕТАЛЛИЗАЦИЕЙ ДЛЯ ЭЛЕМЕНТОВ СВЧ-ДИАПАЗОНА

Д.Л. Шиманович

Повышение функциональной сложности СВЧ-устройств при одновременном увеличении требований к их электрофизическим параметрам, надежности и технологичности требуют новых подходов к выбору несущих оснований и токопроводящих коммутационных структур, выполняющих функцию микрополосковых СВЧ-линий. Анализ возможностей алюмооксидной технологии и проведенных исследований [1] показал, что, используя комбинированное сочетание процессов фоторезистивного маскирования, двухстороннего сквозного анодирования и химического травления исходных алюминиевых пластин, можно одновременно формировать несущие основания и системы алюминиевых межсоединений, встроенных внутри диэлектрического тела пластин из свободного анодного оксида алюминия с односторонним или двухсторонним выходом на поверхность контактных площадок, что может найти применение при создании пассивной элементной базы СВЧ-систем. Связанное с этим научное направление является весьма актуальным, если учесть, что исключается применение процессов вакуумного напыления или электрохимического осаждения металлических пленок, и можно варьировать толщиной встроенных коммутационных элементов и глубиной их залегания в объеме диэлектрика.

Сущность разработанной технологии изготовления сквозных Al_2O_3-пластин, которые выполняют роль несущих диэлектрических оснований и одновременно служат межэлементной диэлектрической средой для встроенной металлизации, заключается в следующем. Вначале на предварительно подготовленную и отполированную Al-пластину толщиной 150-200 мкм наносили в два этапа фоторезистивные маски проводников и контактных площадок по схеме разнотемпературного задубливания (соответственно T = 120 ^oC и T = 180 ^oC). Затем открытые места Al анодировали на необходимую толщину в 7 % щавелевой кислоте ($H_2C_2O_4$) в гальваностатическом режиме при плотности тока 25–35 мА/см^2. Далее, селективным

химическим травлением в растворе CrO_3:H_3PO_4:H_2O при температуре 85 °С удаляли выращенный Al_2O_3 с образованием микрорельефа. Затем осуществляли вторую стадию анодирования в том же электролите, снимали слабозадубленные фоторезистивные маски с мест формируемых встроенных проводников и проводили двухстороннее сквозное анодирование уже всей открытой поверхности оснований. Так как толщина Al в местах, соответствующих будущим зонам межэлементного разделения меньше, то они анодировались полностью до смыкания встречнорастущих Al_2O_3-слоев, а на других участках анодирование прекращалось с образованием встроенных внутри оксида проводников. Причем, какой величины был сделан уступ микрорельефа, такой же толщины формировались Al-проводники внутри Al_2O_3-пластин. Таким образом, получены встроеннные коммутационные элементы с толщиной Al от 5 до 100 мкм и различной глубиной их залегания в объеме Al_2O_3-пластин.

Список литературы

1. Сокол В.А., Шиманович Д.Л., Литвинович Г.В. Технологические приемы формирования Al–Al_2O_3 микроструктур для мощных электромеханических систем // Доклады БГУИР. 2012. № 8 (70). С. 44–49.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ВИРТУАЛЬНЫХ СРЕД

А.Н. Шляхтич, А.С. Шилов

На сегодняшний день виртуализация является одним из основных направлений развития информационных технологий. Это обусловлено тем, что путем применения указанной технологии можно значительно сократить затраты на создание информационных систем и сетей. Одной из основных задач, решаемых в ходе создания информационной системы или сети на основе технологии виртуализации (виртуальной среды) является разработка подходов по защите этих сред от угроз информационной безопасности. Один из таких подходов связан с выбором программного обеспечения для организации функционирования виртуальных сред.

Авторами проведен анализ уязвимостей программного обеспечения, используемого в настоящее время для организации функционирования виртуальных сред. На основе проведенного анализа определено, что наибольший уровень защищенности виртуальных сред может быть обеспечен в том случае, если для организации их функционирования применяется следующее программное обеспечение:

– платформа виртуализации VMware vSphere в составе гипервизора VMware ESXi и сервера управления VMware vCenter Server 5.1;

– платформа виртуализации и обеспечения безопасности сети VMware NSX версии 6.3;

– многофункциональное виртуальное устройство защиты информации FortiGate-VM под управлением программного обеспечения FortiOS v.5.6 для установки в среде виртуализации VMware.

Указанные программные продукты сертифицированы на территории Республики Беларусь.

РАСЧЕТ ЭКСПЛУАТАЦИОННОЙ ИНТЕНСИВНОСТИ ОТКАЗОВ ПЕЧАТНЫХ ПЛАТ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Н.С. Шматко

Надежность – одно из важнейших свойств изделий, в том числе электронных устройств, которое определяет их эксплуатационную пригодность. Особенно важно оценить эксплуатационную интенсивность отказов электронной аппаратуры в сфере защиты информации, так как преждевременный и незапланированный отказ средства защиты информации может привести к потере или утечке информации. Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования.

Для прогнозирования отказов аппаратуры защиты информации необходимо предварительно оценить ее надежность. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств, которые в большинстве случаев разработаны на основе печатных плат. В связи с этим необходимо определить методику для расчета надежности печатных плат обеспечивает получение более достоверных результатов. В работе рассмотрены подходы и методы определения эксплуатационной интенсивности отказов печатных плат, включенные в справочники или стандарты по расчету надежности электронного оборудования следующих стран: Россия, США, Франция. На основе анализа установлено, что в большей степени учет условий эксплуатации, конструкторско-технологических и других особенностей печатных плат обеспечивает модель расчета эксплуатационной надежности, включенная в справочник «RDF 2000 : Reliability Data Handbook. A universal model for reliability prediction of Electronics components, PCBs and equipment» [1]. Эта модель учитывает следующие важнейшие факторы: температуру окружающей среды, количество слоев печатной платы, количество отверстий для установки элементов, площадь печатной платы, количество токопроводящих дорожек, значение преобладающей ширины токопроводящих дорожек, возможные тепловые изменения при использовании печатной платы на объекте в составе аппаратуры.

Список литературы

1. 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.

ФИЛЬТРАЦИЯ HTTP-ТРАФИКА СИСТЕМ ВЕБ-АНАЛИТИКИ

Е.А. Юхо, Т.В. Борботько

Веб-аналитика (web-analytics) – система для измерения, сбора, анализа информации о посетителях веб-сайтов для улучшения и оптимизации работы ресурса. Главным назначением веб-аналитики является мониторинг посещений веб-страниц. На основе полученных данных изучается поведение пользователей сайта, принимаются решения о развитии и расширении возможностей ресурса.

Типовой алгоритм работы систем веб-аналитики:

– при загрузке страницы обрабатывается JS код;

– в браузер записываются, или считываются cookies;

– GIF хит отправляется на сервер системы веб-аналитики;

– данные обрабатываются на сервере и передаются в интерфейс системы в виде отчетов;

– доступ к полученным системой данным реализуется через API.

Чтобы изменить или скрыть данные от веб-аналитики, пользователю потребуется внести изменения в настройки своей операционной системы, браузера, или использовать средства фильтрации, такие как анонимайзер (веб-прокси) HideMe.nameVPN.

Для оценки эффективности известных способов защиты от сбора данных системами веб-аналитики проведен эксперимент, в ходе которого использовался тестовый стенд, выполненный на основе персонального компьютера с операционной системой Windows и браузером Firefox. В качестве средства оценки применяемых методов и средств защиты использовалась система веб-аналитики Яндекс Метрика. Показано, что достаточно использовать настройки указанного браузера для блокирования запросов Яндекс Метрики, дополнительных программных средств не требуется.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

В.Н. Янкович, Р.В. Кислинский

Система защиты персонального компьютера должна позволять пользователю при соответствующем контроле получать доступ к информации. Для защиты от чужого вторжения следует предусмотреть меры непосредственной защиты вычислительных устройств и информации от несанкционированного доступа.

Защита встроенного жесткого диска от доступа осуществляется обычно путем применения паролей для идентификации пользователя.

Средства защиты диска от записи (чтения) и средства контроля за обращением к диску рассчитаны на защиту диска от конкретных действий. в частности, средства защиты могут установить определенный режим обращения к диску, установить контроль, требующий подтверждения пользователя, или контроль, позволяющий пользователю визуально выяснить, было ли обращение к диску.

Эти средства защиты достаточно эффективны, но не обеспечивают абсолютной защиты.

Если на диск сохраняются остатки секретной информации, это требует особого обеспечения безопасности вычислительной техники. Специальные программные средства позволяют уничтожать такие остатки информации или стирать информацию при удалении файлов, что исключит возможность возникновения секретных остатков.

Защита, осуществляемая сетевым программным обеспечением, включает:

– подтверждение подлинности пользователей (парольная идентификация);

– установление и проверку полномочий пользователя по доступу к информационному объекту;

– контроль атрибутов защиты (возможных действий) информационного объекта (профиль безопасности основного информационного объекта);

– установление и проверку атрибутов защиты отдельного файла (детализация профиля безопасности информационного объекта).

Список литературы

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

2. Завгородний В.Л. Комплексная зашита информации в компьютерных системах. М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XVII Белорусско-российской научно–технической конференции
(Минск, 11 июня 2019 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 03.06.2019. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 10,0. Уч.-изд. л. 8,2. Тираж 100 экз. Заказ 142.

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.
220013, г. Минск, ул. П. Бровки, 6