Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Общественное объединение «Белорусское инженерное общество»

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XX Белорусско-российской научно-технической конференции
(Республика Беларусь, Минск, 7 июня 2022 года)

Минск БГУИР 2022

УДК 004.056.5
ББК 32.972.5
Т38

Т38 **Технические** средства защиты информации : тез. докл. XX Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 7 июня 2022 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2022. – 112 с.

ISBN 978-985-543-651-6.

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

УДК 004.056.5
ББК 32.972.5

ISBN 978-985-543-651-6

ОГЛАВЛЕНИЕ

APPLICATION OF SOFT DECISION DECODING FOR REED SOLOMON CODES IN BIOMETRIC SYSTEMS

B. Assanovich, Ayad Merawiy Abdullah

Error-correcting codes (ECC) are widely used in communication systems, and information security applications, where it is important to ensure access security with noisy input data. In recent years, the non-binary code constructions have attracted the particular interest because of their flexibility high efficiency at low signal-to-noise ratio. In this abstract we propose to use the new error-and-erasure decoding algorithm based on Reed Solomon (RS) symbol reliability. This algorithm applies the Soft Decision Decoding (SDD) technique for RS ECC by the search for the "unreliable" RS symbols calculated as absolute value of the deviation in magnitude relative to its mean for a current biometric measurement. It is an iterative method and can be easily realized with hardware or/and software components with low complexity compared to Hard Decision Decoding (HDD).

The SDD procedure is performed on the basis of the updating the erasure vector, in which the elements are cyclically shifted in case of failure appearance in the HDD algebraic method. The decoding procedure ends when decoding is successful and the message (key R) is found, or after all possible cyclic shifts of the initial erasure vector are completed. Since the positions of the most unreliable symbols will be at the beginning of the vector of indices K, correct decoding is achieved after a few shifts.

We have studied the biometric authentication system (BAS) [1] that uses a known Fuzzy Commitment (FC) scheme and several RS codes constructions and two types of helper data (HD1 and HD2) obtained from the biometric measurements at the enrollment stage. In our experiments we found that the application of a proposed SDD technique for RS code resulted in better efficiency (code rate) of RS code with SDD compared to RS (63,15) and RS (31,9) ECC concatenated with linear code and separately with repetition codes (3,1,1). Several experiments have been carried out to train neural network (stacked autoencoder) for 10 different groups of 40 users each, randomly selected from the UvA-NEMO database. For this compiled dataset the encoding-decoding procedures were modeled using the above-mentioned ECC. For processed 200 subjects from the dataset, the real-valued data with lengths of 63 and 31 elements obtained from SAE and equidistantly quantized have been encoded with non-binary RS codes. We applied the RS code (63,31), which made it possible to expand the cryptographic key to |R|=21*=126 bits in the absence of the 2nd coding stage with efficiency 126/63*6=0.33. The proposed SDD algorithm was used with erasure vector lengths of 21-19 elements. In the following experiments, we also examined the coding of two blocks of RS code (31,17), which made it possible to obtain the total key length |R|=2*17*5=170 bits with an efficiency of 85/170=0.5. The EED decoding was used as in previous experiments with erasure vector lengths of 6-5 elements.

The simulation of BAS has shown the possibility of achieving FRR values of no more than 0.7% and 0.3% for crypto keys of size 170 and 126 bits for biometric feature data dimensions of 63, 31 elements and simplify the overall structure of a biometric system.

References

1. Assanovich B., Kosarava K. Authentication System Based on Biometric Data of Smiling Face from Stacked Autoencoder and Concatenated Reed-Solomon Codes // Communications in Computer and Information Science. 2022. Vol 1562. P. 205–219.

SOFTWARE MODULE FOR IRIS SELECTION IN THE IMAGE

O.D. Chkoidze, I.V. Ibragimov

The selection of the iris in the image is a search in the image a relatively dark object close in shape to a circle containing a concentric darker object (pupil) inside. One more condition is added in most systems: inside the pupil there must be a bright glare of a certain shape (glare from the illuminator). This problem can be solved in many ways for example by searching for concentric circles using the Hough transform or using a correlator to search a glint of a given shape with subsequent detection of the contours of the pupil containing this glint and then of the iris concentric to pupil [1]. Specific is the presence of eyelids in most cases covering the upper and lower parts of the iris. Some systems such as Iridian explicitly highlight eyelids and discard false data from covered areas. As a result of the work a software module for iris detection in the image was developed. The work of this module consists of the following main stages.

1. Image erosion. Allows you to enhance the border of the transition of brightness in the image and make the outline of the iris clearer.

2. Median filtering. Used to reduce noise in the image particularly around the outline of the iris.

3. Binarization by the Canny boundary detection method. Allows you to get the contours of the iris.

4. Selection of circles using the Hough algorithm [2].

The software module was implemented by the C++ programming language in the Visual Studio environment using the ltilib library. This module allows to work with images of different formats, such as bmp, jpeg, and different sizes.

Literature

1. Gonzalez R., Woods R. Digital Image Processing. Moscow: Technosfera, 2005.

2. Ecabert O., Jean-Philippe Thiran J.-P. Adaptive Hough Transform for the Detection of Natural Shapes Under Weak Affine Transformations // Pattern Recognition Letters. 2004. Vol. 25. P. 1411–1419.

SOFTWARE TOOL FOR SPEAKER RECOGNITION

U.O. Kunitsky, N.S. Lun, V.S. Zaikovsky

The rapid development and widespread dissemination of information systems and technical means necessitates computer processing of speech information because the voice interaction interface seems to be the most convenient. Thus it is advisable to use voice technologies for biometrics namely the verification of the speaker by voice. Verification by voice is a procedure for confirming identity using individual speech characteristics. There are text-dependent and text-independent verification systems. Text-dependent require the pronunciation of a certain phrase and compare it with the standard for each user. Verification in text-independent systems is carried out on the basis of any speech fragment of a given length. The primary task of speaker verification is speech signal recognition. To solve it a software module is proposed that analyzes the acoustic environment and calculates the following signal parameters: root mean square value, average number of signal zero crossings, pitch period. Then the calculated parameter values are compared to user-defined threshold values. If the values of all parameters simultaneously meet the established requirements, then the analyzed fragment of the signal is considered to be a speech. This module is implemented in the C++ programming language in the Visual Studio environment. It is possible to manually set the threshold values of the parameters in order to adapt the algorithm settings and study the features of speech recognition. The user verification is implemented in a separate module which receives signal fragments classified

as speech as input. The verification module is also implemented in the C++ programming language in the Visual Studio environment. The operation of the module is designed in such a way that a text login is required first in order to identify the user and then the pronunciation of password is required to verify the user. This avoids the need for an empirical search for a balance between the possibility of errors of the first and second types while lowering the coefficient of cognitive resistance of the end user [1]. A vector of Mel-frequency cepstral coefficients [2] is calculated from the frequency characteristic of the signal using a discrete cosine transform and is compared to the database of reference user records. As a reference record for each user the average value of vectors of Mel-frequency cepstral coefficients calculated for three pronunciations of the passphrase is used. The comparison is implemented using a self-organizing Kohonen neural network.

Literature

1. Kunitsky U.O., Zelmansky O.B. Verification of the Speaker by voice Based on the Method of Dynamic Time Distortion // Abstracts of the XIX Belarusian and Russian scientific and Technical Conference "Technical means of information protection", Minsk, June 8, 2021. P. 59.

2. Zapryagaev S.A., Konovalov A.U. Recognition of Speech Signals // Bulletin of VSU. 2009. No. 2. P. 39–48.

VOICE PROTECTION MODULE

K.P. Shakin, N.A. Muhyev, I.L. Soqashe

The development of digitalization is inextricably linked to the protection of information which is one of the most important assets of any organization. In this regard one of the problems of information security is the leakage of information through the acoustic channel. Protection of speech information is an important sphere in the ensuring information security and is implemented by using passive and active means of information protection. Active means for speech information protection involve the use of white, pink and speech-like noise generators to create masking noise. It has been proven that the noise in its spectral composition should be close to the speech signal for effective masking. To generate a speech-like signal it is proposed to apply the compilation method of speech synthesis which consists in compiling the minimum acoustic units – allophones. At the same time the building of a database of allophones for the Russian language is carried out on the basis of articulatory syllabic and word tables corresponding to GOST 16600-72. The developed speech information protection module [1] performs the following functions: formation of a phonemic pseudo text, compilation of a speech-like signal and its reproduction. In turn the implementation of a phonemic pseudo text is carried out in accordance with the rules and algorithm proposed in [2] based on the features of the language in which a confidential conversation is conducted. The features of the Russian, Arabic, Kazakh and Turkmen languages were studied in order to achieve the greatest similarity of the generated speech-like speech signal in the corresponding language. As a result, a speech-like noise is formed at the output of the module which then enters the input of the acoustic system.

Literature

1. Shakin K.P., Zelmansky O.B. Development of the System for Synthesizing a Speech-Like Signal // Abstracts of the XIX Belarusian and Russian scientific and Technical Conference "Technical means of information protection", Minsk, June 8, 2021. P. 99.

2. Lobanov B.M. Synthesis of Speech by Text. Collection of Scientific Papers of the 4th International School-Seminar on Artificial Intelligence. Minsk: BSUIR, 2000.

INCREASED RELIABILITY OF COMPUTER SYSTEM BY USING FAULT TOLERANCE TECHNIQUE

H.H. Sudani

Fault-tolerant computing began between 1965 and 1970, probably with the highly reliable and widely available AT&T electronic switching systems.

Fault-tolerant computing is a general term describing redundant design techniques with redundant components or repetitive computations that provide continuous (tolerant) performance in response to component failures. Sometimes system failures are caused by neglecting the principles of redundancy and independence from failures. Codes are developed that detect and correct errors, and an analysis is made of the probability of failure of such codes.

Fault tolerance refers to numerous issues regarding various aspects of system development, deployment, and maintenance, the two most common of which are reliability and availability [1]. The reliability and availability of computer, standby, and voting systems are analyzed and compared, and such analyses are also applied to modern RAID memory systems and commercial Tandem and Stratus fault-tolerant computers. Fault-tolerant computing means computing correctly despite the existence of errors in a system. Any system containing redundant components or functions has some of the properties of fault tolerance. Computing systems can provide several benefits such as scalability, fault tolerance, and load balancing. Collaboration with distributed systems and data storage is associated with several problems and difficulties [2]. Fault tolerance is to perform multiple computations through multiple channels, either sequentially or concurrently. When tolerance of physical faults is foreseen, the channels may be of identical design, based on the assumption that hardware components fail independently [3].

Methods of fault tolerance in large computing systems. These methods can be divided into two categories: protecting the hardware and software infrastructure for cluster management and protecting the compute nodes and the long-running applications that run on them. Employing fault-tolerance techniques to improve general reliability. Fault-tolerant solutions can be implemented in various forms. This includes software libraries, special programming languages, compiler or preprocessor modifications, operating system extensions, and system middleware.

References

1. Barringer H.P. Life Cycle Costs & Reliability for Process Equipment. Houston, 1997. 22 p.

2. Bobed C., Ilarri S., Mena E. Distributed Mobile Computing Development of Distributed Applications Using Mobile Agents // Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA 2010, Las Vegas, Nevada, USA, July 12–15, 2010. P. 1–7.

3. Avižienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Transactions on Dependable and Secure Computing. 2004. № 1. P. 11–33.

МЕЖДУНАРОДНЫЕ ОЛИМПИАДЫ ПО КРИПТОГРАФИИ SARCRYPT

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

Две важнейшие задачи для подготовки специалистов в области защиты информации: 1) привлечение заинтересованных школьников для поступления на направления обучения, связанные с информационной безопасностью; 2) выявление талантливых студентов, обучающихся по направлениям информационной безопасности, и повышение их мотивации. Одним из методов решения этих задач является проведение профильных соревнований. В Саратовском научном исследовательском государственном университете имени Н. Г. Чернышевского с этими целями с 2002 года проводятся олимпиады по криптографии SarCrypt.

Первые годы олимпиада проводилась для старшеклассников с целью популяризации криптографии и привлечения талантливых школьников к поступлению на соответствующие направления обучения в вузы. Задания составлялись для учеников 9–11 классов. Студенты могли принимать участие в олимпиаде вне конкурса. С 2019 года олимпиада стала проводиться для трех категорий участников: учеников 6–8 классов, 9–11 классов и студентов. Олимпиада проходит в два тура. В первую полную неделю декабря проводится дистанционный тур (отборочный), а в январе проводится очный тур на базе факультета компьютерных наук и информационных технологий Саратовского государственного университета. На решение задач дистанционного тура дается одна неделя, а на решение задач очного тура – 3 часа. Ученикам 6-8 классов предлагается 6 задач, ученикам 9–11 классов – 8 задач, студентам – 10 задач по криптографии, теории кодирования, комбинаторике и другим разделам математики и информатики.

В 2021-2022 учебном году дистанционный тур проводился с 6 по 12 декабря 2021 года. В отборочном туре приняли участие 56 учеников 6–8 классов, 92 ученика 9–11 классов и 56 студентов из городов России, Республики Молдовы и Туркменистана. Кроме участников из Саратова и области были участники из городов Абакан, Белебей, Далматово, Ессентуки, Йошкар-Ола, Калининград, Красноярск, Курумкан, Магнитогорск, Минусинск, Назарово, Нижний Новгород, Орел, Рыбница, Самара, Сочи, Старый Оскол и других населенных пунктов. Победители первого тура получили приглашение на второй тур, который состоялся 30 января 2022 года.

В условиях сложной эпидемиологической обстановки очный тур второй год подряд проводился в режиме онлайн на базе платформы ZOOM. Во II туре приняли участие 28 участников из городов Абакан, Саратов, Красноярск (Россия), города Рыбница (Республика Молдова) и этрапа Каахка (Туркменистан): 8 участников в категории 6-8 классы, 31 участник в категории 9–11 классы и 8 студентов. Все участники I и II туров получили электронные дипломы, а их руководители – грамоты. Итоги обоих туров олимпиады можно посмотреть на сайте [1].

Литература

1. Олимпиады по криптографии [Электронный ресурс] // Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского [Электронный ресурс]. – Режим доступа: https://www.sgu.ru/structure/ computersciences/theorcompsafe/ olimpiady-po-kriptografii. – Дата доступа: 04.05.2022.

АНАЛИЗ ПАРАМЕТРОВ МАЛОГАБАРИТНЫХ ВИДЕОКАМЕР ДЛЯ СКРЫТОГО СЪЕМА ВИЗУАЛЬНОЙ ИНФОРМАЦИИ

В.М. Алефиренко, А.М. Асиненко

Для скрытого получения визуальной информации используются малогабаритные видеокамеры, которые для этого устанавливаются в наиболее удобных местах, включая и их монтаж в предметы обихода. Полученная видеоинформация может записываться непосредственно в память видеокамеры или передаваться в режиме реального времени по проводному или электромагнитному каналу [1]. Для обнаружения малогабаритных видеокамер используются специальные детекторы – обнаружители видеокамер. Обнаружение скрытых видеокамер такими детекторами может осуществляться как по электромагнитному каналу путем фиксации электромагнитного излучения работающей видеокамеры, так и по оптическому каналу путем фиксации отражения световых лучей, посылаемых детектором, от объектива скрытой видеокамеры. Для правильного выбора соответствующего детектора необходимо знать возможности и технические характеристики малогабаритных видеокамер, модели которых широко представлены на рынке технических средств для скрытого съема информации. Сравнительный анализ их характеристик требует комплексного подхода из-за большого количества различных моделей и характеристик, отличающихся своими количественными значениями.

Для сравнительного анализа использовался комплексный метод определения уровня качества с использованием единичных показателей [2], в качестве которых брались следующие технические характеристики малогабаритных видеокамер: угол обзора, видеоразрешение, количество кадров в секунду, время автономной работы, дистанция ночной подсветки, объем поддерживаемых карт памяти, емкость аккумулятора, габаритные размеры, вес, цена. Для сравнения были выбраны следующие модели: BOBLOV (10 моделей), Vandlion (5 моделей), SQ (7 моделей), Camsoy (3 модели), MD (2 модели), Jozuze (2 модели), W6 (1 модель). Всего для сравнения было выбрано 30 моделей. Расчет проводился с использованием средневзвешенного арифметического показателя качества [3]. Предварительно было проведено нормирование единичных показателей и соответствующих им коэффициентов значимости. Результаты расчетов показали, что наилучшие значения показателей качества были у модели W6 (0,69), на втором месте – SQ28 (0,58) и на третьем месте – SQ11 (0,56).

Анализ полученных результатов также показал, что значения арифметического показателя для исследуемых малогабаритных видеокамер лежат в пределах от 0,69 до 0,37, то есть максимальное и минимальное значения отличаются почти в два раза.

Литература

1. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов информатизации: справочное пособие. СПб.: Лань, 1996. 272 с.

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

3. Алефиренко В.М., Никитенко Д.А. Оценка уровня качества генераторов шума для защиты информации от утечки по акустопреобразовательным каналам // Scientific Pages. 2021. № 31. С. 17–20.

КОМПЛЕКСНЫЙ АНАЛИЗ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ПЕРЕНОСНЫХ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ПОДАВЛЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

В.М. Алефиренко, А.Д. Денскевич

В последнее время наблюдается стремительное развитие технологий беспилотной авиации, которые значительно повысили автономность и дальность действия, а также существенно расширили спектр задач, решаемых беспилотными летательными аппаратами (БПЛА) [1]. В связи с этим, остро встает вопрос защиты объектов от несанкционированного проникновения таких аппаратов на их территорию [2]. Одним из способов борьбы с БПЛА является использование переносных радиоэлектронных средств подавления (ПРСП). Такие средства способны нейтрализовывать БПЛА на расстоянии до 2-х километров и автономно работать несколько часов, что в случае своевременного обнаружения БПЛА, позволяет достаточно эффективно бороться с ними.

Как показал обзор, на рынке технических средств защиты информации и обеспечения безопасности объектов представлено большое разнообразие моделей ПРСП, выпускаемых различными фирмами. Поэтому, выбор наиболее оптимальной по своим техническим характеристикам модели представляет определенную трудность, так как требует анализа большого числа различных характеристик, отличающихся своими количественными значениями.

Для оптимального выбора предлагается использовать комплексный метод определения уровня качества с использованием единичных показателей [3]. В качестве единичных показателей для ПРСП использовались такие технические характеристики как дальность подавления, время непрерывной работы, диапазоны частот блокирования, диапазон рабочих температур, вес и габаритные размеры. Для сравнения были выбраны следующие модели: Аргумент-2, ПАРС, Дрон 1200, Гарпун-2М, Novasky SC-J1000m, Drone Hunter XR, QLY-F069, Droneshield MKIII, Vodasafe DJ600, Greetwin GW-UAV90Pro и ряд других. Всего для сравнения было выбрано 32 модели. Расчет проводился с использованием средневзвешенного арифметического показателя качества [4]. Предварительно было проведено нормирование единичных показателей и соответствующих им коэффициентов значимости. Как показали результаты расчетов, наилучшие значения показателей качества были у модели QLY-F90S (0,59), на втором месте – Eagle QR-0783 (0,55) и на третьем месте – Greetwin GW-UAV70 (0,54).

Таким образом, определение качественных характеристик ПРСП, выраженных относительными численными значениями, позволило провести их сравнение и определить лучшую модель по выбранным для сравнения техническим характеристикам.

Литература

1. Васильев О.А. Тихий дрон // Защита информации. INSIDE. 2020. № 1. С. 26–30.

2. Петровская М.Р., Лысов А.В. Состояние и перспективы развития средств защиты от БПЛА // Защита информации. INSIDE. 2020. № 5. С. 78–81.

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

4. Алефиренко В.М., Никитенко Д.А. Оценка уровня качества генераторов шума для защиты информации от утечки по акустопреобразовательным каналам // Scientific Pages. 2021. № 31. С. 17–20.

СИСТЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В СЕНСОРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ КОМБИНАТОРНЫХ БЛОК-СХЕМ

М.А. Алисеенко, С.Б. Саломатин

Рассматривается распределенная сенсорная сеть, в которой N сенсорных узлов случайным образом разбросаны по территории. Сенсорные узлы взаимодействуют друг с другом и требуют парных ключей для защиты своей связи. Каждый датчик имеет связку из K ключей, которая хранится в его ПЗУ перед развертыванием. При этом пара сенсорных узлов должна иметь пул общих ключей в своей цепочке ключей.

Проблема состоит в том, чтобы выбрать размер цепочки для ключей и размер пула ключей, чтобы каждая пара узлов могла установить ключ сеанса напрямую или через путь с высокой вероятностью [1].

Математической основой системы является сбалансированные блок-схемы (BIBD), представленные множеством взаимных ортогональных латинских квадратов [2].

Алгоритм системы распределения ключей включает в себя следующие действия. Нахождение степень простого числа n, удовлетворяющего квадратичному соотношению, соответствующему размеру сети N. Формирование $(n-1)$ полного набора взаимных ортогональных латинских квадратов (MOLS) порядка n. Построение аффинной плоскости порядка n по MOLS. Построение проективной плоскости порядка n по аффинной плоскости.

Для симметричных блок-схем справедливо, что любая пара блоков разделяет ровно один объект. Таким образом, вероятность совместного использования ключа между любой парой узлов равна 1, поэтому средняя длина пути к ключу равна 1.

Комбинаторный подход увеличивает вероятность того, что пара сенсорных узлов будет иметь общий ключ, и уменьшает длину ключевого пути.

Литература

1. Song, Y., Wool A., Yener B. Combinatorial Design of Multi-Ring Networks with Combined Routing and Flow Control. Computer Networks. 2003. Vol. 3 (3). P. 247–267.

2. Colbourn, C.J., Dinitz J.H. The CRC Handbook of Combinatorial Designs. CRC Press, 1996. 753 p.

АДАПТИВНЫЕ ТЕПЛОВЫЕ ПОЖАРНЫЕ ИЗВЕЩАТЕЛИ В СИСТЕМАХ АВТОМАТИЧЕСКОГО ПОЖАРОТУШЕНИЯ

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

Характерной особенность автоматических систем пожаротушения являются высокие требования к достоверности и своевременности обнаружения пожара, особенно на начальных стадиях [1]. При позднем обнаружении возгорания высок риск снижения эффективности пожаротушения, при ложном срабатывании – возникает угроза персоналу от непосредственного воздействия огнетушащих составов. Наличие таких условий автоматически поднимает требования к пожарным извещателям. На сегодняшний день практическое применение нашли следующие типы извещателей: оптические дымовые, максимальные и максимально-дифференциальные тепловые и пламени [2].

Анализ применения перечисленных выше извещателей позволяет отметить их характерные недостатки, лишающие их универсальности. В частности, оптические дымовые и извещатели пламени не допускают использования в помещениях повышенной запыленности и загазованности, а также требуют периодической очистки оптической системы (дымовой камеры, линз для линейных систем).

Максимальные тепловые извещатели, как правило, не позволяют обнаруживать пожар на ранних стадиях из-за большой инерционности срабатывания [3]. Максимально-дифференциальные извещатели отчасти решают эту проблему, но установленная на стадии монтажа скорость нарастания температуры, соответствующая пожару, не учитывает возможные изменения пожарной обстановки на объекте.

В качестве альтернативы перечисленным выше извещателям может служить адаптивный тепловой извещатель, в котором максимальная температура и скорость ее нарастания, соответствующая пожару, может меняться в зависимости от внешних условий. Эти изменения осуществляются автоматически блоком управления, представляющим из себя либо единое целое с датчиком температуры, либо отдельно расположенным. В качестве примера можно привести ситуацию с объектом из металлоконструкций. В солнечный, особенно летний день нагрев конструкции приводит к заметному увеличению температуры внутри помещения, с заметной скоростью нарастания. Для обычных максимальных или максимально-дифференциальных извещателей данная ситуация может оказаться близкой к пороговой, занижение чувствительности приведет к более позднему обнаружению возгорания. Адаптивный извещатель может оперативно скорректировать свои показатели в сторону загрубления по результатам измерения внешней температуры или температуры металлоконструкций. Подобный подход удобен в случае обнаружения пожара по двум извещателям, например, при сработке первого любого извещателя адаптивный тепловой извещатель корректирует свои характеристики в сторону повышения чувствительности.

Таким образом, используя автоматический программируемый тепловой извещатель, можно существенно повысить оперативность обнаружения возгорания без риска ложных срабатываний. Опыт практического применения показал высокую эффективность применения таких извещателей в пожарной сигнализации транспортных средств и зерносушильных комплексов.

Литература

1. ГОСТ 12.1.004-9. Пожарная безопасность. Общие требования.
2. СТБ 11.16.01-98. Системы пожарной сигнализации. Общие требования.
3. СТБ 2218-2011. Извещатели пожарные тепловые.

РЕАЛИЗАЦИЯ МЕТОДА ЦИФРОВОЙ СТЕГАНОГРАФИИ С ПОМОЩЬЮ МОДУЛЕЙ И БИБЛИОТЕК PYTHON

А.М. Ахапкина, С.В. Способ

В век высоких технологий информация представляется наибольшей ценностью. Поэтому не удивительно, что в последнее время создается множество средств для ее защиты. Стеганография – способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи. В данном случаи у злоумышленника нет никаких зацепок, где искать закрытые и уже зашифрованные данные, как и, собственно, нету намеков, что уже что-то где-то спрятано.

Существует множество способов и методов стеганографии, каждые из которых преследуют свои цели. В статье будет рассмотрен метод наименее значащих битов (Least Significant Bit, LSB), который считается наиболее популярным для цифровой стеганографии. Цифровая стеганография основывается на ограниченности способностей органов чувств человека и, как следствие, неспособности распознать незначительные вариации звука/цвета. Для простоты понимания рассмотрим

графический контейнер – изображение. В данном формате для описания каждой точки (пикселя) используются 3 байта, обозначающие в какой пропорции необходимо смешивать красный, зеленый и голубой цвета (цветовая схема RGB). Если произвести замену старших бит в этих байтах, цветовые изменения в картинке будут бросаться в глаза. Младшие же биты дают куда более незначительный вклад в изображение. Если использовать по одному младшему биту в каждом цвете для записи скрываемого сообщения, то распознать изменения человеческий глаз будет не способен.

Алгоритм стеганографии можно реализовать с помощью различных языков программирования. В нашей статье будут рассмотрены модули и библиотеки Python. Программу, которая будет записывать и как следсвтие скрывать текст в изображение можно реализовать засчет модуля lsb. Однако, у данного модуля есть большой недостаток – восприятие кириллицы, данный модуль не распознает ее. Поэтому, если необходимо работать как с английским текстом, так и с кириллицей необходимо использовать модуль exifHeader

Однако, в независимости от выбора модуля и метода, отрытое сообщение легко разрушить, сжимая или отображая изображение. При таком подходе не обеспечивается секретность встраивания сообщения: точно известно местоположение информационных битов (каждый крайний с конца бит). Для преодоления второго недостатка можно встраивать сообщение не во все пиксели изображения, а выбирать их при помощи генератора псевдопростых чисел (инициализированного ключом стеганосистемы). Стоит заметить, что пропускная способность при этом уменьшится. Для генерации ключей необходимо воспользоваться библиотеками wheel и steganocryptopy. Генерация ключа происходит методом generate_key(), в параметрах которого необходимо передать путь, куда будет сохранен файл с ключом

Само шифрование происходит методом encrypt(), где параметрами передаются путь до ключа, изображение и путь до файла, в котором будет содержаться сообщение. Затем необходимо вызывать метод save() и передать в нем путь к изображению, в котором будет скрыт текст. Дешифрование происходит методом decrypt() схожим образом.

Естественно у данного метода стеганографии есть недостаток: видимость битых пикселей изображения в случаи скрытия большого количества символов. Однако этот недостаток отлично исправляется высоким разрешением изображения.

НОВЫЙ ТИП ПРИЗНАКОВ ДЛЯ ОПИСАНИЯ ИЗОБРАЖЕНИЙ РУКОПИСНОЙ ПОДПИСИ НА БАЗЕ ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ

У.Ю. Ахунджанов, В.В. Старовойтов

В работе предлагается новый признак подписи, инвариантный к ее размерам и ориентации. Подпись — один из старейших способов защиты документов, который является исторически подтвержденным и наиболее часто используемым средством защиты документов, особенно финансовых. Ежегодно появляются новые подходы к решению проблемы распознавания рукописных подписей. Проблема проверки подлинности рукописной подписи относится к задачам распознавания образов. Основные сложности с распознаванием подписи связаны со следующими факторами:

- подпись – это краткое и малоинформативное представление данных;
- она может быть скопирована с применением технических средств;
- почерки разных людей естественным образом бывают похожи;
- подпись человека всегда вариативна;
- злоумышленник пытаются подделывать чужие подписи.

Для решения задачи распознавания подписи человека важное значение имеет

ее инвариантное представление в виде цифрового изображения. Чем выше разрешение и меньше цифрового шума, тем точнее будут сформированы признаки подписи. Для этого авторами предлагается универсальная процедура предварительной обработки и нормализации размера произвольной оцифрованной в виде изображения подписи. Процедура состоит и последовательности преобразований, выполняющих бинаризацию изображения подписи, его фильтрацию, поворот изображения до горизонтальной ориентации подписи, вырезание описывающего прямоугольника и масштабирование в шаблон фиксированного размера.

Локальные бинарные шаблоны (LBP) известны с 1994г, как текстурные признаки для полутоновых изображений. LBP вычисляются в окрестности каждого пикселя как однобайтовое число. Они описывают окрестность размером 3×3 в зависимости от значений яркости [1]. Порядок всех соседей фиксируется, их позиции пронумерованы от 0 до 7. Если яркость *i*-го соседнего пикселя больше яркости центрального, ему присваивается код 2^i, если меньше – присваивается ноль. Затем коды всех восьми соседей суммируются. Сумма находится в диапазоне от 0 до 255 и присваивается в виде текстурного кода центральному пикселю. В данной работе впервые предлагается к нормализованному бинарному изображению подписи применить вычисление LBP к пикселям бинарного представления подписи. Они вычисляются аналогично вышеописанному, но код 2^i присваивается *i*-му соседнему пикселю при условии, что он имеет черный цвет. После кодирования всех пикселей строится гистограмма LBP значений, представляющая собой массив из 256 элементов. Из него отбрасываются первый и последний элементы, соответствующие вариантам кода все восемь соседний пикселей, имеют белые либо черные значения. Получившийся набор из 254 чисел является новым инвариантным признаком нормализованного представления подписи, описывающим распределение локальных особенностей подписи человека независимо от ее исходных размеров и ориентации. Эксперименты показали, что, вычисляя корреляцию Пирсона между такими признаками, можно различить подписи разных людей.

Литература

1. Ojala T., Pietikainen M., Maenpaa T.Multi Resolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2002. Vol. 24, № 7. P. 971–987.

МОДЕЛИРОВАНИЕ ОПТИМАЛЬНЫХ РЕЛЯТИВИСТСКИХ ЛБВ-0

И.В. Баженова

На основе строгой электродинамической теории [1] и эффективного метода матричной прогонки для решения краевой задачи, описывающей возбуждение электронным потоком связанных волн нерегулярного волновода, выполнен поиск оптимальных по КПД вариантов ЛБВ-0 с нерегулярным профилем гофра. Показано, что за счет оптимального профилирования глубины гофра КПД может быть повышен почти в два раза и достигает 65 %.

Предложенная ранее в работах строгая электродинамическая теория возбуждения симметричных E_{01}-волн нерегулярного волновода является основой для создания адекватной модели релятивистских сверхмощных ЛБВ-0 и ЛОВ-0 на нерегулярном гофрированном волноводе. Согласно этой теории, решение задачи возбуждения нерегулярного волновода ищется в виде разложения в ряд по системе собственных

волн (как распространяющихся, так и закритических), цилиндра единичного радиуса на который отображается нерегулярный волновод.

На основе упрощенной модели, в которой не учитывались закритические волны, были получены варианты релятивистских ЛБВ-0 с расчетным КПД до 80 %. Однако, для адекватного описания процессов взаимодействия, позволяющего найти точные значения параметров оптимальных вариантов, необходим учет ближайших закритических волн.

Метод пристрелки на основе решения задачи Коши, который использовался в [2], оказывается непригоден ввиду его неустойчивости при учете закритических волн, поэтому в настоящей работе использовалась оригинальная методика решения краевой задачи для системы обыкновенных дифференциальных уравнений [1] с использованием метода блочной матричной прогонки [3].

Литература

1. Гуринович А.Б., Кураев А.А., Синицын А.К. Электродинамическая теория ЛБВ-0 на гофрированном волноводе с учетом высших гармонических составляющих сигнала. // Электромагнитные волны и электронные системы. 2000. Т. 5, № 6. С. 11–16.

2. Закалюкин А.Б., Кураев А.А. Оптимальные по коэффициенту полезного действия релятивистские лампы бегущей волны 0-типа с замедляющей системой в виде гофра с изменяющимся периодом и глубиной канавки // Радиотехника и электроника. 2000. Т. 45, № 4. С. 499–501.

3. Батура М.П., Кураев А.А., Синицын А.К. Оптимизация релятивистских ЛБВ-0 на нерегулярных волноводах с учетом высших мод // Материалы 14 Международной конференции «КрыМиКо 2004», Севастополь, 13–17 сентября 2004 г.

МОДЕЛИРОВАНИЕ РЕЛЯТИВИСТСКИХ КЛИСТРОНОВ-ГЕНЕРАТОРОВ

И.В. Баженова

В результате исследований были найдены восемь вариантов трех- и двухкаскадных клистронов-генераторов. Изучены физические параметры, особенности моделирования и применения для двух- и трехкаскадных клистронов-генераторов. Простейшие двух- и трехкаскадная конструкции генератора, работающего по схеме клистрона с обратной связью, в котором роль модулятора и отбирателя играют резонансные канавки. Резонансные канавки, настроенные на отражение E_{01}-волны, выполняют одновременно роль рефлектора, закрывающего катод, что важно при многоволновой реализации генератора. Обратная связь в генераторе осуществляется за счет отраженной волны от замедляющей системы и дополнительных нерегулярностей волновода, которые совместно с модулирующей канавкой образуют резонансную систему.

Электродинамическая система предлагаемой конструкции соответствует пространственно развитой структуре сильноточного релятивистского пучка [1]. Показано, что даже при частичной оптимизации в двухкаскадной конструкции возможен мягкий режим генерации с КПД до 20 %. Также показано, что в трехкаскадной конструкции возможен режим генерации с КПД до 31 %, что приближается к лучшим вариантам черенковских генераторов.

Моделирование проводилось следующим образом: строились двух- и трехкаскадной конструкции генератора на сильноточном релятивистском пучке с электродинамической системой в виде отрезка полого цилиндрического волновода, имеющего две или три резонансные канавки. В поле первой канавки реализуется

начальная модуляция электронного пучка, вторые две обеспечивают отбор энергии. Обратная связь реализуется на волне E_{01}.

Проведенные исследования свидетельствуют о достаточно высокой эффективности релятивистских клистронов-генераторов сверхбольшой мощности, сопоставимой с эффективностью лучших вариантов черенковских генераторов такой же мощности.

Литература

1. Батура М.П., Кураев А.А., Синицын А.К. Оптимизация релятивистских ЛБВ-0 на нерегулярных волноводах с учетом высших мод // Материалы 14 Международной конференции «КрыМиКо 2004», Севастополь, 13–17 сентября 2004 г.

СОРЕВНОВАНИЯ В ФОРМАТЕ CTF КАК ЭЛЕМЕНТ ГЕЙМИФИКАЦИИ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

Г.А. Беззубик, А.П. Базыльчик, А.М. Кадан

Бесспорно, что геймификация, как использование игровых подходов для неигровых процессов, эффективно стимулирует интерес учащихся к получению новых знаний, позволяет повысить их вовлеченность в решение прикладных задач. В свою очередь, сфера компетенций, необходимых специалисту по кибербезопасности, не только сложна, но и неуклонно расширяется, причем требует не только и не столько хорошую теоретическую подготовку, сколько большой практический опыт. Такое положение приводит к необходимости использования технологий геймификации, как важного преимущества, позволяющего донести до «современного студента», с его специфичным отношением к получению информации, сложные знания и навыки.

В докладе представлен подход, предполагающий использование при подготовке специалистов в области компьютерной безопасности методов гейтификации на основе элементов соревнований в формате CTF (Capture Thre Flag). CTF-соревнования весьма популярны среди специалистов по кибербезопасности и внедрение их непосредственно в учебный процесс отвечает представлениям студентов о характере их специальности.

Решение о создании собственного CTF-проекта, несмотря на то, что существует целый ряд ресурсов близкой направленности, оказалось оправданным. Наряду с Task-Based сервисом (использован продукт CTFd), к настоящему времени он включает интерактивный сервис для заданий в формате PPC (Professional Programming and Coding) (использован суперсервер inetd, язык Python и доступ через ncat) и сервис для изучения web-уязвимостей (с использованием Apache, PHP). В настоящее время проект содержит более 200 задач по направлениям «Кодировки», «Буквенные шифры», «Симметричное шифрование», «Асимметричное шифрование», «Анализ кода», «Форензика», «Стеганография», PPC, OSINT, «Угрозы Web».

CTF-проект доступен по адресу (https://ctf.mf.grsu.by), популярен у студентов и активно используется при изучении ряда общеобразовательных (Основы кибербезопасности, Теория информации) и специальных (Основы компьютерной безопасности, Компьютерная криминалистика) дисциплин студентами различных специальностей факультета математики и информатики, а также при проведении традиционных (Junior.Crypt) и профильных олимпиад ГрГУ им.Янки Купалы.

ПРИМЕНЕНИЕ ГРАФОВЫХ БАЗ ДАННЫХ В КОНКУРЕНТНОЙ РАЗВЕДКЕ

Т.Е. Белогривая, Р.А. Фортель

Развитие методов и средств мониторинга, адаптивного агрегирования и обобщения потоков информации из глобальных компьютерных сетей для поддержки информационно-аналитической деятельности в различных прикладных сферах является весьма актуальной проблемой, требует использования специальных технических средств и соблюдения определенных этических норм. Подобный вид деятельности, известный как конкурентная разведка по открытым источникам данных, часто ставит своей целью исследовании рынка для развития бизнеса и разработки стратегии его дальнейшего продвижения.

В докладе представлен пример реализации методов конкурентной разведки по открытым источникам - веб-сайтам, публикующим объявления о вакансиях. Целью ставилось изучение потребностей белорусских работодателей в специалистах ИТ-сферы и динамики изменения таких потребностей за последнее время. Учитывая объем информации и ее сетевой характер, в качестве среды анализа и визуализации была выбрана графовая база данных Neo4j, решение с открытым кодом.

В качестве содержательных и надежных общедоступных источников данных были использованы сайты, публикующие в статической форме информацию из внутренних баз данных (подобно сайтам rabota.by, praca.by). Скрейпинг (парсинг) информации веб-страниц производился средствами библиотек requests**,** bs4 и selenium языка Python. Сайты, использующие динамическое формирование контента средствами JavaScript и работу с объектной моделью документа, не рассматривались. Типовые поля данных о вакансии: ИТ-компания, адрес, период, должность, зарплата, опыт работы.

Собранная информация была представлена в формате кортежей вида <object, relation, object>, что позволило анализировать и визуализировать ее средствами графовой базы данных Neo4j, а также приложениями, реализующими технологию гиперболического браузера. Были получены эффективные представления о конкурирующих на рынке компаниях, приоритетах ИТ-отрасли, изменениях атрибутов вакансий и динамике спроса на специалистов. Использование средств графовой БД показало их высокую эффективность в сравнении со средствами реляционных СУБД.

ВЛИЯНИЕ РАЗМЕРА ГЕОМЕТРИЧЕСКИХ НЕОДНОРОДНОСТЕЙ УГЛЕСОДЕРЖАЩЕГО ПОГЛОТИТЕЛЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ЧАСТОТНЫЕ ХАРАКТЕРИСТИКИ КОЭФФИЦИЕНТОВ ОТРАЖЕНИЯ

Е.С. Белоусова, О.В. Бойправ, И.Н. Валова

В данной работе представлены результаты исследований закономерностей частотных характеристик коэффициентов отражения и передачи электромагнитного излучения (ЭМИ) в диапазоне частот 2,0–17,0 ГГц при изменении диаметра геометрических неоднородностей в виде полусфер для углесодержащих поглотителей, получаемых путем смешивания порошкообразного активированного кокосового угля (25–30 %) с полимерным связующим веществом. Для изготовления геометрических неоднородностей использовались гибкие полимерные формы в виде совокупности полусфер высотой 1,1 см и диаметром 1,5 и 2,5 см. Размер неоднородностей был выбран на основе изучения резонансного способа уменьшения отражения или принципа экрана Солсбери, в котором утверждается, что падающая электромагнитная волна на поглощающую поверхность, расположенная до используемой поверхности на расстоянии четверть длины волны ЭМИ, будет испытывать эффект отражения как от внешней,

так и от внутренней поверхностей, и результатом данного отражения станет появления интерференционной картины нейтрализации начального ЭМИ [1]. Для выбранной частоты 6 ГГц из рассматриваемого диапазона частот 2,0–17,0 ГГц и формул расчета, представленных в [2], получено, что для углесодержащих поглотителей с высотой геометрических неоднородностей в виде полусфер высотой 1 см минимальное значение коэффициента отражению будет для резонансной частоты 6,8 ГГц. Результаты проведенных измерений коэффициентов отражения в режиме короткого замыкания для углесодержащих поглотителей с геометрическими неоднородностями в виде полусфер показали, что действительно на частотах 6,7–7 ГГц значение коэффициента отражения является минимальным и составляет –22,6 дБ. Также присутствуют резонансные частоты 9,5 ГГц, 10,5 ГГц, 11,5 ГГц, оценка которых позволила сделать вывод, что диаметр неоднородностей влияет на величину значения коэффициента отражения, а именно чем меньше диаметр, тем меньше значение коэффициента отражения.

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

Литература

1. Панкрашин Р.А., Сарматин Я.И., Глуховской А.Д. Технологии разработки широкополосных радиолокационных поглощающих покрытий // Меридиан. № 10 (44). 2020. С. 1–6. URL: http://meridian-journal.ru/site/article?id=3854&pdf=1.

2. Панова Е.В. Исследование геометрических критериев электромагнитных резонансов // Технологии техносферной безопасности. № 1 (53). 2014. С. 1–12. URL: http://agps-2006.narod.ru/ttb/2014-1/14-01-14.ttb.pdf.

ОБОСНОВАНИЕ НОВЫХ ПРИНЦИПОВ ПРОВЕДЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

В.А. Бойправ, Л.Л. Утин

Установлено, что основными недостатками при проведении аудита систем менеджмента информационной безопасности (СМИБ) организаций являются следующие:

- необходимость выполнения интеграции принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и национальных технических, нормативных и правовых актов (ТПНА) в сфере защиты информации;
- противоречивость требований принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и требований национальных ТНПА в сфере защиты информации, что затрудняет как процесс интеграции документов указанных видов, так и процесс их одновременного использования в ходе проведения аудита СМИБ;
- исключение из процесса аудита СМИБ сотрудников и персонала, участвующих в создании информационной инфраструктуры организации;
- низкая заинтересованность руководителей организации в проведении аудита СМИБ и слабая их вовлеченность в этот процесс, вследствие чего руководители, как

правило, ориентированы на снижение затрат как на регулярное проведение аудита СМИБ, так и на устранение обнаруженных в ходе аудита недостатков этой системы;

- высокий уровень затрат временных и человеческих ресурсов на проведение аудита СМИБ (как внутреннего, так и внешнего), что обусловлено как вышеперечисленными недостатками, так и отсутствием средств для автоматизации этого процесса.

Для нивелирования указанных недостатков авторами предложено дополнить существующие принципы проведения аудита СМИБ, представленные в ISO/IEC 27007:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности», принципами, обоснованными в работе [1], а также нижеследующими принципами.

1. Принцип всеохватываемости. В соответствии с этим принципом в процессе аудита должны быть задействованы не только работники аудируемой организации, которые в рамках выполнения своих должностных обязанностей используют информационную систему, но и работники, которые обеспечивают создание и эксплуатацию инфраструктуры для этой системы.

2. Принцип оптимизации. В соответствии с этим принципом необходимо принимать все возможные меры для сокращения временных и человеческих ресурсов на проведение аудита путем. Для этого необходимо использовать специальные программные средства для проведения аудита и опросные листы для сотрудников аудируемой организации, составленные на основе принципа разумной достаточности.

3. Принцип своевременности. В соответствии с этим принципом проведение аудита должно проводить как на регулярной, так и на внеплановой основе. Внеплановое проведение аудита СМИБ целесообразно реализовывать после издания новых нормативных документов в сфере защиты информации или внесения изменений и дополнений в такие документы.

Литература

1. Бойправ В.А., Утин Л.Л. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи // Доклады БГУИР. 2016. № 6 (100). С. 94–99.

ГИБКИЕ СЛОИСТЫЕ УГЛЕСОДЕРЖАЩИЕ ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

О.В. Бойправ, С.Э. Саванович, Е.С. Белоусова, Е.С. Ахметдинова

Одно из направлений использования поглотителей электромагнитного излучения (ЭМИ) связано со снижением степени влияния помех на средства вычислительной техники, что сопряжено с решением такой задачи в сфере защиты информации, как обеспечение свойства целостности последней в ходе ее обработки и передачи по каналам связи. На основе таких поглотителей создаются перегородки, предназначенные для отделения зон в помещениях, в которых расположены средства вычислительной техники, или отделочные панели для стен этих помещений. Так как материалоемкость обозначенных изделий высока, то представляется актуальным использовать для их создания поглотители ЭМИ, характеризующиеся невысокой стоимостью. Авторами предложено использовать порошкообразный активированный уголь (древесный или кокосовый) в качестве основного компонента для получения поглотителей ЭМИ, отвечающих обозначенному требованию. В свете этого авторами была разработана серия методик получения поглотителей ЭМИ, содержащих указанный компонент. Одна из разработанных методик, а именно, методика получения

гибких слоистых углесодержащих поглотителей ЭМИ, будет представлена в докладе. Разработанная методика основана на реализации следующих процессов:

- изготовление внутреннего относительно фронта распространения ЭМИ слоя поглотителя путем нанесения слоем толщиной не более 4,0 мм полимерного связующего вещества на одну из поверхностей стекловолокнистого полотна и закрепления с помощью клея на другой из поверхностей этого плотна фольгированной полимерной пленки;
- изготовление внешнего относительно фронта распространения ЭМИ слоя поглотителя путем нанесения слоем толщиной не более 6,0 мм полимерного связующего вещества на одну из поверхностей стекловолокнистого полотна и равномерного распределения по поверхности этого вещества частиц керамзита с закрепленными на их поверхности частицами активированного угля;
- соединение внутреннего слоя на внешний слой таким образом, чтобы внутренний слой был ориентирован по отношению к внешнему слою поверхностью, на которую нанесено полимерное связующее вещество.

Установлено, что значения коэффициентов отражения и передачи ЭМИ в диапазоне частот 0,7–17,0 ГГц поглотителей ЭМИ, изготовленных в соответствии с представленной методикой, достигают соответственно величин –15,0 дБ и –30,0 дБ, что обусловлено такими механизмами, как рассеяние ЭМИ (как падающего, так и отраженного поверхностью фольгированного материала) на границах раздела слоев поглотителей, а также на частицах керамзита и порошкообразного угля.

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

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ф.Т. Борботько

При построении систем защиты информации важным аспектом является обеспечение мониторинга информационных систем [1], сущность которого заключается в обнаружении и реагировании на инциденты информационной безопасности. Практическая реализация мониторинга возможна с использованием соответствующих программно-технических средств, например, Incident Response Platform.

Incident Response Platform компании R-Vision [2] представляет собой программное обеспечение, предназначенное для агрегации данных об инцидентах из различных источников, их обработки, реагирования на них и координации действий подразделения, которое обеспечивает информационную безопасность в организации. Указанное программное обеспечение позволяет выполнить инвентаризацию активов организации, реализовать объединение в единой базе данных информации от различных средств информационной безопасности (сканеры уязвимостей, антивирусные средства защиты, SIEM системы и т.д.). Ее применение совместно

с программным обеспечением Threat Intelligence Platform которая используется для получения данных о моделях нарушителя (данные кибербразведки), позволяет разработать сценарии реагирования (playbook) на действия нарушителя. Сокращение времени реагирования обеспечивается за счет того, что отдельные этапы в рамках предварительно разработанного сценария реагирования, могут быть выполнены в автоматическом режиме без участия оператора системы. Это в свою очередь, позволяет оптимизировать штат сотрудников, деятельность которых направлена на обнаружение и реагирование на инциденты информационной безопасности.

Литература

1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны. М.: ДМК Пресс, 2020. 326 с.

2. R-Vision IRP / R-Vision [Электронный ресурс]. – 2022. – Режим доступа: https://rvision.ru/products/irp. – Дата доступа: 02.05.2022.

НАДЕЖНОСТЬ И ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ: ПОДХОД К ПОДГОТОВКЕ СПЕЦИАЛИСТОВ

С.М. Боровиков, А.В. Будник

Защита информации в разных сферах деятельности людей во многом определяется надежностью используемых электронных средств. При этом, когда говорят о надежности электронных средств, то обычно понимают отсутствие при их использовании устойчивых отказов, устранение которых предполагает ремонт электронных средств. Методы расчета надежности применительно к таким случаям хорошо рассмотрены в учебной литературе [1]. В действительности на защиту информации оказывают некоторое влияние также сбои (вре́менные отказы) электронных устройств, входящих в комплекс технических средств защиты информации. Причинами возникновения сбоев являются воздействия на электронные устройства внешней окружающей среды, проявляющиеся в виде естественных и искусственных помех (молнии, раскаты грома, электромагнитный импульс при включении мощной промышленной установки, преднамеренные действия злоумышленников и т. п.), что проводит к кратковременной потере работоспособности устройств. Поэтому могут иметь место случаи, когда электронное устройство защиты информации, находясь в технически исправном состоянии, из-за сбоя кратковременно не способно выполнять задачу по защите информации. После окончания действия указанных помех работоспособность электронных средств восстанавливается без выполнения ремонта. Не следует также забывать о влиянии человеческого фактора (надежности оператора) на эффект обеспечения защиты информации, например, при мониторинге изображений, получаемых с видеокамер. Учитывая все сказанное, в общем случае лучше говорить об эффективности защиты информации с помощью электронных средств. Эта эффективность определяется надежностью электронных средств с точки зрения отсутствия устойчивых отказов, вероятностями появления сбоев и степенью их влияния на работоспособность электронных средств, а также надежностью оператора. В качестве показателя эффективности может рассматриваться вероятность защиты информации с помощью электронных средств в заданных условиях окружающей среды.

Подход, аналогичный описанному, был реализован применительно к оценке эффективности функционирования электронной системы обеспечения безопасности в некоторых лабораторных работах для студентов специальности «Электронные

системы безопасности» на кафедре проектирования информационно-компьютерных систем БГУИР. В частности, студентам предлагается выполнение лабораторной работы, в которой оценивается эффективность защиты объекта с помощью электронной системы обеспечения безопасности, включающей системы охранной сигнализации и видеонаблюдения [2].

Если изложенный подход к оценке эффективности функционирования электронных средств защиты информации вызвал интерес, то можно обращаться по e-mail: bsm@bsuir.by.

Литература

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

2. Теоретические основы проектирования электронных систем безопасности / С.М. Боровиков [и др.]. Минск: БГУИР, 2014. 70 с.

СИСТЕМА ФИЛЬТРАЦИИ ФИШИНГОВЫХ ПИСЕМ

М.Н. Бычек, Т.В. Борботько

За последние 10 лет появилось множество разновидностей фишинга: фишинг с использованием SMS сообщений – смишинг, голосовой фишинг – вишинг, фишинг беспроводных сетей и др. Самым распространенным все еще остается фишинг с использованием электронной почты. По данными Statista, мировая база пользователей электронной почты достигла 3,9 миллиарда в 2019 году и, как ожидается, достигнет 4,3 миллиарда к 2023 г. Согласно отчету PhishMe research, 91 % кибератак производится с помощью фишинговых электронных писем, причем главными причинами, по которым люди обманываются фишинговыми письмами, являются любопытство (13,7 %), страх (13,4 %) и срочность (13,2 %) [1].

Система фильтрации фишинговых писем включает два подхода:

1. Информирование пользователей о наиболее заметных признаках фишинговых писем, таких, как:

- орфография и грамматика (грамматические и орфографические ошибки – две наиболее распространенные особенности фишинговых писем);
- общее приветствие или поздравление (поскольку фишинговые электронные письма отправляются случайным пользователям, нарушитель не обращается к получателям по имени – особенно, если электронное письмо содержит информацию об учетной записи или другую конфиденциальную информацию);
- вложения с гиперссылками, причем гиперссылка отличается от реальной ссылки [2].

2. Анализ входящей электронной почты программными средствами. В этом случае система анализирует заголовок, тело письма, содержащиеся ссылки и вложения. В частности, ссылки проверяются по множеству признаков, среди которых:

- наличие в ссылке IP-адреса;
- использование в ссылке символа @;
- использование шестнадцатеричных кодов символов;
- количество поддоменов в ссылке;
- возраст связанных доменных имен и др.

Вложения могут быть любого формата. Наиболее опасными являются файлы с расширениями *.bat, *.exe, *.zip, наиболее распространенными – *.xls, *.docx, *.pdf. наличие файлов такого типа является косвенным признаком фишинга. Кроме того, выполняется анализ тела письма на наличие JavaScript или HTML кода.

Литература

1. Sonowal G. Phishing and Communication Channels. A Guide to Identifying and Mitigating Phishing Attacks. Apress, 2022. 230 p.

2. Analysis of phishing emails / L. Burita [et al.] // AIMS Electronics and Electrical Engineering. 2021. Vol. 5, iss. 1. P. 93–116.

КОРРЕКЦИЯ ДВОЙНЫХ НЕЗАВИСИМЫХ И МОДУЛЬНЫХ ОШИБОК ДЛИНЫ ЧЕТЫРЕ БЕЗ ОБЩЕЙ ПРОВЕРКИ НА ЧЕТНОСТЬ ДЛЯ ПОМЕХОУСТОЙЧИВОГО ХРАНЕНИЯ ИНФОРМАЦИИ

Г.А. Власова

При хранении информации в запоминающих устройствах часто происходит ее искажение под воздействием помех. При этом возникают не только независимые ошибки в отдельных битах, но и группирующиеся модульные ошибки, длина которых кратна байту [1]. Эффективным методом коррекции ошибок является использование помехоустойчивых кодов.

Известны реверсивные коды для совместной коррекции одиночных байтов и двойных независимых ошибок, построенные на основе кодов Боуза-Чоудхури-Хоквингема (БЧХ) с кодовым расстоянием шесть [2]. Недостатком данных кодов является наличие разряда общей проверки на четность.

Реверсивный БЧХ-код с кодовым расстоянием пять, позволяет корректировать двойные независимые ошибки и не содержит разряда контроля четности [3]. Можно показать, что перестановкой столбцов проверочной матрицы данного кода, получим код, корректирующий не только двойные, но и все возможные модульные ошибки длины четыре. Алгоритм перестановки столбцов следующий: представим степени ненулевых элементов поля Галуа в виде таблицы, содержащей четыре строки, причем элементы размещены последовательно (1, 2, 3, …, 0) сверху вниз и слева направо (последний столбец неполный и содержит три строки); первую строку полученной таблицы циклически сдвигаем на 2 позиции, а третью строку – на 1 позицию. Элементы первого столбца построенной проверочной матрицы образуют первый модуль, второго столбца– второй модуль и т.д. Правило формирования последних двух модулей зависит от длины кода.

В проверочной матрице полученного кода с дополнительной коррекцией модульных ошибок длины четыре, столбцы верхней подматрицы группируются по рассмотренному правилу, а столбцы нижней подматрицы есть обратные элементы к столбцам верхней. Для предложенного метода формирования проверочной матрицы расчеты показали, что синдромы модульных ошибок веса три и четыре различны и не совпадают с синдромами одиночных и двойных независимых ошибок. Таким образом, построенные коды корректируют не только одиночные и двойные независимые ошибки (как известные реверсивные коды БЧХ с кодовым расстоянием пять), но и дополнительно исправляют одиночные модули ошибок длины четыре. Следует отметить, что перестановка столбцов проверочной матрицы эквивалентна перестановке разрядов кодовой последовательности и не влияет на сложность устройства обработки кода.

Литература

1. Конопелько В.К., Лосев В.В. Надежное хранение информации в полупроводниковых запоминающих устройствах. Москва : Радио и связь, 1986. 240 с.

2. Двоичные реверсивные коды для контроля байтовых ошибок / В.А. Липницкий, [и др.] // Известия национальной академии наук Беларуси. Серия физико-математических наук. 2000. № 1. С.127–131.

3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. Москва: Связь, 1979. 744 с.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ БАНКОМАТОВ, ПЛАТЕЖНЫХ ТЕРМИНАЛОВ САМООБСЛУЖИВАНИЯ, ЭЛЕКТРОННЫХ ДЕПОЗИТАРНЫХ МАШИН ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С.Ю. Воробьёв, Г.В. Мишнев

В государственном стандарте Республики Беларусь «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения» [1] (далее – СТБ 34.101.41-2013) и нормативном правовом акте Национального банка Республики Беларусь, регулирующим сферу обеспечения информационной безопасности банков Республики Беларусь «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения и терминология» [2] (далее – ТТП ИБ 1.1-2020)) отсутствует предписание на обеспечение антивирусной защиты банковского терминального оборудования (банкоматов, информационных платежных терминалов самообслуживания, электронных депозитарных машин и т.п.).

Так, согласно абз. 1 п. 7.5.1 СТБ 34.101.41-2013 «На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты, сертифицированные в национальной системе сертификации либо имеющие положительное заключение государственной экспертизы». Таким образом, требование по установке антивирусного программного обеспечения на терминальное оборудование в вышеуказанном СТБ отсутствует. Абз.1 п. 7.5.1 ТТП ИБ 1.1-2020 фактически дублирует требование стандарта «на всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты».

На практике установка антивируса фактически осуществляется банками-владельцами терминального оборудования «инициативно» по своему усмотрению (при этом необходимо учитывать, что стоимость одной лицензии антивирусного ПО на банкомат существенно дороже стоимости лицензии антивируса на ПЭВМ (сервер)).

Полагаем целесообразным в вышеуказанных СТБ и ТТП дополнить абз. 1 п. 7.5.1 словами «а также терминальном оборудовании» изложив его в следующей редакции: «На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, а также терминальном оборудовании (банкоматах, платежно-справочных терминалах самообслуживания, электронных депозитарных машинах) должны применяться средства антивирусной защиты».

Литература

1. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения = Інфармацыйныя тэхналогіі і бяспека. Забеспячэнне інфармацыйнай бяспекі банкаў Рэспублікі Беларусь. Агульныя палажэнні : СТБ 34.101.41-2013. - Введ. впервые. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2013. 40 с.

2. Технические требования и правила информационной безопасности в банковской деятельности [Электронный ресурс] // Официальный сайт Национального банка Республики Беларусь. Режим доступа: https://www.nbrb.by/legislation/ informationsecurity. – Дата доступа: 12.04.2022.

ТАКТИКА ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ МНОГОЭТАЖНЫХ ГАРАЖЕЙ-СТОЯНОК

В.Е. Галузо, О.В. Калита, А.И. Пинаев

Согласно [1] помещения хранения автомобилей в гаражах–стоянках (ГС) закрытого типа, независимо от показателей подлежат защите спринклерными установками водяного пожаротушения. Кроме того, в соответствии с [1] помещения, оснащенные спринклерными установками пожаротушения (УП), не требуется оборудовать системами пожарной сигнализации (СПС) в случае, если они должны оборудоваться тепловыми пожарными извещателями (ТПИ). Согласно приложению П [1] помещения для хранения и обслуживания автомобилей должны оборудоваться ТПИ. Таким образом в ГС закрытого типа спринклерные УП выполняют функции СПС.

В соответствии с [2] систему вытяжной противодымной вентиляции с искусственным побуждением (СДУ) следует предусматривать в помещениях для хранения автомобилей ГС закрытого типа. При этом согласно [2] в зданиях и помещениях, оборудованных СДУ, следует предусматривать автоматическую пожарную сигнализацию или автоматические установки пожаротушения. То есть в ГС закрытого типа СДУ может запускаться от спринклерных УП. В то же время, согласно [2], система оповещения о пожаре в ГС должна запускаться от дымовых ПИ (ДПИ).

Согласно [2], помещения площадью более 3000 м^2, подлежащие оборудованию СДУ, должны быть разделены на дымовые зоны (резервуары дыма) с учетом возможности возникновения пожара в одной из них. Каждую дымовую зону (ДЗ) следует ограждать строительными конструкциями и (или) стационарными (опускаемыми) вертикальными завесами (далее – завесами) из материалов группы горючести не ниже Г1, выступающими с потолка (перекрытия, покрытия) к полу, но не ниже чем 2 м от пола, образующими под потолком (перекрытием, покрытием) резервуары дыма. Минимальную глубину дымовой зоны (резервуара дыма) следует принимать 0,5 м. Согласно [3] время заполнения такого резервуара дыма составило 258 с.

Время сработки ДПИ на практике не более 80 с [3]. А это значит, что от сработки ДПИ и запуска СОП до заполнения резервуара дыма пройдет около трех минут. Расстояние от наиболее удаленной точки ДЗ до ее края не превышает 30 м. При скорости эвакуации в горизонтальной плоскости ГС равной 60м/мин это расстояние может быть преодолено за 30 с. То есть эвакуация из ДЗ произойдет до заполнения резервуара дыма, а значит СДУ для обеспечения эвакуации не нужна.

В многоэтажных ГС каждый этаж отделяется от других этажей препятствующими распространению пожара противопожарными дверями (шторами), которые закрываются при сработке СПС. Запуск СДУ от сработки спринклерной УП не обеспечит удаление продуктов горения из ДЗ из-за отсутствия притока воздух. И это имеет положительный эффект, который заключается в том, что отсутствие притока

и движения больших объемов воздуха (около 50000 $м^3$/ч согласно расчетам) не будет способствовать горению и не изменит карты орошения УП.

Предлагается запуск СДУ делать вручную (как это делается в случае газового тушения) по прибытии пожарного расчета, что будет способствовать его эффективной работе, а не автоматически от сработки спринклерной УП.

Литература

1. СН 2.02.03-2019 Пожарная автоматика зданий и сооружений.

2. СН 2.02.07-2020 Противодымная защита зданий и сооружений при пожаре. Системы вентиляции.

3. Хорошко В.В. Эффективность электронных систем пожарной безопасности в зоне горения автомобилей для подземных гаражей-стоянок жилых зданий // Доклады БГУИР. 2020. № 18(7). С. 63–70.

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

А.Н. Гамова

На сегодняшний день известно сравнительно небольшое число криптосистем с открытым ключом, причем к ним зачастую предъявляются претензии, как ввиду их малой скорости работы, так и по поводу недостаточного обоснования их стойкости. В основании стойкости таких систем обычно лежит вычислительная трудность решения некоторой задачи для какой-то алгебраической системы, чаще всего с элементами числовой природы. В подавляющем большинстве случаев это или задача факторизации больших чисел, или задача дискретного логарифмирования в циклической группе. Еще более печальны перспективы указанных криптосистем в случае появления квантового компьютера, работающего с тысячами кубит. Поиск же других алгебраических систем, применимых в криптографии с открытым ключом в постквантовом мире, является трудной задачей и требует вовлечения в криптографический обиход новых математических объектов. В этой связи стоит обратить особое внимание на клеточные автоматы, которые представляют собой некоммутативные алгебраические структуры, распараллеленность которых позволяет увеличивать скорость работы и пропускную способность аппаратных реализаций криптоалгоритмов. Эволюция КА развертывается в дискретном пространстве, состоящем из клеток. Законы эволюции локальны, т.е. динамика системы задается неизменным набором правил, по которым осуществляется вычисление нового состояния клеток в зависимости от состояния окружающих ее соседей. Эта смена состояний происходит одновременно и параллельно, а время идет дискретно. Несмотря на простоту построения, КА могут демонстрировать разнообразное и сложное поведение, что дает возможность использовать КА в моделировании природных систем и физических процессов, а также и для генерации случайных чисел. В классических клеточных автоматах набор ячеек представляется в виде упорядоченного множества, элементы которого располагаются в узлах *n*-мерной решетки (наибольшее распространение получили автоматы с одно-, двух- и трехмерными решетками). Кроме того, для классических клеточных автоматов выполняются свойства однородности и локальности. Однородность означает, что все ячейки клеточного автомата являются неразличимы ми по своим свойствам: для них используются одни и те же правила переходов и одинаковые способы выбора окрестности. В окрестность каждой ячейки входит подмножество ячеек, удаленных от данной на расстояние не более заданного и, возможно, она сама. Одной из основных проблем при использовании клеточных

автоматов в генераторах псевдослучайных последовательностей является непредсказуемость их периода в силу нелинейности функции переходов. При этом лавинный эффект позволяет гарантировать, что период последовательности внутренних состояний клеточных автоматов не меньше периода выходной последовательности регистра сдвига. Начальные значения ячеек памяти регистра сдвига также являются ключом выработки псевдослучайной последовательности генератора в целом, т. е. определяют выбор конкретной последовательности из множества возможных.

Литература

1. Ефремова А.А., Гамова А.Н. Самопрограммируемые клеточные автоматы в криптографии // Прикладная дискретная математика. 2017. № 10. С. 76–81.

ПРОЕКТ ПРОГРАММНОГО СРЕДСТВА ОПТИМИЗАЦИИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С УЧЕТОМ ДАННЫХ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В.А. Герасимов, Л.Л. Утин, А.М. Ахапкина

Выбор средств защиты информации для нейтрализации известных угроз является актуальной научной и практической задачей. Основными факторами, влияющими на ее решение, являются непрерывное совершенствование возможностей нарушителей по преодолению систем защиты информации, финансовые ограничения предприятий, внедрение новых информационных технологий и многие другие.

Для анализа известных угроз, как правило, используют информацию банка данных угроз безопасности информации ФСТЭК (БДУ), в котором содержатся данные о наименованнии угрозы безопасности информации, ее идентификатор, краткие сведение, информация об объектах поражения данной угрозой и последствиях. При этом сведения БДУ периодически обновляются.

С целью автоматизации подбора средств защиты информации для нейтрализации известных угроз проводится работа по разработке проекта программного обеспечения по подбору средств защиты, которые могут обеспечить максимально возможное подавление уже известных угроз.

Основными составными частями программы являются база данных угроз и база средств защиты информации, а также модуль аналитических расчетов.

В модуле аналитических расчетов осуществляется назначение весовых коэффициентов каждой угрозе, которую может использовать нарушитель с учетом ущерба, наносимого защищаемой системе. При планировании выбора средств защиты учитывается какие угрозы могут быть нейтрализованы и какой бюджет будет при этом потрачен. В основе аналитических расчетов лежит целевая функция максимизации количества нейтрализуемых угроз при заданных финансовых ограничениях.

В настоящее время проект разработанного программного средства используется для получения аналитических зависимостей в рамках дипломного проектирования и написания магистреской диссертации, но при определенной доработке может быть использован при планировании применения средств защиты информации на предприятиях.

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В АУДИОФАЙЛАХ

А.С. Гераськин, А.С. Конюшенко

Массовое использование цифровых данных вызывает обеспокоенность в защите интеллектуальной собственности, контроле копирования и подтверждении права на обладание данных. Среди технических средств защиты авторских прав на медиаданные наиболее перспективными являются технологии применения средств стеганографии, а именно цифровых водяных знаков. Цифровой водяной знак (ЦВЗ) – это специальная метка, встраиваемая в цифровой контент с целью защиты авторских прав и подтверждения целостности самого документа.

ЦВЗ можно встраивать в электронные документы любого типа. В работе рассматривается внедрение текстовой и графической информации в аудиосигналы методом изменения времени задержки эхосигнала. Его идея основана на особенности человеческого слухового аппарата: если подряд идут сильный и слабый сигналы, то при прослушивании сильный сигнал маскирует слабый. Чаще всего, звук в пространстве передается таким образом, что до слушателя доходит и направленный звук и множество различных эхо с задержками. Слуховая система человека приспособлена отфильтровывать эхосигналы, особенно короткие.

В данном методе создаются искусственные эхосигналы, имеющие ту же структуру, что и естественные. Следовательно, слышимость и возможность извлечения встроенных данных напрямую зависит от исходного сигнала. Водяные знаки на основе эхосигналов не слышны в звуке, в котором мы обычно различаем множество эхосигналов, и наоборот, слышны в ситуациях, когда наш слух не привык к наличию эхосигналов.

Внедрение представляет собой следующий алгоритм. Аудиофайл делится на некоторое количество частей, равное количеству внедряемых бит. Создаются сигналы для кодирования 0 и 1, а также переключающие сигналы. Далее обрабатывается каждая часть аудиофайла, встраивая бит, на выход будет подаваться сигнал с задержкой 0 или 1. Причем гарантируется плавный переход между участками аудио благодаря переключающим сигналам.

Была разработана программа, реализующая предлагаемый алгоритм. Также был проведен анализ эффективности внедрения цифрового водяного знака, найдены основные параметры: отношение сигнал/шум, интенсивность битовых ошибок, субъективная оценка качества звука. Из полученных данных можно сделать вывод, что при внедрении в аудиофайл цифрового водяного знака методом изменения времени задержки эхосигнала искажения при прослушивании значительны. Метод не устойчив к сжатию, однако он сохраняет большую часть внедренной информации при использовании частотных фильтров.

Литература

1. Иваненко В.Г. Родченко С.В. Встраивание цифровых водяных знаков в аудиосигналы // Безопасность информационных технологий. 2011. № 1. С. 94–95.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. Салон-Пресс, 2009. 265 с.

3. Столов Е.Л. Цифровая обработка сигналов. Водяные знаки в аудиофайлах. Учебное пособие. Лань, 2018. 176 с.

ИССЛЕДОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ВСТРОЕННЫХ МЕТОДОМ DEW, НА УСТОЙЧИВОСТЬ К ОПРЕДЕЛЕННЫМ ВИДАМ АТАК

А.С. Гераськин, А.А. Шуликина, А.А. Лукьянова

Развитие компьютерных технологий придали новый импульс развитию и совершенствованию нового направления в области защиты информации – компьютерной стеганографии. Одна из областей применения методов компьютерной стеганографии, которые получили широкое распространение, стали методы встраивание цифровых водяных знаков (ЦВЗ) и цифровых отпечатков пальцев, предназначенных для защиты авторских и имущественных прав на цифровую информацию различного рода.

Современные системы компьютерной стеганографии используют в качестве контейнеров растровые графические изображения различных форматов. Самое широкое распространение в последнее время получил формат JPEG.

Существует множество методов, основанных на внедрение ЦВЗ в коэффициенты матрицы дискретно-косинусного преобразования (ДКП). Наиболее интересным является метод дифференциального встраивания энергии (DEW). Его идея заключается в выборочном отбрасывании части высокочастотных коэффициентов ДКП изображений и видеоизображений, в которые можно осуществить встраивание дифференциального энергетического водяного знака [1].

Целью данной работы является исследование ЦВЗ, встроенных методом DEW, на устойчивость к определенным видам атак. Для достижения этой цели было разработано программное обеспечение, которое проводило атаки на базу, содержащую изображения с ЦВЗ, встроенными методом DEW. Были реализованы следующие группы атак: атаки, направленные на удаление ЦВЗ; геометрические атаки; криптографические атаки и атаки против используемого протокола.

Для оценки устойчивости цифрового водяного знака применялись коэффициент Пирсона и подсчет процента побитового совпадения между внедренным и извлеченным ЦВЗ.

В процессе анализа устойчивости ЦВЗ встроенных методом DEW к атакам были получены следующие результаты: Геометрические атаки: обрезка – коэффициент Пирсона ≈0.5; масштабирование – коэффициент Пирсона < 0,1; поворот – коэффициент Пирсона ≈0..5.

Статистические атаки: сжатие – коэффициент Пирсона >= 0,5; шумоподавление – коэффициент Пирсона >0.3; внесение шума – коэффициент Пирсона > 0,5. Внедрение нового ЦВЗ – коэффициент Пирсона > 0,5.

На основе полученных результатов, был сделан вывод, что метод DEW можно считать в достаточной мере устойчивым ко многим видам воздействий на контейнер. Однако, в результате исследования был сделан вывод: для повышения эффективности, методы встраивания ЦВЗ нужно осуществлять в области средних частот, а не высоких, что повысит устойчивость ЦВЗ.

Литература

1. Иваненко В.Г., Ушаков Н.В. Защита изображений формата JPEG при помощи цифровых водяных знаков // Безопасность информационных технологий. 2018. № 2. С. 106–113.

УСТРОЙСТВО АВАРИЙНОЙ СИГНАЛИЗАЦИИ ДЛЯ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ ТЕПЛОСЕТЕЙ ОБЪЕКТОВ ВОЕННОГО НАЗНАЧЕНИЯ

А.О. Гирко, Д.С. Шарак

Необходимость разработки данного устройства обусловлена тем, что качество работы образцов вооружения, военной и специальной техники (ВВСТ) во многом зависит от влажностно-температурного режима внутри помещений. При слишком низких или высоких значений температуры личный состав начнет отвлекаться от выполнения своих функциональных обязанностей. ВВСТ, в свою очередь, от перегрева или переохлаждения может давать сбой, вследствие чего задача по предназначению может быть не выполнена. В то же время простота элементной базы и разрабатываемой схемы, а также относительно небольшая цена используемых элементов позволят быстро производить ремонт и обеспечит возможность широкого применения подобных устройств.

Исходя из проведенного анализа стоимости и характеристиках в качестве среды разработки была выбрана Arduino IDE, которая используется для программирования контроллеров на базе Arduino. Проведенный анализ микроконтроллеров позволил выбрать микроконтроллер Arduino UNO для проектирования устройства исходя из его низкой стоимости, при довольно широких возможностях, простоты использования и программирования. В начале производится запуск устройства аварийной сигнализации путем подключения его к источнику питания (выполнено с помощью USB-кабеля). Далее происходит настройка порога срабатывания датчиков, путем вращения ручки, изменяющей сопротивление, на каждом датчике, до получения требуемых параметров. После установки порогов срабатывания аварийной сигнализации происходит считывание показаний датчиков температуры и влажности, после чего полученные данные отправляются на микроконтроллер. Полученные показания сравниваются и проверяются на превышение порога.

Если показания датчиков не превышают порога, то цикл повторяется и происходит дальнейшее считывание и сравнение показаний до момента превышения порога. В случае превышения допустимого порога происходит срабатывание пьезоэлемента и на LCD дисплей выводится сообщение и срабатывает аварийная сигнализация, что является предупреждением о критическом состоянии объекта либо аварии на нем. В случае нажатия кнопки сброса показания дисплея, дисплей вернется в исходное состояние и выключится (дисплей включается только при срабатывании датчиков). Работа системы аварийной сигнализации является циклической и не выключается, пока не будет лишена источника питания. Разработанное устройство аварийной сигнализации рабочего места оперативного дежурного может получить широкое применение как в гражданской, так и в военной сферах. Применение его в ВВС и ВПВО значительно сократит затраты на закупку дорогостоящих систем. Ввиду доступности элементной базы возможно в кротчайшие сроки начать их производство.

Устройство позволяет контролировать состояние теплосетей и служебных помещений, своевременно получать сигнал об аварии на объекте, производить настройку порогов срабатывания аварийной сигнализации. Данное устройство является удобным и простым в использовании, так как дает возможность визуального наблюдения за параметрами теплосети и звукового оповещения при аварии на объекте. Данное устройство может быть применено для охраны складов, служебных, режимных и других помещений, требующих охраны или за которыми нужны отдельные виды контроля.

МЕТОД НЕЧЕТКИХ МНОЖЕСТВ КАК СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ

К.Ю. Гиро, В.А. Федоренко

Сегодня одним из наиболее перспективных направлений научных исследований в области анализа, моделирования и прогнозирования слабо структурированных процессов и явлений являются нечеткая логика и математический аппарат теории нечетких множеств. Механизм нечеткого логического вывода, позволяет объективно отражать причинно-следственные связи между слабо структурированными и/или вовсе неструктурированными характеристиками, более адекватен процессу выявления информационных угроз на самой ранней стадии, «пластично» учитывает особенности потенциальных атак.

Теория нечетких множеств хорошо согласуется с условиями моделирования систем защиты, так как многие исходные данные моделирования (например, характеристики угроз и отдельных механизмов защиты) не являются строго определенными. Одним из главных преимуществ нечеткого моделирования является его способность к быстрой адаптации на предмет решения новых классов информационных угроз. На основе базовых лингвистических правил создается так называемая «грубая» нечеткая модель, которая в условиях эксплуатации системы информационной защиты и программной симуляции может быть скорректирована и представлена второй моделью. Далее, в процессе эксплуатации пользователь этой модели может обнаружить новые закономерности и взаимосвязи и, тем самым, трансформировать ее в более адекватную причинно-следственную связь. Процесс адаптации нечеткой модели является итерационным и длится ровно столько, сколько необходимо шагов для идентификации новых параметров, обеспечивавших адекватное сходство с реальными векторами признаков информационных угроз.

Выделяют 3 этапа формирования нечетких множеств угрозы информационной безопасности.

Этап 1. Формирование модели угроз, определение взаимосвязи между угрозами и рисками информационной безопасности.

Этап 2. Построение функций принадлежности начальных нечетких множеств уровня ущерба информационной системе.

Этап 3. Построение обобщенного нечеткого множества уровня воздействия класса угроз на информационную систему.

Достоинства метода:

- не использует аппарат теории вероятностей в силу отсутствия реальной статистики воздействия угроз;
- не применяет процедуру оценки степени соответствия информационной системы определенному набору требований по обеспечению информационной безопасности, что может быть весьма дорогой процедурой для предприятия.

Таким образом, учитывая все достоинства и особенности метода, математический аппарат нечеткой логики является адекватным инструментом для решения задач информационной безопасности [1, 2].

Литература

1. Асланов К.Дж. Построение интеллектуальных интегрированных систем информационной безопасности в открытых корпоративных сетях: диссертация / Азербайджанский государственный университет экономики. Баку, 2018. 92 с.

2. Дубинин Е.А. Методика получения нечеткого множества уровня воздействия класса угроз на информационную систему // Информационно-управляющие системы. 2006. № 5. С. 76–80.

АНАЛИЗ ОПЫТА БОЕВОГО ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ, ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ МАЛОРАЗМЕРНЫМ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ В БЛИЖНЕЙ ТАКТИЧЕСКОЙ ЗОНЕ

В.Ю. Горшанов

Беспилотный летательный аппарат (БЛА) – летательный аппарат без экипажа на борту самолетного либо вертолетного типа, управляемых по каналу связи или по заранее заложенной на борту программе [1].

Основные задачи, решаемые БЛА в ходе боевых действий [2, 3]:

- ведение наблюдения и разведки, в том числе и в реальном масштабе времени;
- радиационная, химическая и биологическая разведка местности;
- нанесения ударов по целям, самостоятельно (барражирующий боеприпас, также дрон-камикадзе) или носимыми средствами поражения;
- применение средств РЭБ, постановка радиоэлектронных помех;
- целеуказания для других средств поражения, а также корректировка их применения;
- транспортировка и доставка грузов в заданный район;
- ретрансляция данных между удаленными абонентами сетей связи;
- применения БЛА в качестве ложных целей.

Лица ведущие противозаконную деятельность, а также незаконные вооруженные формирования преимущественно используют малоразмерные БЛА для решения следующего ряда задач [3]: доступ за периметр охраняемых объектов и ведение там наблюдения, точное уничтожение отдельных важных лиц, заброска самодельных средств поражения, нанесение повреждений объектам инфраструктуры и транспортным средствам, препятствование воздушному движению в аэропортах.

Для адекватной оценки эффективности применения БЛА в различных условиях обстановки рассмотрим основные недостатки БЛА [2]: ограничения по применению в зависимости от времени суток и погодных условии для отдельных категорий БЛА, низкая автономность, низкая скрытность каналов управления и передачи информации, низкая живучесть конструкции, высокая подверженность каналов управления и передачи информации, а также каналов спутниковой навигации воздействию радиоэлектронных помех, ограничения по массе и составу полезной нагрузки, сравнительно небольшая дальность действия дистанционного управления БЛА с пункта управления при отсутствии дополнительных средств ретрансляции.

Таким образом на современном этапе БЛА способны решать широкий спектр боевых задач, выполнять задачи полностью автономно по заранее заложенной программе, или при дистанционном управлении оператором, с большой степенью эффективности.

Литература

1. Авиация: Энциклопедия / под ред. Г.П. Свищёв. М.: Большая Российская энциклопедия, 1994. 736 с.

2. Еремин Г.В., Гаврилов А.Д., Назарчук И.И. Малоразмерные беспилотники – новая проблема для ПВО // Отвага. 29.01.2015. 6 (14). [Электронный ресурс]. – Режим доступа: https://otvaga2004.ru/armiya-i-vpk/armiya-i-vpk-vzglyad/malorazmernye-bespilotniki/. Дата доступа: 04.04.2022.

3. К вопросу борьбы с незаконным использованием беспилотных летательных аппаратов коммерческого типа / Р.В. Аниськов [и др.] // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 9–10 (111–112). С. 71–75.

САМОСТОЯТЕЛЬНАЯ РАБОТА – ОСНОВА ПОВЫШЕНИЯ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ

М.С. Гурский

В настоящее время стремление человека к познанию, умению самостоятельно учиться становится основным критерием успешности образовательной системы. К сожалению, в средней школе на это обращается очень мало внимания и будущие студенты в своем большинстве не имеют навыков поиска, сбора, анализа и обобщения полезной информации. Отсюда очевидна важная функция высшего образования – приобщение студента к самообразованию с тем, чтобы он сам свободно определял направление своего умственного труда, имел возможность выбора и обоснования принятого решения.

Сегодня мало кто станет сомневаться в том, что традиционный метод обучения изжил себя. В условиях этого метода роль преподавателя чрезвычайно сужена, т. к. его основная задача – донести до студента побольше сведений по программе курса, при этом студент выступает в качестве пассивного слушателя. Такая технология обучения формирует особый тип личности – интеллектуального потребителя. В этой односторонней модели учебного процесса студент всегда только объект обучения, он никогда не приобретет вкус к самостоятельному познанию, творчеству, не научится учиться. Поэтому в высшей школе необходима кардинальная перестройка технологии обучения – переход к объемной модели учебного процесса, включающей: преподавателя, студента, изучаемую дисциплину, средства обучения. При этом акцент переносится на самостоятельную работу студента, методическую работу преподавателя, их сотрудничество в процессе консультаций и, по возможности, уменьшение аудиторных занятий. Активизировать познавательную деятельность студентов также позволяют интерактивные методы обучения.

Ныне в учебном процессе есть возможность применять модели дистанционного обучения, методы контроля и самоконтроля знаний при помощи компьютерных технологий, а также осуществлять индивидуальную связь между студентом и преподавателем. Ведь базовые знания, навыки и умения у студентов формируются в процессе самостоятельного обучения более глубоко, чем в процессе аудиторных занятий. Сегодня преподаватель выступает не только в своей традиционной роли источника знаний, но и является советчиком, организатором, консультантом и, естественно, контролирует процесс усвоения знаний Оптимально организованный текущий и итоговый контроль является своеобразным стимулом в учебе, выступает в качестве обучающей функции, способствующей равномерному распределению самостоятельной работы студента на протяжении всего семестра. Особенно важно для контроля индивидуальное собеседование «преподаватель – студент». Такое собеседование активизирует самостоятельную работу студентов, воспитывает целеустремленность, настойчивость в овладении программным материалом. Самостоятельная работа дает возможность снизить негативный эффект таких индивидуальных особенностей студентов, как инертность, неспособность распределять внимание, самостоятельно выбирать время, темп работы, носители информации.

В заключение следует подчеркнуть, что самостоятельная работа представляет собой особую учебно-познавательную деятельность, средство повышения творческой активности и профессионального мастерства с помощью выполнения различных заданий по решению учебно-творческих, научно-исследовательских задач с применением современных технологий обучения.

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ПЛАТФОРМЫ CTFd ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

Т.Н. Гуцко, А.Ю. Суботковская

Capture the Flag или CTF в подготовке специалистов по кибербезопасности – это соревнования в форме командной игры. Участники решают прикладные задачи, чтобы получить уникальную комбинацию символов (флаг). Далее участники отправляют флаг в специальную форму и получают подтверждение, что задача решена верно или стоит попытаться дать ответ еще раз. CTF-турниры традиционно проводятся в двух форматах: в формате Task-Based (или Jeopardy), когда игрокам предоставляется набор заданий, к которым требуется найти и отправить ответ. Или в формате Classic (или Attack-Defense), когда участники получают идентичные серверы с набором уязвимых сервисов, на которых необходимо найти приватную информацию – флаги.

Надо отметить, что если в условиях проведения CTF-соревнований говорить о нарушениях не приходится, то при попытке использовать CTF в учебном процессе отмечаются постоянные нарушения академических требований – использования чужих флагов, передача решений другим участникам, несанкционированная коллективная работа и прочее, что не позволяет получить адекватную картину усвоения студентами материала и формирования у них необходимых компетенций.

Решением данной проблемы стал пакет на языке Python, используемый для анализа базы данных платформы CTFd и методика его применения с целью анализа работы академической группы и поиска инцидентов нарушения академических требований учебного процесса. База данных платформы представлена в виде файлов в json-формате. Основные данные, используемые для анализа, связаны с активностью участников и включают идентификаторы участника и его команды, задачи и время отправки флага, ip-адрес участника, сам флаг. Важные характеристики анализа: выбор периода рабочего времени, приоритет задач, динамика работы и пр.

Использование пакета предоставило преподавателю инструмент для анализа хода и динамики учебного процесса, а также подтвердило существенное повышение уровня сознательности и ответственности обучаемых. Платформа CTFd развернута с 2021 г. на платформе облачного кластера Гродненского государственного университета им. Янки Купалы (http://ctf.mf.grsu.by).

СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЧЕБНОГО ПРОЦЕССА В РАМКАХ ПРОЕКТА COURSERA FOR CAMPUS

Т.Н. Гуцко, А.Ю. Суботковская

С 2019 года ГрГУ им. Янки Купалы является участником проекта Coursera for Campus, реализуемого крупнейшей в мире платформой дистанционного обучения Coursera в рамках ее политики в условиях пандемии COVID-19. Наряду с бесплатным доступом к более чем 4000 программам удаленного обучения, проект предоставляет доступ к средствам и сервисам контроля использования учебных ресурсов и средствам администрирования, встроенные в платформу Coursera for Campus. Однако упомянутые сервисы ориентированы либо на отдельных обучаемых, либо на все сообщество студентов, работающих в рамках проекта. Возможность контролировать работу студенческой группы, в случае необходимости, должна быть реализована дополнительными средствами. Очевидно, что возможности, предоставляемые в рамках проекта Coursera for Campus, недостаточны для мониторинга требований таких категорий как «безопасность учебного процесса», «академическая честность», интерес к которым несоизмеримо вырос в условиях дистанционного и гибридного обучения.

В докладе представлен пакет скриптов для контроля хода учебного процесса в условиях гибридного обучения на основе анализа базы данных платформы Coursera for Campus и методика его использования с целью изучения работы академической группы и поиска инцидентов нарушения академических требований учебного процесса.

Стандартная аналитика платформы построена на фильтрации LOG-файла активностей студентов и не позволяет работать с сущностью «учебная группа». Допустимы выборки, группировка данных и агрегирование по изучаемым программам и времени активностей. Среди стандартных информационных панелей: успеваемость ученика; еженедельный прогресс; информация по изучаемым программам. База данных платформы представлена в виде файлов в csv-формате. Цели анализа могут быть сформированы преподавателем самостоятельно и практически не ограничены. К примеру, может быть оценено оптимальное для студентов время проведения самостоятельной работы, определены кластеры студентов, предпочитающих «корпоративное обучение», на основании количества и времени попыток, затраченных на прохождение тестов, определены недобросовестные студенты и т. д. Использование разработанных средств контроля показало их эффективность как при организации управляемой самостоятельной работы студентов, так и в режиме полностью самостоятельной работы учащихся.

ОБНАРУЖЕНИЕ АППАРАТНЫХ СРЕДСТВ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ

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

В работе рассматриваются критерии принятия решений при проверке вычислительной техники на наличие недекларированных возможностей (НДВ), которые могут использоваться нарушителем. При проверке предлагается проводить контроль теплового поля проверяемого объекта и отдельных его элементов при внешнем провоцирующем электромагнитном и акустическом воздействиях.

При описании процесса проверки объекта на наличие НДВ можно использовать два состояния проверяемого объекта: H_0 – отсутствие НДВ и H_1 – наличие НДВ. В соответствии с состояниями объекта H_0 и H_1 вероятностями их будут P_0 и P_1.

При принятии решений необходимо учитывать и стоимости потерь и затрат. C_{00} и C_{11} – затраты при правильных решениях об отсутствии и наличии НДВ соответственно. C_{01} – потери при ошибке, когда НДВ отсутствует, а принимается решение о его наличии и C_{10} – потери при ошибке, когда НДВ присутствует, а принимается решение о его отсутствии, что иногда называется пропуском цели. Первый случай называют ошибкой первого рода, а второй – ошибкой второго рода.

Одним из возможных вариантов принятия решений является использование критерия оптимальности Байеса. Основой байесовского подхода к проблемам обнаружения является использование показателей потерь. При этом обычно правильным решениям соответствует нулевой размер штрафа. Решение принимается на основании минимума средних потерь.

Одним из существенных недостатков байесовского правила обнаружения сигналов является большое количество априорной информации о потерях и вероятностях состояния объекта, которая должна быть в распоряжении наблюдателя. Этот недостаток проявляется при проверке вычислительной техники на наличие НДВ, когда указать априорные вероятности наличия НДВ и величины потерь за счет ложной тревоги или пропуска цели оказывается весьма затруднительным. Поэтому для такого типа задач вместо байесовского критерия используется критерий Неймана-Пирсона [1]. Согласно этому критерию выбирается такое правило обнаружения, которое

обеспечивает минимальную величину вероятности пропуска НДВ (максимальную вероятность правильного обнаружения) при условии, что вероятность ложной тревоги не превышает заданной пороговой величины. Таким образом, оптимальное, в смысле критерия Неймана-Пирсона, правило обнаружения минимизирует величину пропуска НДВ в зависимости от вариации видов провоцирующих воздействий и алгоритмов обработки теплового поля проверяемого объекта.

Литература

1. Ивановский Р.И. Теория вероятностей и математическая статистика. Основы, прикладные аспекты с примерами и задачами в среде Mathcad. СПб: БХВ-Петербург, 2008. 528 с.

МЕДИАВИРУСНОЕ ЗАРАЖЕНИЕ КАК ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНЫХ СИСТЕМ В УСЛОВИЯХ КОРОНАКРИЗИСА

А.Г. Давыдовский

В условиях пандемии COVID-19 важной проблемой информационной безопасности социальных систем является выяснение механизмов влияния интенсивности и тематической специфики поисковой активности интернет-пользователей на распространение коронавирусной инфекции.

В этой связи осуществлен сценарный анализ связей заболеваемости COVID-19 и поисковой активности интернет-пользователей в период очередной волны пандемии на основе впервые разработанных биоинспирированных алгоритмов квазимолекулярного синтеза сценариев (БАКСС) динамики временных рядов.

Тематические тезаурусы были сформированы с использованием web-сервиса контекстной рекламы портала Google (https://ads.google.com), общедоступных сервисов Wordstat.Yandex.by (https://wordstat.yandex.by) и GoogleTrends.com (https://trends.google.ru) были собраны данные за период в период с января 2020 г. по апреля 2022 г. На основе БАКСС выполнен сценарный анализ динамики временных рядов поисковых обращений интернет-пользователей по COVID-19-ассоциированной тематике в русскоязычном сегменте Сети в локации Республики Беларусь совместно с данными о заболеваемости и смертности от COVID-19 от Всемирной организации здравоохранения [1]. Аппроксимация на период прогнозирования до 12 мес. с момента исследования осуществлена с помощью искусственной нейросети в среде программирования Mathlab. Установлена корреляция между прогнозируемыми временными рядами частотой поисковых обращений интернет-пользователей по COVID-19-тематике и новых случаев заболеваемости, смертности и вакцинации.

Распространение информации COVID-19-тематике в сообществ интернет-пользователей [2] осуществляется по механизмам медиавирусного заражения (МВЗ) благодаря тому, что медиапространство интернет является активной социотехнической средой с диффузионными и квазиупругими свойствами, где медиавирусы распространяются подобно гармоническим, резонирующим или затухающим колебаниям: $D\frac{d^2n}{dz^2}-\alpha(f-g)\frac{dt}{dz}-\beta\left(\frac{df}{dz}-\frac{dg}{dz}\right)n=0,\ z=\gamma\Delta\tau N\sum_{i=1}^{N}C_i\sum_{j=1}^{M}M_j$, где n – количество медиапользователей, подверженных влиянию МВЗ; z – функция связи между интернет-пользователями (N), числом связей, образуемых каждым из них, по передаются сообщения (M_j) в течение периода времени $\Delta\tau$; γ – средний показатель пропускной способности каждого медиаканала; D – коэффициент МВЗ зависимый

от свойств медиасреды; f – функция интенсивности медиазаражения; g – функция ограничения медиазаражения; α и β – коэффициенты.

Таким образом, МВЗ способны вызывать инфодемию в интернет-сообществах, нарушать информационную безопасность социальных систем, механизмы индивидуального и коллективного иммунитета и, как следствие, усугубляют последствия коронакризиса, а зачастую индуцируют новую волну пандемии COVID-19.

Литература

1. WHO Coronavirus (COVID-19) Dashboard. – [Электронный ресурс]. – Режим доступа: https://covid19.who.int/. – Дата доступа: 16.03.2022.

2. Левчук Н.Н. Принцип медиавируса в процессе коммуникативного взаимодействия // Веснік Беларускага дзяржаўнага універсітэта. Серыя 4, Філалогія. Журналістыка. Педагогіка. 2009. № 3. С. 96–100.

ЗАЩИТА ИНФОРМАЦИИ В УСТРОЙСТВАХ ИНТЕРНЕТА ВЕЩЕЙ, МАТРИЦА РИСКОВ

Н.Ю. Дашко, С.П. Способ

Информационные технологии являются неотъемлемой частью жизни человека на сегодняшний день. Данные технологии работают на базе использования множества средств и методов сбора, обработки, а также передачи данных с целью получения информации необходимого качества и состоянии какого-либо объекта, процесса или явления. С стремлением за улучшением качества жизни человека, повышением ее безопасности и автоматизации бытовых и иных задач сформировался «Интернет вещей». Это сеть, состоящая из взаимосвязанных физических объектов (вещей) или устройств, которые имеют встроенные датчики, а также программного обеспечения, позволяющего осуществлять передачу и обмен данными между физическим миром и компьютерными системами, с помощью использования стандартных протоколов связи. Основная проблема использования сетей IoT заключается в том, что они не имеют защиты от воздействий со стороны злоумышленника. Это может привести, в лучшем случае, к причинению вреда имуществу пользователя, а в худшем – его здоровью и жизни. Например, устройства контроля и управления электрической сетью могут быть захвачены злоумышленником с помощью любого устройства, имеющего доступ к сети Интернет, и соответствующего программного обеспечения. Получив полный или частичный контроль над устройством, злоумышленник может осуществить отключение или порчу электрических приборов, в том числе критически необходимых приборов (систем жизнеобеспечения в больницах, систем мониторинга на производстве, охранных систем и т.д.), создать короткие замыкания в сети и даже вызвать пожар или аварию, если речь идет о производстве.

Универсальным и удобным способ выявления наиболее уязвимых и рискованных мест в сети, например, умного дома является матрица рисков. Матрица представляет из себя таблицу столбцы которой называются «Активы» и строки «Уязвимости». Под активами понимается ресурсы, допустим. Для умного дома – личная жизнь, финансы, личные данные. Оценивая уязвимости можно выявить риск, в том случае, если злоумышленник воспользуется ей и какие это принесет потери активов. Наиболее важные и слабые места выделяются красным, менее желтым или зеленым.

В объемах современного мира трудно на глаз определить риски от взлома того, или иного сетевого узла Вашего дома. Требуется метод, позволяющий комплексно анализировать сеть умного дома и эффективно выявлять наиболее рискованные объекты сети, которые нуждаются в проработки вопросов безопасности

Литература

1. Попов В.Г., Галиаскаров Д.Ф, Гвоздев Л.Б. Актуальность обеспечения информационной безопасности в сетях IoT // StudNet. 2021. № 4.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб: Питер, 2012. 960 с.

ТРЕБОВАНИЯ К СИСТЕМАМ АВАРИЙНОГО ЭЛЕКТРОСНАБЖЕНИЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ ПО ОБЕСПЕЧЕНИЮ ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ

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

Система аварийного электроснабжения (САЭ), осуществляющая электроснабжение потребителей систем безопасности во всех состояниях энергоблока АЭС, включая аварии и обесточивание, играет важную роль в обеспечении безопасности АЭС. Ухудшение качества электроснабжения или его полное отсутствие может привести к разрушению барьеров безопасности АЭС и к загрязнению окружающей среды выше допустимых пределов. Одним из фундаментальных принципов обеспечения безопасности АЭС является нормативное регулирование, в основе которого лежат разработка требований к системам и оборудованию АЭС, отвечающих современному уровню развития технологий, а также контроль их соблюдения. События аварии на АЭС «Фукусима-дайити» в 2011 г., когда в результате землетрясения и цунами произошло полное обесточивание станции, привели к пересмотру в ряде стран регулирующих требований к САЭ.

В докладе представлены результаты сравнительного анализа требований, установленных к САЭ в Республики Беларусь до 2011 года [1, 2], с требованиями в документах МАГАТЭ [3], Российской Федерации [4], Украины [5], которые разработаны с учетом уроков аварии на АЭС «Фукусима-дайити».

Проведенный анализ позволил авторам доклада разработать нормативный правовой акт Республики Беларусь [6], устанавливающий требования к САЭ с учетом современного международного опыта проектирования и эксплуатации АЭС.

Литература

1. НП ЯРБ Общие положения по устройству и эксплуатации САЭ АЭС, утвержденные постановлением МЧС Республики Беларусь от 11.05.2010 № 19 // Использование атомной энергии. Ядерная и радиационная безопасность: сб. норм. прав. актов: в 4 ч. – Минск, Институт радиологии, 2010. – Ч.2. – С. 104–117.

2. НП ЯРБ Правила проектирования САЭ АЭС, утвержденные постановлением МЧС Республики Беларусь от 11.05.2010 № 19 // Использование атомной энергии. Ядерная и радиационная безопасность: сб. норм. прав. актов: в 4 ч. – Минск, Институт радиологии, 2010. – Ч.2. – С. 118–134.

3. Design of Electrical Power Systems for Nuclear Power Plants. IAEA Safety Standards. Specific Safety Guide. № SSG-34. – Vienna, IAEA, 2016. – 122 p.

4. НП-087-11 «Требования к САЭ атомных станций», утвержденные приказом Федеральной службы по экологическому, технологическому и атомному надзору Российской Федерации от 30.11.2011 № 671. [Электронный ресурс]. – Режим доступа: https://docs.secnrs.ru/documents/nps/НП-087-11/НП-087-11_conv.pdf. – Дата доступа: 22.04.2022.

5. НП 306.2.205-2016. Вимоги до систем електропостачання, важливих для безпеки атомних станцій. Затверджено наказом Державної інспекції ядерного регулювання України від 24.12.2015 № 234. [Электронный ресурс]. – Режим доступа: https://zakon.rada.gov.ua/laws/show/z0078-16#Text (дата обращения: 22.04.2022).

6. Нормы и правила по обеспечению ядерной и радиационной безопасности «Требования к САЭ АЭС», утвержденные постановлением МЧС Республики Беларусь 18.05.2021 № 39. [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=W22136963p&p1=1 (дата обращения: 22.04.2022).

ЭФФЕКТЫ СЛАБОЙ ЛОКАЛИЗАЦИИ В ТОПОЛОГИЧЕСКИХ ИЗОЛЯТОРАХ

В.А. Зайцев

Необычные свойства поверхностных электронов топологических изоляторов делают их чрезвычайно перспективными для создания устройств по спиновому транспорту, например, по инжекции и детектированию спин-поляризованных электронов. В топологических изоляторах (ТИ), как показывают экспериментальные данные, наблюдается качественно различное поведение магнитосопротивления (МС). МС может уменьшаться, носить экстремальный характер, а также увеличиваться при различных плотностях тока через ТИ. С учетом общей тенденции смены зависимостей МС при повышении плотности тока, имеющиеся экспериментальные результаты связывают с проявлением эффектов слабой локализации, действием магнитного поля, а также влиянием спин-зависимых процессов, таких как спин-орбитальное рассеяние, рассеяние на парамагнитных примесях [1, 2].

Вклад слабой локализации в проводимость определяется временем сбоя фазы из-за неупругих процессов и рассеяния с переворотом спина. Сбой фазы (дефазировка) характеризуется временем, вклад в которое вносят такие процессы, как электрон-электронное рассеяние, рассеяние на фононах, рассеяние на парамагнитных примесях с взаимным (электрона и примеси) переворотом спина. В магнитном поле разрушается интерференционная добавка, что ведет к уменьшению квантовой поправки, т. е. к увеличению проводимости. Это объясняется подавлением в магнитном поле когерентности сопряженных волн. В большинстве случаев в слабой локализации преобладает МС, которое возникает из-за дефазировки когерентного обратного рассеяния, вызывающего слабую локализацию. Магнитные примеси двояко влияют на МС: прямой вклад из-за полевой зависимости рассеяния с переворотом спина и косвенный вклад от расфазировки волновой функции электрона с переворотом спина. Спин-орбитальное взаимодействие (СОВ) приводит к перевороту спина электрона проводимости при упругом рассеянии, при этом интерференционная картина слабой локализации усложняется за счет перемешивания спиновых состояний.

Расчеты квантовых поправок в ТИ основаны на HLN модели [3] для 2D электронных систем, учитывающей различные механизмы рассеяния. Важность учета конкурирующих эффектов, особенно влияния спин-орбитального рассеяния и рассеяния на парамагнитных примесях, обусловлена имеющимися экспериментальными данными для широкого круга материалов. Проведенные расчеты показали, что величина и знак квантовой поправки в зависимости от напряженности магнитного поля определяются соотношением времени спин-орбитального рассеяния и времени дефазировки, а время рассеяния на парамагнитных примесях вносит корректирующий вклад. Установлено, что если время спин-орбитального рассеяния много больше времени дефазировки, то вклад СОВ мал и квантовая поправка положительная, а магнитное поле ведет к подавлению слабой локализации, увеличивая проводимость. С усилением СОВ и уменьшением времени спин-орбитального рассеяния зависимость квантовой поправки от напряженности магнитного поля сначала становится немонотонной, а затем переходит в область отрицательных величин. При этом снижается проводимость и возникает положительное МС.

Литература

1. Bergmann G. Weak localization in thin films: a time-of-flight experiment with conduction electrons // Physics Reports. 1984. Vol. 107 (1). P. 1–58.
2. F. Rortais [et al.]. Spin-orbit coupling induced by bismuth doping in silicon thin films // Appl. Phys. Lett. 2018. Vol. 113. P. 122408.
3. Hikami S., Larkin A.I., Nagaoka Y. Spin-Orbit Interaction and Magnetoresistance in the Two Dimensional Random System // Prog. Theor. Phys. 1980. Vol. 63. P. 707–710.

ПРОБЛЕМА ПЕРЕДИСКРЕТИЗАЦИИ В ЗВУКОВЫХ ГЕНЕРАТОРАХ

И.В. Закерничный, А.Ю. Клюцкий

Подавляющее большинство интегральных схем (ИС) операторных звуковых генераторов с цифровым аудиовыходом подразумевают мгновенное преобразование сигнала в аналоговую форму. При этом используются нестандартные частоты дискретизации, являющиеся непригодными для дальнейшей цифровой передачи и обработки сигнала [1]. Авторами предложен метод решения данной проблемы, который заключается во внедрении блока преобразования частоты дискретизации (передискретизации) выходного сигнала в систему формирования аудиосигналов, построенную на базе ИС операторного звукового генератора. Такой метод позволяет получить аудиосигнал любой стандартной частоты дискретизации одновременно нескольких различных спецификаций в соответствии с конфигурацией гибко настраиваемого блока передискретизатора, а также избежать использования лишних вычислительных мощностей при дальнейшей работе с сигналом на персональном компьютере, а при отсутствии такой необходимости позволяет вовсе исключить обработку сигнала на более сложном и уязвимом аппаратном и программном обеспечении персонального компьютера и передавать информационный поток в стандартной форме непосредственно на принимающее устройство. Реализация рассмотренной методики осуществлялась с помощью ИС серии SRC43. К преимуществам данной серии микросхем можно отнести наличие интегрированного интерфейса S/PDIF, что делает возможным передачу аудиопотока по волоконно-оптическим линиям связи для минимизации шансов утечки информации по каналу побочных электромагнитных излучений [2].

Литература

1. Yamaha LSI Data Book Ongen-hen : Dētabukku Ongen-hen Catalog No. 7610002 1994.10. Yamaha Corporation, 1994. 343 p.
2. SRC4392 Two-Channel, Asynchronous Sample Rate Converter with Integrated Digital Audio Interface Receiver and Transmitter: Datasheet. Texas Instruments Incorporated, 2012. 93 p.

ИЗМЕРИТЕЛЬНЫЙ СМЕСИТЕЛЬ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

И.А. Захаров, О.А. Карманова, А.В. Гусинский

Особое место в области радиоэлектроники занимают вопросы создания и применения радиоэлектронных СВЧ-систем и устройств, в том числе сантиметрового, миллиметрового, а в последние годы и субмиллиметрового диапазонов волн. При создании подобных систем используют разнообразные СВЧ-устройства и их соединения. Исследования характеристик и параметров СВЧ-устройств при их создании

и проверка соответствия таких устройств спецификационным требованиям при производственном выпуске, а также многие другие задачи и исследования требуют соответствующих средств инструментального анализа СВЧ-устройств и их соединений.

Многообразие используемых в СВЧ-диапазонах типов устройств обуславливает многообразие параметров и характеристик, описывающих их свойства и требующих экспериментального определения. Это в свою очередь приводит к необходимости решения разнообразных измерительных задач, что возможно с помощью соответствующих измерительных средств. Парк, существующих и создаваемых измерительных средств весьма велик, так как должен обеспечивать измерения всех параметров и характеристик СВЧ-устройств, интересующих разработчиков систем и других потребителей, в различных частотных диапазонах и для разных используемых типов линий передач [1]. В современной аппаратуре можно обнаружить множество смесительных каскадов. Они известны как устройства, которые, при подаче на них сигналов двух частот, дают дополнительные сигналы, равные по частотам сумме и разности подаваемых на смеситель сигналов. Одна из вновь образованных компонент выделяется настроенным полосовым фильтром (резонансным контуром) и подается для обработки далее. Не следует забывать, что остальные компоненты, как входные, так и полученные, также, присутствуют в той или иной степени в выходном сигнале смесителя, они никуда не девались, а просто были уменьшены по амплитуде при селекции. (Следует отметить, что входные сигналы, будучи поданными на нелинейное устройство, каким является смеситель, образуют собственные гармоники, которые тоже взаимодействуют, как между собой, так и с исходными сигналами, подаваемыми на смеситель, получаемые суммарные и разностные сигналы, взаимодействуют как друг с другом, так и с исходными сигналами, их гармониками и комбинационными сигналами, полученными в результате взаимодействия уже вторичных сигналов: каждый сигнал взаимодействует с каждым, давая все новые и новые частоты, так что на выходе нелинейного смесителя присутствует целый спектр частот с разными амплитудами.

Также смесители широко применяются в генераторах сигналов СВЧ-диапазона, а также в векторных и скалярных анализаторах цепей, и в другой измерительной технике. Для создания смесителей необходимо провести моделирование схемы смесителя, решить задачи согласования нелинейных элементов с волноводной линией передач, разработать конструкцию и изготовить смеситель. Для определения его параметров и технических характеристик необходимо разработать методики их исследования и с использованием этих методик провести исследование характеристик и параметров смесителя.

Литература

1. Белоус А.И., Мерданов М.К., Шведов С.В. СВЧ-электроника в системах радиолокации и связи. Техническая энциклопедия издание 2-е, дополненное. М.: Техносфера, 2018.

К ВОПРОСУ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В МОБИЛЬНЫХ ПЕРЕГОВОРНЫХ КАБИНАХ

О.Б. Зельманский, Е.О. Кауфман, К.П. Шакин

В настоящее время одной из проблем сотрудников, работающих в офисах в стиле Open Space, где рабочие места расположены рядом, является офисный шум, мешающий сосредоточится, а также провести переговоры или телефонный разговор. Установлено, что устранение шума и обеспечение работников отдельным рабочим помещением позволяет повысить работоспособность, увеличить скорость выполнения

задач, снизить утомляемость. Для решения данной проблемы разработаны и с успехом применяются звукоизолированные мобильные переговорные кабины, которые позволяют сотрудникам работать в комфортных акустических условиях без необходимости переоборудования офиса [1]. В то же время актуальной задачей остается защита речевой информации от утечки по акустическим и вибрационным каналам за пределы кабины, так как в переговорной кабине может проводится конфиденциальный разговор. Для решения данной задачи предлагается оборудование переговорной кабины модулем активной акустической маскировки [2], содержащим акустические и вибрационные излучатели, устанавливаемые вентиляционные каналы и интегрируемые в корпус и дверь кабины соответственно. Предлагаемый модуль генерирует сложный маскирующий сигнал, состоящий из белого шума и речеподобного сигнала, что снижает вероятность обнаружения и распознавание конфиденциальной речевой информации. Значения отношения «белый шум» / речеподобный установлены эмпирически исходя из экспериментальных исследований. В результате оценки эффективности и достаточности мер защиты от утечки информации по акустическим и виброакустическим каналам посредством осуществления инструментального контроля установлено, что эффективность защиты переговорной кабины, оборудованной модулем активной акустической маскировки, соответствует требованиям нормативных правовых актов по защите объектов от утечки информации по акустическому и виброакустическому каналам, словесная разборчивость не превышает 0,19.

Литература

1. Офисные кабины для переговоров [Электронный ресурс]. – Режим доступа: https://vc.ru/office/199045-10-dizaynerskih-ofisnyh-kabin-dlya-peregovorov. – Дата доступа: 04.05.2022.

2. Шакин К.П., Зельманский О.Б. Модуль синтеза речеподобного сигнала для защиты акустической информации // Материалы XVIII Международной научно-практической конференции «Управление информационными ресурсами», Минск, 10 марта 2022 г. С. 265–268.

СИСТЕМА ЗАЩИТЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ОТ АКТИВНЫХ АТАК ПЕРЕХВАТА УПРАВЛЕНИЯ ПОСРЕДСТВОМ GPS-НАВИГАЦИИ

А.В. Казак

Перехват управления беспилотных летательных аппаратов (БПЛА) путем отправки ложных данных системы GPS – один из самых распространенных и сложных одновременно видов электронной атак на БПЛА. Итогом такой атаки, проведенной с использованием современного оборудования, может быть, как минимум, отклонение от курса и вылет за нужный квадрат, а в худшем случае – отказ всех необходимых датчиков. Беспилотные летательные аппараты находят широкое применение в различных областях, в любой из которых, перехват является нежелательным или недопустимым. Зачастую, возможность реализации подобного рода атак определяется уязвимостями каналов управления. Но чаще всего это связано со стандартными протоколами обмена данными между оператором и БПЛА, а также БПЛА и спутником GPS.

Существующие на сегодняшний день методы противодействия подобного рода атакам нельзя считать высокоэффективными. В качестве методов борьбы с «GPS-Spoofing» рассматривают системы криптографии, а также применение средств помехоустойчивости кодирования с использованием управляемых перестановок,

позволяющих на коротком отрезке времени осуществлять маскировку истинной структуры сигнала [1]. Также существуют методы с использованием коротких сегментов дынных GPS-приемника и методы, которые позволяют изменять положение антенны с определенной частотой [2].

Предлагается новый альтернативный подход к проблеме защиты БПЛА от «GPS Spoofing» и подобного рода активных атак перехвата управлением аппаратом, который заключается в реализации, так называемой, Системы Альтернативного Ориентирования (САО). Принцип работы данной системы базируется на математическом вычислении положения БПЛА относительного последних данных, полученных от GPS-спутника до начала разрыва соединения при попытке реализации атаки типа «GPS Spoofing» и изменении его курса по записанному ранее маршруту. Система благодаря наличию специфических датчиков определяет значения скорости, направления, высоты и других критичных параметров управления БПЛА и на основании этого производит математический расчет пройденного пути, записывая это на внутреннюю карту местности. Представленный метод может обеспечить защиту БПЛА от атаки типа «GPS Spoofing», безопасно перенаправить аппарат в ближайшую заданную ранее точку пройденного маршрута до момента восстановления соединения с оператором. В отличие от известных методов, предложенная система незначительно повышает стоимость БПЛА, его массу и не усложняет его конструкцию.

Литература

1. Навроцкий Д.А. Система защиты радиоканалов БПЛА от несанкционированного вмешательства // Национальная ассоциация ученых. Технические науки. 2015. № III (8). С. 95–99.

2. Spoofed' GPS signals can be countered, researchers show [Электронный ресурс]. – Режим доступа: https://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attack. – Дата доступа: 2.05.2022.

АНАЛИЗ АКТИВНЫХ АТАК НА БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ

А.В. Казак, Г.А. Пухир

Современный этап развития беспилотных летательных аппаратов (БПЛА), которые применяются в различных сферах не только в гражданской области, но и для военного назначения, порождает проблемы безопасности БПЛА, как связанные с возможностью перехвата самих устройств злоумышленниками, так и с обеспечением безопасного воздушного пространства в условиях применения БПЛА. Беспилотные летательные аппараты – это летательные аппараты без экипажа, которые управляются дистанционно (например, с земли или с другого воздушного судна) или при помощи другого автономного программного обеспечения, установленного на борту [1]. Принцип управления БПЛА строится на связи между оператором и самим БПЛА.

Существующие методы противодействия БПЛА делятся на два типа: контактные и бесконтактные. Контактными методами являются методы, которые влияют кинетически на сам БПЛА. Примерами контактного противодействия являются противодроны, сети, кинетическое оружие и обученные животные. В связи с разнообразием задач, выполняемых БПЛА в различных климатических условиях и местах базирования, во время боевого дежурства и на траектории полета по условиям эксплуатации БПЛА могут подвергаться прямому электромагнитному воздействию [2]. Кроме этого необходимо учесть, что сегодня в мире существует реальная угроза воздействия на БПЛА различных преднамеренных деструктивных электромагнитных

воздействий, например, посредством сверхкороткоимпульсного электромагнитного излучения, что можно отнести к бесконтактным методам противодействия БПЛА.

Также существует возможность перехвата управления беспилотным летательным аппаратом третьими лицами. Одним из существующих методов перехвата является GPS Spoofing [3]. Данный принцип строиться на замещении сигнала GPS, который передается от спутника до БПЛА, за счет более мощного сигнала от ретранслятора третьего лица. Реализация этого способа перехвата довольно проста, что делает данную угрозу весьма вероятной.

Литература

1. Павлов А.М. Принципы организации бортовых вычислительных систем перспективных летательных аппаратов // Мир компьютерной автоматизации. 2001. № 4.

2. Комягин С.И., Соколов А.Б. Требование по стойкости радиоэлектронной аппаратуры летательных аппаратов в условиях воздействия электростатических разрядов // Технологии электромагнитной совместимости. 2008. № 2. С. 3–8.

3. Можно ли защититься от атак на GPS? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/gps-spoofing-protection/22674/. – Дата доступа: 2.05.2022.

МЕТОДИКА ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ ПО ИНФОРМАТИВНЫМ ПАРАМЕТРАМ

В.О. Казючиц

Рассматриваемая методика использует подход к прогнозированию работоспособности полупроводниковых приборов, описанный в [1]. Прогнозирование надежности выполняется в виде распознавания класса с точки зрения работоспособности экземпляра для заданной наработки: класс работоспособных экземпляров или класс неработоспособных экземпляров. Прогнозирование основано на использовании информативных параметров, выбор которых может быть сделан по результатам предварительных исследований полупроводниковых приборов интересующего типа [2]. Методика предназначена для применения ее к полупроводниковым приборам, прошедших выходной контроль в условиях производства и признанных годными к использованию в составе электронной аппаратуры. Использование методики позволит формировать выборки однотипных полупроводниковых приборов повышенного уровня надежности (класс работоспособных экземпляров для заданной наработки).

Для принятия решения о классе работоспособности экземпляра для заданной наработки, используя информативные параметры, измеренные у экземпляра в начальный момент времени, необходимо иметь модель прогнозирования. Получение модели является составной частью методики и включает следующие этапы:

- формирование обучающей выборки;
- измерение у каждого экземпляра обучающей выборки значений информативных параметров в начальный момент времени;
- проведение обучающего эксперимента в виде ускоренных испытаний на наработку экземпляров обучающей выборки в течение времени, эквивалентного заданной наработке с точки зрения надежности;
- получение модели прогнозирования.

Полученная модель прогнозирования может быть использована для определения класса работоспособности для заданной наработки других однотипных экземпляров, т.е. тех экземпляров, которые не принимали участия в обучающем эксперименте.

Методика была применена для прогнозирования уровня надежности (класса работоспособности для заданной наработки) партии транзисторов большой мощности типа КП744А. Исследования показали, что для получения результатов прогнозирования, отвечающим по достоверности целям практики, достаточно использование 2…4 информативных параметров.

Литература

1. Казючиц В.О., Боровиков С.М., Шнейдеров Е.Н. Эвристическая модель прогнозирования работоспособности полупроводниковых приборов // Доклады БГУИР. 2022. Т. 20, № 1. С. 92–100.

2. Казючиц В.О., Боровиков С.М., Шнейдеров Е.Н. Выбор информативных параметров для прогнозирования индивидуальной надежности полупроводниковых приборов // Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 50–51.

МОДЕЛИРОВАНИЕ ПОСТЕПЕННЫХ ОТКАЗОВ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРИЧЕСКИХ НАГРУЗОК В КАЧЕСТВЕ ИМИТАЦИОННОГО ВОЗДЕЙСТВИЯ

Е.В. Калита, А.И. Бересневич

Биполярные транзисторы большой мощности в немалой степени определяют надежность электронных устройств защиты информации. Известно [1], что примерно 80 процентов отказов полупроводниковых приборов являются постепенными, поэтому обеспечению надежности биполярных транзисторов по постепенным отказам необходимо уделять особое внимание. Одним из способов обеспечения требуемой надежности биполярных транзисторов по постепенным отказам является индивидуальный отбор экземпляров, используя метод имитационных воздействий [2]. Метод включает два этапа. Первый этап – это выбор имитационного воздействия, моделирующего изменение электрического функционального параметра транзистора для заданной наработки, и получение с помощью предварительных исследований транзисторов интересующего типа имитационной модели в виде функции связи наработки со значением имитационного воздействия. Второй этап – это применение имитационной модели для прогнозирования постепенных отказов тех однотипных экземпляров, которые не принимали участия в предварительных исследованиях. Для этого по модели рассчитывают уровень воздействия, имитирующего изменение параметра для заданной наработки, и у экземпляра измеряют значение электрического параметра при этом найденном имитационном уровне воздействия. Результат измерения рассматривается в качестве прогноза электрического функционального параметра для заданной наработки, что позволяет принять решение о надежности экземпляра по постепенному отказу в будущем (для заданной наработки).

В работе в качестве имитационного воздействия, моделирующего изменения электрического функционального параметра биполярных транзисторов большой мощности типа КТ872А, был выбран такой параметр электрической нагрузки как ток коллектора. С помощью экспериментальных исследований выборки транзисторов объемом 100 экземпляров получена усредненная экспериментальная зависимость электрического функционального параметра (напряжения коллектор–эмиттер) от тока коллектора транзистора [2]. Затем для этой выборки транзисторов были проведены ускоренные испытания на длительную наработку и по результатам этих испытаний получена усредненная экспериментальная зависимость напряжения коллектор–эмиттер от наработки. Использование этих двух экспериментальных зависимостей позволило

получить имитационную модель в виде функции пересчета наработки на имитационное значение тока коллектора. Имитационная модель может быть применена для индивидуального прогнозирования значения напряжения коллектор–эмиттер для любых интересующих наработок применительно к однотипным экземплярам, не участвовавшим в описанных экспериментальных исследованиях. Использование тока коллектора в качестве имитационного воздействия позволило более оперативно выполнять прогнозирование значения электрического параметра и, следовательно, постепенных отказов транзисторов, нежели в случае использования температуры в роли такого воздействия.

Литература

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

2. Боровиков С.М., Калита Е.В., Бересневич А.И. Моделирование электрического параметра транзисторов при прогнозировании их надежности методом имитационных воздействий // Интернаука. 2022. № 7-2 (230). С. 25–30.

ПРОГНОЗИРОВАНИЕ НАДЕЖНОСТИ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ БОЛЬШОЙ МОЩНОСТИ ДЛЯ ЭЛЕКТРОННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛИТЕЛЬНОГО ФУНКЦИОНИРОВАНИЯ

Е.В. Калита, А.И. Бересневич, С.М. Боровиков

Эффективность защиты информации в разных сферах деятельности людей во многом определяется надежностью используемых электронных средств. Биполярные транзисторы большой мощности широко используются в электрических схемах управления, импульсных источниках питания и других функциональных частях электронных средств защиты информации и от их надежности по постепенным отказам во многом зависит работоспособность электронных устройств при длительном их функционировании. Одним из способов обеспечения требуемой надежности биполярных транзисторов по постепенным отказам является их индивидуальный отбор методом имитационных воздействий [1]. Суть метода состоит в выборе подходящего имитационного воздействия и получении с помощью предварительных исследований транзисторов интересующего типа имитационной модели в виде функции связи наработки с уровнем имитационного воздействия. Применение имитационной модели сводится к определению по модели значения имитационного воздействия, соответствующего заданной длительной наработке, и дальнейшему измерению у конкретного нового однотипного экземпляра значения электрического функционального параметра при рассчитанном уровне имитационного воздействия. Под «новыми» однотипными экземплярами понимают те экземпляры, которые не принимали участия в предварительных исследованиях – обучающем эксперименте. Результат измерения считают прогнозом электрического функционального параметра данного экземпляра для заданной наработки. С учетом прогноза принимают решение о соответствии или несоответствии данного экземпляра требованию надежности транзисторов по постепенным отказам. Традиционно в качестве имитационного воздействия вначале используют температуру. Исследования показали [2], что использование температуры имеет ряд существенных недостатков. Поэтому актуальным является выбор других, более эффективных имитационных воздействий. В качестве такого воздействия предлагается использовать ток коллектора транзисторов или напряжение коллектор–эмиттер. При этом следует различать рабочий ток коллектора (рабочее напряжение коллектор–эмиттер) при использовании транзистора

в электрической схеме электронного устройства и имитационный ток коллектора (имитационное напряжение коллектор–эмиттер). Имитационный ток (или напряжение) используется только для получения информации о значении электрического функционального параметра конкретного экземпляра для заданной наработки, т. е. в конечном итоге прогноз значению электрического параметра конкретного экземпляра дают по реакции этого параметра на рассчитанное имитационное значение тока коллектора (напряжения на коллекторе).

Заинтересованные организации могут обращаться по e-mail: bsm@bsuir.by.

Литература

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

2. Калита Е.В., Бересневич А.И., Боровиков С.М. Выбор имитационных факторов для моделирования постепенных отказов биполярных транзисторов большой мощности // Материалы XXVI Международной научно-технической конференции «Современные средства связи», Минск, 21–22 октября 2021 г. С. 247–248.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

О.В. Калита

Еще 30 лет назад все проектирование систем производилось исключительно с помощью ручного труда. Компьютеризация внесла свои коррективы и в эту сферу деятельности. Проектировщики постепенно перешли от работы на кульманах к работе за ЭВМ. Одной из первых программ стала выпущенная в 1982 году Autocad. В 1989 появилась первая версия nanoCAD. До недавнего времени для проектирования систем защиты информации: будь то система видеонаблюдения, система контроля управления доступом или система охранной сигнализации хватало программ, помогающих проектировать в 2D-формате. Однако, время вносит свои коррективы. В последние 20 лет подрядчики и архитекторы стали все чаще использовать информационное моделирование зданий для сокращения конфликтов, расчета комплексных спецификаций материалов и получения красивых изображений в 3D, что позволяет совершенствовать сферу проектирования и строительства зданий. На рынке появились программы типа Revit.

В настоящее время проектировщик это уже не просто инженер, умеющий проектировать системы. Это еще и специалист, освоивший программы для проектирования не только в 2D, но и в 3D. Самая большая проблема для организаций по проектированию инженерных систем, пытающихся перейти от 2D-программ (в частности, таких, как AutoCAD) к BIM в 3D, – это кадры. Старшее поколение инженеров работает в 2D-программах на протяжении двадцати и более лет, и они, разумеется, не горят желанием изучать новые программы. Однако, как ни странно, более молодому поколению инженеров по проектированию инженерных систем еще не преподают использование программ для BIM в учебных заведениях.

Как следствие, если раньше подготовка специалистов велась в основном в области изучения нормативно-правовых актов, оборудования, то в настоящее время все больше времени занимает «программная» часть: изучение программ для проектирования систем. Задача ВУЗа в нынешних реалиях выпустить специалиста, обладающего знаниями в области не только проектирования систем, но и успешно освоившего программы для проектирования систем. Одним из преимуществ изучения программных комплексов в стенах ВУЗа является лучшая «усваиваемость» материала: при изучении

на обучающих семинарах, за столом в конференц-залах усваивается не так уж много знаний о сложном программном средстве.

Литература

1. Талапов В.В. Технология BIM. Суть и особенности внедрения информационного моделирования зданий. М.: ДМК Пресс, 2015. 410 с.

2. Преимущества Revit для подготовки BIM модели. – [Электронный ресурс]. – Режим доступа: https://infars.ru/blog/preimuschestva-revit-dlya-podgotovki-bim-modeli/. – Дата доступа: 11.04.2022.

АППАРАТНЫЕ ЗАКЛАДКИ В ИНТЕГРАЛЬНЫХ МИКРОСХЕМАХ

О.А. Карманова, И.А. Захаров, В.Р. Стемпицкий

Стремление обеспечения максимальной скорости обработки информации при минимальных массогабаритных параметрах, помехоустойчивости, наталкивается на все больше проблем, связанных с достижением оптимальных свойств конструкций современных интегральных радиоэлектронных устройств (ИРЭУ) и соответствием действующим нормам обеспечения безопасного их использования, бессбойного функционирование устройства. Одной из угрозы безопасной эксплуатации электронного оборудования является не санкционированная или не документированная модификация интегральных схем.

Модификации интегральных схем (ИС), именуемые аппаратными закладками (АЗ), – это устройство скрытно устанавливаемое (внедряемое, встраиваемое) или подключаемое к элементам информационной системы (ТС обработки и передачи информации) в целях получения несанкционированного доступа к информации (т. е. в нужный момент времени обеспечить утечку информации, нарушение ее целостности или блокирование. К остальным элементам, которое способно вмешаться в работу системы [1, с. 16].

Аппаратной закладкой может быть специальная микросхема, выполняющая те же функции, что и программная закладка. Одним из видов аппаратных закладок является радиозакладка. С помощью аппаратной закладки могут перехватываться видеоизображение, выводимое на экран монитора; информация, вводимая с клавиатуры, выводимая на принтер, записываемая на жесткий диск компьютера; записываемая на внешние накопители (flesh-память, USB-накопитель, DVD. CD и др.) [1, с. 16–17].

Вредоносное действие аппаратных закладок является серьезной проблемой безопасности электронных устройств, особенно, если речь идет о выполнении критически важных задач государственного уровня. Несанкционированные аппаратные закладки могут привести к катастрофическим последствиям во время эксплуатации приложений с повышенными требованиями к информационной безопасности, например, в военных структурах, в коммуникационных и национальных инфраструктурах.

Результатом работы аппаратной закладки может быть, как полное выведение системы из строя, так и нарушение ее нормального функционирования, ее изменение или блокирование. Данные ИС могут, также, стать объектами умышленных манипуляций [2, с. 450]. В данной работе авторы исследуют существующие угрозы распространяющихся уязвимых аппаратных компонентов с внедренными в них уязвимостями – аппаратными закладками (аппаратными троянами) в интегральные микросхемы. Систематизируют классификации аппаратных закладок, способы их внедрения, методы выявления и защиты интегральных микросхем от несанкционированного вмешательства.

Литература

1. Дождиков В.Г., Салтан, М.И. Краткий энциклопедический словарь по информационной безопасности. М.: Энергия, 2010. 240 с.

2. Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия. Книга 2. М.: Техносфера, 2019. 630 с.

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ АНАЛИЗА ДАННЫХ СИСТЕМЫ «УМНЫЙ ДОМ»

М.И. Карпейчик, И.О. Сидоренков, Г.В. Юдин

Интернет вещей (Internet of Things, IoT) – концепция сети передачи данных между физическими объектами («вещами»), оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. Считается, что организация таких сетей способна перестроить экономические и общественные процессы, исключить из части действий и операций необходимость участия человека. Одна из самых популярных и многообещающих сфер использования IoT – «Умный дом», предполагающий интеграцию умных вещей, которые выполняют повседневные домашние функции, в том числе, носимых гаджетов, в единую экосистему. На данный момент в качестве главной проблемы IoT рассматривается его уязвимость к кибератакам. В то же время вопросам безопасности и комфорта человека, как элемента экосистемы и потребителя услуг умного дома, уделяется недостаточное внимание.

В докладе представлен взгляд на «Умный дом» – не просто как на пространство, в котором можно управлять шторами, холодильником, лампочками и др. «Умный дом», использующий IoT и достижения Data Science, рассматривается как генератор ценных данных, которые непрямую влияют на качество жизни и привычки домовладельца. В то же время, простая интеграция IoT-устройств в рамках «Умного дома» не позволяет убедиться в истинной ценности таких проектов. Требуется нечто большее.

На примере программной платформы с открытым кодом Home Assistant представлена бизнес-модель интеграции устройств «Умного дома», сбора и анализа данных о работе IoT-устройств, формирования управляющих воздействий на экосистему и привычки домовладельца. Основным источником данных является база данных платформы Home Assistant в формате СУБД SQLite. Разработан пакет скриптов для анализа базы и управления IoT-устройствами, мониторинга привычек и состояния домовладельца, формирования обратной связи для элементов экосистемы.

Очевидно, что бизнес-модели, которые формируют и анализируют информацию, особенно те, которые объединяют личные данные и информацию из нескольких источников, должны уделять большое внимание таким вопросам, как согласие потребителей, обучение и безопасность данных, а разработчики продуктов должны учитывать возможность внешнего аудита собираемой и используемой информации.

РЕАЛИЗАЦИЯ SSL СЕРТИФИКАТА В МЕССЕНДЖЕРЕ

Карпов Г.И.

В наши дни сеть Интернет объединяет более сотни миллионов людей по всему миру. Большую часть информации мы получают благодаря различным информационным ресурсам, мессенджерам и многому другому. Каждый день сотни миллионов людей используют различные сайты для передачи и поиска информации. Основное человеческое общение переместилось в сеть Интернет, что не могло сказаться на личной безопасности

каждого. Для сохранения и защиты данных в любых сервисах используются различные методы и инструменты, которые с большой долей вероятности помогают нам доверить информацию о себе им и защититься от будущих хакерских атак. Всем известно, что сертификаты обеспечивают безопасное соединение клиента с сервером, в данной курсовой работе демонстрируется подход, который был реализован как программное обеспечение шифрования на сокетах в сетях с помощью SSL-сертификата, использующего отечественный метод симметрического шифрования [1, с. 3–18].

Для реализации клиент-серверного приложения с SSL сертификатом необходим сервер, который генерирует секрет (большое число 256 бит) с помощь отдельной написанной функции, которая в последствии будет использоваться для шифра и делит его на n частей (*n* – частей зависит от количества клиентов в чате), и отправляет части этого секрета, разделенного по схеме Асмута-Блума клиентам. Первый пользователь, который подключается к серверу задает число *m* клиентов наличие которых необходимо для восстановления секрета, а также для последующей проверки количества клиентов на сервере, то есть, если *m* не равно числу клиентов на сервере, то соединение обрывается автоматически.

Далее рассмотрим взаимодействие подключение клиентов к серверу. Клиент посылает серверу запрос на присоединение. Сервер отправляет клиенту свой сертификат. Далее клиент его проверяет на подлинность. Если проверка прошла успешно, то взаимодействие продолжается, если нет, то соединение обрывается автоматически. Рассмотрим дальнейшую работу программы при успешной проверке. Клиент отправляет серверу служебную информацию об успешности проверки и сервер в ответ отправляет запрос на долю секрета, в последствии которую будет проверять на подлинность. При успешной проверке секрета клиент генерирует параметры шифра и отправляет серверу свой открытый ключ. После того как сервер получил открытый ключ пользователя он с его помощью шифрует новый ключ и синхропосылку для общения между клиентами и отправляет шифрограмму конкретному клиенту.

Подтверждение подлинности клиентов и сервера произошло, и далее рассмотрим общение между клиентами. На этапе подключения к серверу клиент в случайном порядке выбирает шифр для связи с другими клиентами (Магма, Магма с гаммированием, Магма с гаммированием и обратной связью, кузнечик). С помощью выбранного шифра он шифрует отправленные сообщения и на сервер приходят зашифрованные данные. Далее сервер рассылает их всем клиентам (групповой чат). Получив зашифрованные сообщения, клиенты выбирают по метаданным каким шифром их расшифровать. Таким образом, происходит подключение и обмен сообщениями между клиентами.

Литература

1. Ivan R, Melinda R. Bulletproof SSL and TLS. London, 2015. 530 p.

АНАЛИЗ РАСШИРЕНИЙ ПРОТОКОЛА TLS

А.С. Касьян

Основное назначение протокола TLS – организация защищенных соединений по незащищенной сети. Этот протокол характеризуется следующими свойствами, которые обуславливают его преимущества по сравнению с аналогом (протоколом SSL):

- совместимость (возможность разрабатывать программное обеспечение и библиотеки, которые могут взаимодействовать друг с другом с использованием общих криптографических параметров);

- расширяемость (возможность перехода от криптографических примитивов одного вида к криптографическим примитивам другого вида без необходимости создания новых протоколов);

- эффективность (возможность обеспечения использования протокола при приемлемых затратах на производительность информационной системы).

В настоящее время существуют следующие расширения протокола TLS, с помощью которых можно обеспечивать дополнительные его преимущества: Certificate Transparency, Server Name Indication, Session Ticket, Online Certificate Status Protocol (OCSP) stapling.

Использование расширения Certificate Transparency создает условия для совершенствования инфраструктуры открытых ключей в информационной системе путем ведения учета всех сертификатов общедоступных серверов. При использовании этого расширения центр сертификации при выпуске сертификата отправляет его на общедоступный сервер журналирования, а в ответ получает подписанное электронной цифровой подписью подтверждение внесения информации о сертификате в журнал, называемое Signed Certificate Timestamp.

Использование расширения Server Name Indication предоставляет клиенту возможность указать имя сервера, с которым он хочет установить соединение. Данное расширение обеспечивает поддержку виртуальных защищенных серверов в случае, когда одному IP-адресу соответствует несколько сайтов, каждый из которых имеет свой сертификат.

Использование расширения Session Ticket создает условия для сокращения продолжительности процесса «рукопожатия» между клиентом и сервером, что обусловлено исключением необходимости хранения на сервере информации, требуемой для возобновления ранее завершенного соединения за счет того, что сервер перенаправляет эту информацию клиенту, предварительно зашифровав ее. Такая информация называется «Session Ticket». При необходимости возобновления соединения клиент передает Session Ticket серверу, сервер расшифровывает эту информацию, проверяет ее на предмет целостности и далее использует ее для восстановления соединения.

Расширение OCSP представляет собой протокол, с использованием которого приложения определяют состояние отзыва запрашиваемых сертификатов. Сертификат может быть отозван в случаях нарушения его безопасности (например, компрометация приватного ключа сервера) или истечения его срока действия.

Исходя из результатов проведенного анализа расширений протокола TLS, можно заключить, что эти расширения представляются рациональными для использования в ходе реализации мероприятий по повышению эффективности процессов, направленных на защиту информации, циркулирующей в информационных системах.

СПОСОБ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

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

Оборудование, использующее блочные алгоритмы для шифрования данных с симметричным ключом, появилось достаточно давно. Решения задач шифрования данных с использованием специализированных аппаратных систем значительно увеличивало эффективность систем безопасности по сравнению с комплексами, использующими чисто программные решения, и, не только, за счет повышения производительности системы в целом. Эволюция аппаратных комплексов шифрования определялась в первую очередь элементной базой, используемой для создания

специализированных вычислительных средств. Во вторую очередь – за счет создания более сложных алгоритмов шифрования, в условиях появления элементной базы, позволяющей выполнять аппаратную реализацию новых алгоритмов в условиях конструктивных ограничений. Первые устройства были созданы на элементах малой и средней степени интеграции и отличались относительно низкой производительностью и надежностью. Следующим этапом в эволюции подобного оборудования стало использование заказных больших интегральных схем и серийных микроконтроллеров, что позволило решить ряд задач связанных с компоновкой систем. Коренным образом подход к решению задачи изменился в связи с появлением программируемых логических устройств.

В начале такое оборудование реализовывалось в виде проектов, которые использовали декомпозицию на несколько кристаллов программируемых логических устройств. Далее, с повышением количества элементов в микросхеме те же проекты могли быть реализованы в виде одной микросхемы, и, в дальнейшем занимали только часть микросхемы. В современных условиях эта часть является весьма незначительной. То есть появляется возможность использования все более и более сложных алгоритмов, что приводит к использованию большего количества элементов кристалла и повышению криптографической стойкости, либо появляется возможность увеличения производительности за счет конвейеризации и распараллеливания операционной части аппаратных устройств. Алгоритмы блочного шифрования обычно хорошо распараллеливаются и конвейеризируются, что позволяет легко масштабировать аппаратное решения, но только для тех модификаций алгоритма, которые не используют предыдущий зашифрованных блок для обработки следующего блока.

Для решения практических задачи эффективного использования распараллеливания, путем увеличения одновременно работающих вычислительных ядер внутри кристалла, была осуществлена реализация алгоритма, позволяющая перейти к разделения параллельного потока данных на ряд битовых (последовательных) потоков. Каждый поток шифруется с использованием стандартного алгоритма блочного шифрования. Количество потоков может быть произвольным в пределах ограничения, определяемого размером блока. Сцепление блоков осуществляется в пределах каждого потока, то есть для каждого вычислительного ядра отдельно. Для увеличения криптографической сложности реализуется алгоритм случайной перестановки n потоков, которая может быть получена на базе существующего ключа фиксированного размера согласно выбранного алгоритма. Лучшее решение может быть получено при увеличения эффективной длины ключа на m дополнительных разрядов и реализующего перестановку разрядов согласно дополнительному полю ключа, что, в конечном итоге, позволяет повысить количество вариантов перебора в $n!$ раз. Предложенный способ позволяет эффективно использовать топологию программируемого логического устройства, повысить производительность устройства и увеличить криптографическую сложность алгоритма.

ОЦЕНКА КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ, ВЫРАБАТЫВАЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛИНОЙ 512 БИТ

Н.Г. Киевец, А.М. Ярук

От качества работы генераторов случайных чисел (ГСЧ), используемых для создания криптографических ключей, зависит безопасность передачи зашифрованной информации. В связи с этим задача оценки качества работы ГСЧ является актуальной. Оценка качества работы ГСЧ может выполняться на основе двухуровневого тестирования вырабатываемых генераторами случайных последовательностей (СП) с длинами, равными длинам практически используемых криптографических ключей [1].

В докладе обсуждаются результаты двухуровневого тестирования СП длиной 512 бит, выработанных ГСЧ пяти электронных пластиковых карт (ЭПК) с микроконтроллером К5004 ВЕ2. Двухуровневое тестирование выполнялось по частотному тесту и тесту кумулятивных сумм. Для указанных тестов автором были получены теоретические распределения тестовых статистик для СП длиной 512 бит в соответствии с методикой [2]. Все ГСЧ ЭПК успешно прошли тестирование, что свидетельствует об их высоком качестве работы.

Литература

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

2. Киевец Н.Г., Корзун А.И. Методика нахождения эталонных законов распределения вероятностей, получаемых при статистическом тестировании последовательностей ключей // Доклады БГУИР. 2014. № 5 (83). С. 38–43.

ИНТЕГРИРОВАНИЕ ПРОСТРАНСТВ ВОДОРОДОПОДОБНЫХ АТОМОВ ДЛЯ ЗАДАЧ ПЕРЕДАЧИ ДАННЫХ В КАНАЛАХ СВЯЗИ

И.П. Кобяк

Для решения задач синтеза квантово-электронных каналов криптографической связи предложена модель формирования классического радиуса $\vec{r}_{0,L}$ водородоподобного атома в форме релятивистского пространства ядра. Полученные на основе интегральных преобразований соотношения позволили определить преобразования указанных пространств с учетом перехода значений радиусов через барьер скорости света. Определены теоретические соотношения для радиусов, характеризующие процесс образования релятивистского поля ядра со скоростью $-\vec{v}_{st,L}^{\tau=1}$ в пространстве $\tau = 1$ пятого измерения. Определены принципы перемещения плазменного электрона в центр ядерной оболочки на уровень $r_{st,c}$ – радиуса ядра атома на скорости $\left|\vec{v}_{st,L}^{\tau=1}\right|$ равной $|c+\Delta c|$. Основой для проведения исследований послужила гипотеза о влиянии релятивистских пространств на помехоустойчивость криптографических каналов связи при передаче квантовой информации. В соответствии с поставленной задачей доказана следующая теорема.

Теорема. *Re*-пространственная оболочка ядра атома водорода радиуса $\vec{r}_{st}$ в процессе обретения внешней энергии «струн» является образующим началом для скорости движения электрона по радиусу $\vec{r}_{0,L}$, преобразуемому далее в орбиту ядра $r_{st,c} \to r_{st}$ на скорости $-\vec{v}_{st,L}^{\tau=1} \to -\vec{c}\sqrt{2}$. Для доказательства теоремы рассмотрено влияние процесса изменения радиуса ядра на степень изменения нулевого радиуса $\vec{r}_{0,L}$ с использованием механизма интегрирования соотношения для орбиты ядра. С этой целью флуктуирующий радиус $\vec{r}_{0,L}$ рассмотрен как некоторый граничный радиус не изменяемый в процессе интегрирования. Это позволило установить закономерность формирования скорости $-\vec{v}_{st,L}^{\tau=1}$, воздействующей на электрон в пространстве пятого измерения. Принципиально использование методики интегрирования в данной задаче с общетехнической точки зрения следует считать обоснованной механизмом поглощения энергии изначально твердотельной массой покоя электрона.

ПОДСИСТЕМА МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ КАК СОСТАВНАЯ ЧАСТЬ ОБУЧАЮЩЕГО АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА

А.Н. Коваленко

Обучающие аппаратно-программные комплексы – разновидность инженерно-технических систем, решающих задачи подготовки военнослужащих управлению сложными инженерно-техническими системами, в условиях, для выполнения которых требуются значительные материальные средства.

Одним из элементов обучающего аппаратно-программного комплекса, является подсистема математического моделирования.

Подсистема математического моделирования выполняет функции по отработке введенных преподавателем заданий, по расчету управления и по расчету параметров объекта с учетом управляющих воздействий с определением пространственного положения объекта в виртуальном окружении и расчетом параметров для органов управления.

Для более качественного проведения практических занятий необходимо воспроизводить основные сигналы, получаемые при работе на реальных системах. Для повышения эффективности применения комплекса определяются основные для достижения целей занятия ситуации и объекты, следовательно, в первую очередь детально воспроизводятся именно они.

Оценка эффективности подготовки военнослужащих определяется уровнем полученных знаний, значение которого является положительным, если время, необходимое для достижения определенного уровня подготовки на реальной системе, уменьшается путем получения знаний с использованием комплекса.

Литература

1. Сливина Н.А., Чубров Е.В. Приобретение знаний с использованием учебных и научных пакетов / В кн. «Компьютерные технологии в высшем образовании». М.: Изд-во Моск. ун-та., 2015.

2. Аппаратно-программный учебный комплекс. – [Электронный ресурс]. – Режим доступа: http://bankpatentov.ru/node/479070/. – Дата доступа: 21.03.2022.

3. Решетников В.Н., Мамросенко К.А. Основы построения тренажерно-обучающих систем сложных технических комплексов // Международный научно-практический журнал «Программные продукты и системы». 2011. № 3. С. 86–89.

БЕЗОПАСНОЕ ХРАНЕНИЕ JWT-ТОКЕНА АВТОРИЗАЦИИ В WEB-ПРИЛОЖЕНИЯХ

Т.Е. Козляк

Развитие методов авторизации в web-приложениях породило создания нового стандарта авторизации, основанного на формате JSON, позволяющий создавать JSON Web Token (JWT) токены доступа. JWT – это открытый стандарт для создания токенов доступа, основанный на формате JSON. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует токен для подтверждения своей личности. При использования данного типа токенов возникает вопрос о том, как безопасно хранить токены в публичной части web-приложениях.

В работе рассматриваются основные способы хранения JWT-токена, его виды и способы применения при разработке web-приложений. JWT-токены бывают двух видов. 1. Токены доступа (access-token). Для авторизации запросов и предоставляет

доступ его владельцу к защищенным ресурсам сервера. Имеют короткий срок жизни и может нести в себе дополнительную информацию (например, такую как IP-адрес стороны, запрашивающей данный токен). 2. Токены обновления (refresh-token). Для получения нового токена доступа при истечении срока действия предыдущего токена.

Основные способы хранения JWT Access-токена и проблемы безопасности, которые приходится для них решать, следующие. 1. Local Storage / Session Storage (локальное браузерное хранилище). Преимущества заключаются в его юзабилити, т. к. вся работа с хранилищем происходит довольно просто и на чистом JavaScript. Подвержено XSS-атакам, если подключаются сторонние скрипты, которые могут получить доступ к локальному хранилищу. 2. Cookies (небольшой фрагмент данных, до 4Кб). Преимущества заключаются в более гибкой настройке. Простое хранения Access токена в cookie допускает атаки типа CSRF и XSS. Для защиты, можно воспользоваться параметром Cookie SameSite в режиме Strict, который поможет добиться защиты от CSRF-атаки, путем сокрытия ваших cookie при обращении к api других сайтов. Также есть возможность защититься от XSS-атак путем использования флага httpOnly, а добавление флага Secure поможет защититься от Сниффинга (Sniffer).

Хранение токена в Local Storage было использовано автором при разработке веб-приложения для проведения соревнований по программированию искусственного интеллекта «AI Cup Battle», проводимых кафедрой системного программирования и компьютерной безопасности ГрГУ им. Янки Купалы с 2021 г.

ТЕМПЕРАТУРНАЯ ЗАВИСИМОСТЬ ВЕЛИЧИНЫ БАРЬЕРА ШОТТКИ В ГЕТЕРОПЕРЕХОДЕ ГРАФЕН-КРЕМНИЙ

И.В. Комиссаров, А.В. Данильчик, Н.Г. Ковальчук,
Е.А. Дронина, Е.В. Луценко, С.Л. Прищепа

Фотодетекторы, сформированные на основе гетероперехода графен-кремний, имеют большой потенциал применения, обусловленный как их быстродействием и чувствительностью в широком диапазоне длин волн [1], так и совместимостью с существующими кремниевыми технологиями. Несмотря на значительное количество работ, связанных с этой тематикой, наблюдается определенный пробел в исследованиях, посвященных температурным зависимостям параметров таких гетеропереходов. Изучение электрических характеристик гетеропереходов в широком диапазоне температур открывает перспективы не только расширения диапазона рабочих температур, но и более глубокого понимания фундаментальных принципов работы разрабатываемых фотодетекторов. В данной работе исследовались вольтамперные характеристики, зарегистрированные в темновом режиме гетероперехода графен – *n*-кремний, в диапазоне температур 10–300 К. Детали формирования гетероперехода и геометрии образца можно найти в работе [1]. Полученные экспериментальные зависимости тока от напряжения являются выпрямляющими. Используя стандартную модель вольт амперной характеристики для контакта металл-полупроводник, были определены значения высоты барьера Шоттки (см., например, [2]). Установлено, что высота барьера линейно растет с температурой, с коэффициентом линейности ~ 0,002 эВ/К, и достигает значения ~ 0,65 эВ для комнатной температуры.

Литература

1. Femtosecond light pulse response of photodetectors based on Graphene / n-Si heterojunctions. M. Scagliotti [et al.] // Carbon. 2019. Vol. 152. P. 643–651.

2. Di Bartolomeo A. Graphene Schottky diodes: An experimental review of the rectifying graphene/semiconductor heterojunction // Physics Reports. 2016. Vol. 606. P. 1–58.

АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ ОТ ВНЕШНЕГО ВОЗДЕЙСТВИЯ

Д.В. Куприянова, Ю.И. Некревич, Д.Н. Одинец

На сегодняшний день наиболее распространены в качестве биометрической системы идентификации для мобильных устройств (например, ноутбукам, смартфонам и т.д.) следующие подходы: распознавание лица и анализ отпечатков пальцев. При это сканеры отпечатков нашли особую популярность, т. к. данный подход является относительно быстродействующим из-за того. Существует 3 основных типа сканеров: оптические, емкостные и ультразвуковые, отличающиеся между собой по принципу действия (размещены в порядке появления на рынке). Результаты, представленные в [1, 2], указывают, что каждый из указанных типов может быть «обманут», кроме того, можно предположить, что большинство разработчиков анализируют основные признаки, но не обращают внимание на локальные (это связано с необходимостью максимально быстро отсканировать, обработать и принять решение о соответствии эталону), имеются проблемы с высокой чувствительностью используемых сенсоров и некорректной интерпретацией результатов.

Решениями по устранению выявленных недостатков является применение дополнительных аппаратных и/или программных средств: дополнительная фиксация пульса, фиксация теплового излучения от кожи, программный поиск слишком «идеальных» снимков. В то же время, анализ ситуации показывает, что несмотря на выявленные недостатки, применение отпечатков пальца в качестве биометрической системы идентификации для систем, не связанных с хранением критически важной и/или ограниченной к распространению информации, является вполне приемлемым.

Литература

1. Подделка отпечатков пальцев – можно, но сложно [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/sas2020-fingerprint-cloning/28101. – Дата доступа: 21.04.2022.

2. Подделка отпечатков пальцев [Электронный ресурс]. – Режим доступа: http://www.techportal.ru/glossary/poddelka-otpechatkov-palcev.html. – Дата доступа: 21.04.2022.

ОБОБЩЕННАЯ МОДЕЛЬ СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ НЕЙРОМОДУЛЯ

Д.В. Куприянова, Ю.И. Некревич, Д.Н. Одинец, Д.Ю. Перцев

Система идентификации личности - это одно из высокотехнологичных средств доступа к защищаемой личной информации. По своей природе данные системы могут быть основаны как на биологических признаках (отпечатки пальцев, снимок вен, сетчатки глаза и т. д) так и на технологических (коды, пароли, цифровая подпись и т. д). Предлагается схема обобщенной системы идентификации личности, которая может быть использована при моделировании и тестировании систем защиты информации. В предлагаемой модели измерительная часть и классификатор концептуально разделены. Основу модели составляет нейромодуль, на базе которого реализованы функции

Вычисления уникального вектора признаков личности (например, на основе параметризации значений информативных признаков, вычисления значений взвешенных сумм S и логических минимумов L) [1]. Нейромодуль может быть реализован как в виде спецпроцессора, так и программно. В состав модели также входят следующие компоненты:

- база данных векторов признаков личности;
- измерительная часть, где происходит выбор и измерение значений информативных признаков (например, расстояния между зрачками глаз, расстояний от подбородка до зрачков глаз и т. д.);
- блок формирования вектора значений информативных признаков;
- блок формирования параметров классов;
- идентифицирующая часть, где принимается решение об идентификации личности.

Система идентификации личности по своей природе является параллельной. Суть предлагаемого альтернативного подхода к проектированию предложенной системы состоит в следующем: «определить процессы, поддающиеся эффективному распараллеливанию, разработать алгоритмы их решения и реализовать на недорогой аппаратно-программной платформе с параллельной или облачной архитектурой [2].

Литература

1. Adzinets D., Razhkova A., Tatur M. Problem-Oriented Parallel Proces sors for Solving of Classification Tasks // Proceedings of the Ninth International Conference on Digital Technologies. Zilina, Slovakia, May 29–31, 2013. P. 181 185.

2. Pitkevich P.I., Adzinets D.N. Enterprise-scale Computing Resource Virtualization Methodology // Digital Transformation. 2021. No. 3. P. 40–46.

МОДЕЛИРОВАНИЕ КОЛЕБАНИЙ НАМАГНИЧЕННОСТИ, ВОЗНИКАЮЩИХ ПОД ДЕЙСТВИЕМ СПИН-ПОЛЯРИЗОВАННОГО ТОКА В ОТСУТСТВИИ ВНЕШНЕГО МАГНИТНОГО ПОЛЯ

А.В. Кухарев, А.В. Петраковская, Г.А. Неверовский

Колебания намагниченности могут возбуждаться в ферромагнитном слое в составе наноструктуры ферромагнетик/ немагнитный металл / ферромагнетик при пропускании через нее спин-поляризованного тока по механизму переноса спина, открытому Слончевским и Берже [1, 2]. Данный эффект может использоваться для разработки наноразмерных генераторов микроволнового излучения. Колебания намагниченности возбуждаются постоянным током и не требуют приложения внешних переменных магнитных полей. Однако в первых работах устойчивые колебания намагниченности удовалось получить лишь при наличии постоянного внешнего магнитного поля. Позже колебания были получены и в нулевом магнитном поле [3]. В [4] определены условия возбуждения колебаний в приближении «макроспина», т. е. когда намагниченность однородна по всему объему свободного ферромагнитного слоя. В настоящей работе получено уточнение этих результатов с помощью микромагнитного моделирования в программе MuMax3, учитывающее неоднородность намагниченности в ферромагнетике.

Моделируемая структура представляем собой цилиндрическую гетерогенную наноструктуру кобальт/медь/кобальт диаметром 20 нм и с толщинами слоев 5 нм, 2 нм и 5 нм соответственно. Намагниченность одного из слоев кобальта закреплена с помощью антиферромагнетика, а намагниченность второго слоя кобальта остается свободной. При пропускании через структуру электрического тока вдоль оси структуры электроны первого слоя передают спиновый угловой момент атомам решетки второго слоя, что создает вращающий момент, действующий на намагниченность ферромагнетика по механизму Слончевского-Берже.

В результате моделирования установлено, что устойчивые колебания намагниченности в отсутствии внешнего магнитного поля могут возбуждаться в том

случае, когда намагниченность закрепленного ферромагнитного слоя и ось легкого намагничивания свободного ферромагнитного слоя параллельны оси структуры (то есть перпендикулярны плоскостям слоев). Также установлено, что с увеличением величины параметра диссипации свободного ферромагнитного слоя уменьшается частота колебаний намагниченности и увеличивается пороговая плотность тока, необходимая для генерации колебаний. Например, при параметре диссипации 0,02 минимальная пороговая плотность тока составляет $0{,}24\times10^8$ А/см^2, а частота колебаний составляет 439,6 МГц при плотности тока $0{,}3\times10^8$ А/см^2.

Литература

1. Slonczewski J.C. Current-driven excitation of magnetic multilayers // J. Magn. Magn. Mater. 1996. Vol. 159. P. L1–L7.

2. Berger L. Emission of spin waves by a magnetic multilayer traversed by a current // Phys. Rev. B. 1996. Vol. 54, No. 13. P. 9353–9358.

3. Long-Timescale Fluctuations in Zero-Field Magnetic Vortex Oscillations Driven by DC Spin-Polarized Current / V.S. Pribiag [et al.] // Phys. Rev. B. 2009. Vol. 80. P. 180411(R).

4. Кухарев А.В. Данилюк А.Л., Борисенко В.Е. Колебания намагниченности в наноструктуре ферромагнетик/ немагнитный металл/ ферромагнетик под действием поляризованного по спину тока // Микроэлектроника. 2012. Т. 41, № 1. С. 9–19.

ИСПОЛЬЗОВАНИЕ НАНОСТРУКТУРИРОВАННЫХ ПЛЕНОК ОКСИДА ТИТАНА ПРИ ИЗГОТОВЛЕНИИ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

С.К. Лазарук, В.В. Дудич, Л.П. Томашевич, Н.Н. Стешиц, К.А. Антипов

Одним из способов защиты информации от нежелательных утечек является использование экранов электромагнитного излучения. Для этого используются металлические решетки с окнами из оптически прозрачного материала [1]. Нами изготовлены титановые решетки с окнами из нанотрубчатого оксида титана. При формировании исследуемых пленок использовали титановую фольгу толщиной 100 мкм. Локальное анодирование проводили с использованием ниобиевой маски в электролитах на основе водного раствора хлорида натрия с концентрацией от 0,1 до 30 % при плотности тока от 5 до 100 мА/см^2. Полученные результаты отличаются от ранее опубликованных тем, что в данном случае размеры внешнего диаметра трубок находятся в диапазоне от 30 до 100 нм, в то время как для известных наноструктур, формируемых в электролитах на основе фторида аммония этот диапазон составляет 70 – 300 нм [2]. Также рекордно низким является значение анодного напряжения, при котором формируются трубчатые структуры. В частности, рост трубок в используемых электролитах наблюдался при напряжении 12–20 В, в то время как при использовании известных электролитов на основе фторида аммония рост трубок имеет место при напряжениях от 25 до 120 В [3]. На основании вышесказанного следует, что прозрачно-проводящие экраны могут быть изготовлены при низких анодных напряжениях. При этом формируется трубчатый оксид титана с более высоким значением удельной внутренней площади поверхности, способной поглощать электромагнитное излучение в заданных диапазонах частот.

Литература

1. Экраны электромагнитного излучения на основе алюминиевой решетки, встроенной в анодный оксид алюминия / С.К. Лазарук [и др.] // Тезисы докладов

XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021. С. 60.

2. Effect of the Electrolyte Temperature on the Formation and Structure of Porous Anodic Titania Film / S.K. Lazarouk [et al.] // Thin Solid Films. 2012. Vol. 526. P. 41–46.

3. Механизм формирования трубчатого оксида титана электрохимическим анодированием / С.К. Лазарук [и др.] // Журнал технической физики. 2020. Т. 90, вып. 5. С. 746–755.

УВЕЛИЧЕНИЕ БЫСТРОДЕЙСТВИЯ ЛАВИННЫХ СВЕТОДИОДОВ НА ОСНОВЕ НАНОКРИСТАЛЛИЧЕСКОГО КРЕМНИЯ ЗА СЧЕТ УМЕНЬШЕНИЯ ИХ РАЗМЕРОВ

С.К. Лазарук, А.Ю. Клюцкий, А.В. Долбик, И.В. Ходяков, И.О. Макарцов, А.А. Лешок, В.А. Лабунов

Оптические соединения обладают рядом преимуществ по сравнению с электрическими аналогами. Сюда можно отнести значительно более высокую пропускную способность и защищенность каналов передачи информации, так как локализация передаваемого потока информации внутри оптического волновода обеспечивает его защиту от несанкционированного доступа.

Ключевыми элементами оптических межсоединений внутри кремниевых чипов и между ними являются источники оптического излучения, формируемые по технологии, совмещенной с технологией кремниевых интегральных схем. Такими светоизлучающими устройствами являются лавинные светодиоды на основе нанокристаллического кремния.

Лавинные светодиоды на основе нанокристаллического кремния формировали по технологии, интегрированной с технологией КМОП ИС. Ключевой операцией технологии их получения является магнетронное осаждение нанокомпозитной пленки Al/Si с последующим ее электрохимическим анодированием, в результате чего формируются кремниевые нанокластеры, встроенные в матрицу оксида алюминия [1–4].

В данной работе показано, что уменьшение рабочей площади диода с 10^4 мкм^2 до 10 мкм^2 приводит к уменьшению интегральной емкости диода более чем на порядок. Соответственно снижение интегральной емкости светодиодов от единиц пикофарад до сотен фемтофарад позволило увеличить их рабочую частоту и достичь излучения в гигагерцовом диапазоне, что является значимым результатом по сравнению с альтернативными источниками света.

Литература

1. Lazarouk S.K. High Field Porous Anodization of Aluminium Films with a Photolithographic Mask / in “Physics, Chemistry and Application of Nanostructures”. Singapore, World Scientific Press, 2013. P. 355–358

2.Фотолюминесценция легированных эрбием алюмооксидных пленок со встроенными кремниевыми наночастицами / С.К. Лазарук [и др.] // Физика и техника полупроводников. 2005. Т. 39, вып. 8. С. 927–930.

3. Electroluminescence from aluminum-porous silicon reverse bias Schottky diodes formed on the base of highly doped n-type polysilicon / S. Lazarouk [et al.] // Thin Solid Films. 1996. Vol. 276. P. 296–298.

4. 3-D Silicon Photonic Structures Based on Avalanche LED with Interconnections through Optical Interposer / S.K. Lazarouk [et al.] // International Journal of Nanoscience. 2019. Vol. 18. P. 1940091.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТИ «ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ» В КОНТЕКСТЕ ПРОЕКТА «МОДЕРНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ»

В.М. Логин

Проект «Модернизация высшего образования Республики Беларусь» (далее – Проект) ставит своей целью совершенствование учебно-образовательной среды и формирование условий для обеспечения соответствия высшего образования потребностям рынка труда. Реализация Проекта рассчитана на 5 лет, охватывает период с 2020 года по 2025 год. Проектом предусматривается модернизация учебно-образовательной среды, введение инноваций в области преподавания и обучения, а также обеспечение и повышение качества образовательного процесса [1].

Образовательным стандартом высшего образования I ступени по специальности 1-39 03 01 «Электронные системы безопасности» (далее – образовательный стандарт) образовательная программа включает следующую учебно-программную документацию: типовой учебный план по специальности, учебный план учреждения высшего образования по специальности, типовые учебные программы по учебным дисциплинам, учебные программы учреждения высшего образования по учебным дисциплинам и программы практик [2].

Функционирование информационно-образовательной среды учреждения высшего образования обеспечивается соответствующими средствами информационно-коммуникационных технологий и соответствуют законодательству. Научно-методическое обеспечение ориентировано на разработку и внедрение в образовательный процесс инновационных образовательных технологий, адекватных компетентностному подходу, таких как: креативное и диалоговое обучение, вариативность моделей самостоятельной работы, модульные и рейтинговые системы обучения, тестовые и другие системы оценивания уровня компетенций.

Для осуществления образовательного процесса привлекаются ведущие специалисты реального сектора экономики. Для аттестации обучающихся на соответствие их персональных достижений поэтапным или конечным требованиям образовательной программы высшего образования создаются фонды оценочных средств, включающие типовые задания, задания открытого типа, задания коммуникативного типа, контрольные работы, тесты, комплексные квалификационные задания, методические разработки по инновационным формам обучения и контроля за формированием компетенций.

Специалист, освоивший содержание образовательной программы высшего образования, обладает как обязательными универсальными компетенциями, так и дополнительными и специализированными компетенциями, которые устанавливаются на основе требований рынка труда, обобщения зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей соответствующей отрасли, а также иных источников.

Обеспечение и повышение качества образовательного процесса определяется требованиями СТБ ISO 9000-2015 «Системы менеджмента качества».

Литература

1. Проект «Модернизация высшего образования Республики Беларусь» [Электронный ресурс]. – Режим доступа: https://nihe.bsu.by/index.php/ru/proekt-mvorb.

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

СКАНИРУЮЩИЙ ПРИЕМНИК «AR-3000A»

В.М. Логин

В последнее время технические (аппаратные) средства защиты информации все больше входят в нашу жизнь и постепенно становятся ее неотъемлемой составляющей. Современные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов, а также различные электронные и электронно-механические устройства, схемно встраиваемые в аппаратуру и сопрягаемые с нею специально для решения задач защиты информации, достаточно многофункциональны [1].

Одним из таких устройств является сканирующий приемник «AR-3000A». Его частотный диапазон от 100 кГц до 2036 МГц без каких-либо разрывов. Данный приемник позволяет принимать сигналы, начиная с диапазона ДВ, через КВ, ОВЧ и выше, вплоть до верхних границ ОВЧ и СВЧ диапазонов. Очень высокий уровень ВЧ характеристик достигнут благодаря применению перед ВЧ усилителями на GaAs полевых транзисторах 13-ти полосовых фильтров, в отличие от других приемников, которые, в основном, построены на широкополосных усилителях.

Шаг настройки выбирается от сверхточного значения в 50 Гц вплоть до 999,95 кГц. Две расположенных на передней панели кнопки (увеличение в 10 раз и уменьшение в 5 раз) позволяют изменять шаг перестройки однократным нажатием, что еще в большей степени повышает универсальность работы приемника [2].

Жидкокристаллический дисплей расположен на передней панели под углом зрения в 12 часов, на нем отображается индикация поиска, сканирования, частоты, уровня сигнала, ВЧ аттенюатора, переключения банков данных в памяти и т.д. Дисплей включает в себя часы реального времени, таймер и выход записи на магнитофон.

В приемнике имеется 400 каналов памяти, которые могут хранить информация о режиме приема, частоте, состоянии ВЧ аттенюатора, признак пропуска данного канала при сканировании и шаг перестройки. Предусмотрено 4 банка поиска, причем каждый банк может быть запрограммирован пользователем для работы в любом месте частотного диапазона радиоприемника.

В целях облегчения поиска, до 100 конкретных частот может быть исключено из каждого банка поиска для предотвращения остановки приемника на нежелательных или длительно занятых частотах. В режимах поиска, сканирования и приоритетной частоты предусмотрены функции программируемой задержки и изменяемой паузы.

Максимальная скорость поиска и сканирования составляет 50 шагов в секунду. Предусмотрен разъем RS-232, позволяющий осуществлять дистанционное управление приемником при помощи персонального компьютера с применением специализированного программное обеспечения. Управляемыми параметрами являются: частота, режим приема, шаг перестройки, запись в/из памяти, уровень сигнала, ВЧ аттенюатор, выбор банка данных и т. д.

Литература

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

2. Профессиональный сканирующий приемник AR-3000A [Электронный ресурс]. – Режим доступа: https://sicom.ru/files/products/1169/aor-ar3000.pdf. – Дата доступа: 02.05.2022.

О ВАЖНОСТИ ИЗУЧЕНИЯ СЕТЕВЫХ ПРОТОКОЛОВ СТЕКА TCP/IP КАК ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

А.В. Ломако

В соответствии с требованиями образовательного стандарта (поколение 3+) выпускники учреждений высшего образования, обучавшиеся по специальности 1-53 01 02 «Автоматизированные системы обработки информации» (АСОИ), должны быть хорошо подготовлены в области технических и программных средств защиты информации. Для реализации этого требования в учебный план указанной специальности введена дисциплина «Аппаратно-программное обеспечение ЭВМ и сетей» (АПОЭВМиС), включающая 48 часов лекций, 32 часа лабораторных работ и зачет в 7-м семестре. Одним из важных составных элементов освоения данной учебной дисциплины является изучение входящих в стек TCP/IP стандартных международных протоколов информационного обмена. Именно при рассмотрении реализованных согласно протоколам технологий и алгоритмов обработки данных выявляются слабые места создаваемых АСОИ с точки зрения защиты данных. При этом четко проясняются уровни из состава эталонной модели взаимодействия открытых систем, разработанной международной организацией по стандартам (RM OSI ISO), на которых возможно появление таких уязвимостей. Студенты начинают понимать физическую сущность протекающих в оборудовании процессов, что позволяет им более грамотно подходить к решению вопросов обеспечения информационной безопасности при проектировании, реализации и эксплуатации АСОИ.

Первыми изучаются протоколы физического и канального уровней. При этом, в частности, полезным оказывается рассмотрение методов «манчестерского» кодирования данных (применяемого в протоколах технологий Ethernet, Token Ring, ArcNet, FDDI), а также сути методов случайного и маркерного доступа к среде передачи данных (применяемых в соответствующих протоколах, упомянутых выше). Кроме того, рассмотрение формата кадров с описанием назначения полей позволяет студентам понять глубинную суть процессов физической передачи данных при сетевом взаимодействии узлов системы и уже на этих уровнях увидеть элементы, отвечающие за достоверность и надежность передачи информации. Кроме того, студентам разъясняется суть и особенности протоколов, используемых в локальных и глобальных сетях, а также методов согласования протоколов (инкапсуляция, трансляция, мультиплексирование).

Особое внимание уделяется рассмотрению протоколов сетевого уровня (IP, ICMP, ARP, RARP) и транспортного уровня (UDP, TCP) модели OSI, так как они составляют основу верхнего уровня транспортной службы любой современной компьютерной сети. При этом продолжается выявление элементов, обеспечивающих надежность и безошибочность передачи данных, а также определяются точки уязвимости, например, в смысле возможности несанкционированного доступа к объектам сети и работающей на ее основе АСОИ. Наконец, рассмотрение ряда типовых протоколов прикладного уровня (FTP, SMTP, HTTP и др.) позволяет

студентам на конкретных примерах лучше понять принципы реализации собственно прикладных информационно-коммуникационных технологий, обеспечивающих построение АСОИ с высоким уровнем надежности и безопасности данных.

В результате описанного подхода к изучению дисциплины АПОЭВМиС студенты в комплексе с изучением других специальных дисциплин приобретают конкретные знания, навыки и умения, необходимые для обеспечения заданного уровня безопасности информации при проектировании и реализации современных АСОИ в любых прикладных сферах деятельности.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ

И.Н. Лущакова, З.Н. Примичева

В условиях стремительного развития IT-технологий уровень высшего технического образования во многом определяет экономический потенциал общества. Обучение в техническом вузе предполагает не только приобретение будущим инженером конкретных знаний и навыков в профессиональной области, но и формирование определенного типа мышления. Поэтому математика занимает важное место среди фундаментальных дисциплин инженерной подготовки. Высокий уровень математических знаний способствует развитию абстрактного мышления, умению использовать аналогии при построении моделей и поиске решений различных технических задач, творческой активности. В последнее время одной из проблем высшей технической школы является довольно ощутимое сокращение часов на изучение математики, при этом представляется невозможным подвергнуть такому же существенному сокращению содержание данного курса без потери уровня преподавания дисциплины. Поэтому обучение математике целесообразно проводить на основе инновационных педагогических и коммуникационных технологий, которые базируются на самостоятельной познавательной деятельности студентов, сопровождаемой контролем преподавателя. Такую возможность предоставляет система электронного обучения (СЭО), функционирующая в БГУИР.

При организации учебного процесса важную роль играют традиционные аудиторные занятия. Но в определенных ситуациях целесообразно использовать «электронные лекции», которые позволяют студентам виртуально посетить пропущенную лекцию либо повторно обратиться к трудным местам. В СЭО можно разместить и материалы справочного характера, касающиеся различных приложений математических понятий (например, формулы, относящиеся к приложениям кратных интегралов). Также в СЭО можно разместить дополнительный материал, выходящий за рамки программы, в том числе и образцы «математического искусства» в различных жанрах, что способствует поддержанию интереса к обучению (см., например, https://anvaka.github.io/fieldplay/?cx=0&cy=0&w=8.5398&h=8.5398&dt=0.01&fo=0.998&dp=0.009&cm=1). Используя СЭО, можно применять тестовый контроль на основе специальных тестирующих программ, который позволяет с некоторой погрешностью быстро оценить уровень полученных знаний. Неточность при оценивании знаний студентов здесь возникает из-за известных недостатков тестирования (отсутствие контроля хода решения задачи, угадывание правильного ответа, выбор неправильного ответа по невнимательности), которая в спорных ситуациях может быть разрешена преподавателем в «ручном режиме».

Таким образом, применение в учебном процессе платформы СЭО помогает преподавателю наглядно представлять материал и проводить контролируемую самостоятельную работу, повышая качество математической подготовки студентов.

ОПТИМИЗАЦИЯ ЗОНДИРУЮЩЕГО СИГНАЛА РЕЗОНАНСНО-РЕФЛЕКТОМЕТРИЧЕСКОЙ ЛОКАЦИИ ПРИ РАБОТЕ В УСЛОВИЯХ ИНДУСТРИАЛЬНЫХ ПОМЕХ

А.И. Майоров, М.А. Буневич, И.А. Врублевский, А.Ю. Клюцкий

Поиск специальных средств негласного съема информации осуществляется в помещениях в городской черте в условиях индустриальных помех, создаваемых различными электронными радиотехническими средствами и линиями электропередачи. В тоже время устройство, работающее на принципах резонансно-рефлектометрической локации, должно функционировать в реальных условиях эксплуатации при воздействии на него непреднамеренных радиопомех и не создавать недопустимых радиопомех другим радиоэлектронным средствам [1].

Проведенный анализ показал, что чем выше мощность излучения передатчика локатора, тем глубже проникает электромагнитная волна и тем больше вероятность и дальность обнаружения закладного радиоустройства. Однако, с увеличением мощности излучения возрастает значение коэффициента преобразования энергии зондирующего сигнала в энергию высших гармоник [2]. Поэтому в качестве зондирующего сигнала целесообразно использовать короткие импульсы с некоторым периодом повторения, поскольку дальность обнаружения зависит от пиковой мощности передатчика, а не от его средней величины. Такой подход проявляется сильнее при уменьшении длительности импульсов по отношению к периоду их повторения. При использовании импульсного режима также могут быть существенно снижены габариты и масса электронной аппаратуры, которые определяются средней мощностью.

Индустриальные помехи имеют всегда широкую полосу частот и характеризуются случайным распределением. После фильтра сжатия интенсивность таких помех значительно уменьшается. Поэтому целесообразно использовать методы сжатия импульса. В таких методах применяются следующие методы модуляции (кодирования) зондирующего сигнала: частотно-импульсная модуляция (линейная и нелинейная), время-частотное кодирование, фазо-импульсная модуляция.

Таким образом, рассмотрение характеристик индустриальных помех позволило проанализировать их влияние на вероятность и дальность обнаружения закладных радиоустройств для метода резонансно-рефлектометрической локации и провести оптимизацию зондирующего сигнала в условиях реальной эксплуатации.

Литература

1. Буневич М.А., Майоров А.И., Врублевский И.А. Оценка возможностей метода резонансно-рефлектометрической локации для задачи поиска закладных радиоустройств // Журнал радиоэлектроники. 2021. № 12. DOI: https://doi.org/10.30898/1684-1719.2021.12.5.

2. Основы построения радиолокационных станций радиотехнических войск / под ред. В.Н. Тяпкина. 2011. 402 с.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ДЛИТЕЛЬНОСТИ ХЕШ-ФУНКЦИИ И ИЗМЕНЕНИЯ ВЕРОЯТНОСТИ КОЛЛИЗИЙ НА УСТОЙЧИВОСТЬ КРИПТОГРАФИЧЕСКОЙ ХЕШ-ФУНКЦИИ К АТАКАМ

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

Одной из важных характеристик, влияющих на стойкость к атакам путем перебора возможных текстов, является длина хеш-функции. В работах [1–3] были рассмотрены атаки на основе парадокса дня рождения и «встречи посередине» применительно к хеш-функции, построенной по схеме Рабина. В приведенных исследованиях были получены результаты для больших значений длины хэш-функции.

При использовании технологий криптографии в системах, имеющих практический интерес для социально-экономической сферы, желательно получить точные оценки влияния параметра, связанного с длинной хэш-функции, на стойкость ее к атакам типа «атака в лоб». Таким параметром служит число переборов, зависящее от вероятности коллизий и длины хеш-функции.

В результате проведенного исследования было получено точное выражение для нахождения числа переборов и определено влияние длины хеш-функции и изменения вероятности коллизии на устойчивость криптографической хеш-функции.

Расчеты числа переборов, проведенные с помощью выведенной формулы, позволили визуализировать зависимость их от длины хеш-функции при заданной вероятности коллизии $P = 0{,}5$. Кроме того, были получены формы графиков при отклонении вероятности коллизии от 0,5 ка в одну, так и в другую сторону.

Полученные результаты точного анализа характеристик криптостойкости хэш-функций в зависимости от ее длинны позволяют найти компромисс между стойкостью ее к атакам, быстродействием обработки данных и затратами на аппаратуру.

Литература

1. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. СПб.: БХВ-Петербург, 2005. 228 с.

2. Мао В. Современная криптография: теория и практика. М.: Издательский дом «Вильямс», 2005. 768 с.

3. Haber S., Stornetta W.S. How to Time-Stamp a Digital Document // J. Cryptology. 1991. P. 99–111.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРОГРАММ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ, УДАЛЕННОЙ СО СЪЕМНЫХ НОСИТЕЛЕЙ

А.В. Макатерчик, В.В. Маликов

Одной из актуальных проблем информационной безопасности является надежное удаление устаревшей и ненужной для дальнейшей деятельности информации. С этой целью применяются как встроенные в операционные системы утилиты, так и программы сторонних разработчиков. В данных программах используются алгоритмы, соответствующие стандарты, такие как Russian GOST R 50739-95, US Army AR380-19, British HMG IS5 Enhanced.

Злоумышленники при попытках восстановления применяют следующие программные продукты: ФЕНИКС, Recuva, Disk Drill, File Recovery, EaseUS и т. п. Целью исследования являлось установление возможностей программ ФЕНИКС, Recuva, Disk Drill, File Recovery, EaseUS, по восстановлению информации удаленной с использованием алгоритмов ГОСТ Р 50739-95, US Army AR380-19, British HMG IS5 Enhanced, Peter Gutmann, German VSITR.

По результатам исследований установлено, что восстановление файлов, удаленных со съемных носителей с использованием перечисленных выше алгоритмов данными программными продуктами не представляется возможным. Однако с помощью программы Recuva, обнаруживается структура удаленных с использованием ГОСТ Р 50739-95 каталогов и файлов, без возможности восстановления находящейся в ней информации.

Литература

1. Кузьмицкий А. М. Организационные меры защиты информации // Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 57–58.

2. Криштопова Е.А. Защита удаленной пользовательской статистики с помощью механизмов дифференциальной приватности // Тезисы докладов XVII Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 11 июня 2019 г. С. 39–40.

ЭЛЕКТРОСТАТИКА ГРАФЕНОВОЙ ТРАНЗИСТОРНОЙ СТРУКТУРЫ

В.В. Мельникова, Д.А. Подрябинкин, А.Л. Данилюк

Графен рассматривается как перспективный материал для полевых транзисторов, несмотря на отсутствие запрещенной зоны, не позволяющей напрямую применять его в цифровой электронике. Однако имеющиеся его преимущества, такие как высокая подвижность и чувствительность к эффекту поля привлекает внимание исследователей для его использования в качестве элемента аналоговых электронных схем. В связи с развитием графеновой электроники встает задача проектирования высокоскоростных графеновых транзисторов. Характеристики таких транзисторов помимо свойств самого графена существенно определяются параметрами диэлектрика, подложки, а также межфазных границ, т.е. интерфейсами электрод / графен, графен / подзатворный диэлектрик, графен / подложка. Это требует помимо развития технологии получения самого графена и создания графеновых транзисторных структур также разработки моделей функционирования полевых графеновых транзисторов, подобных существующим для кремниевых транзисторов. В работе представлены результаты моделирования электрофизических параметров графеновой транзисторной структуры в условиях электростатики, в отсутствии переменного сигнала. В этом случае приложение потенциала полевого электрода эквивалентно смещению электрохимического потенциала, что приводит к изменению электрофизических параметров графеновой структуры, таких как концентрация носителей заряда, квантовая емкость, емкости канала и затвора [1, 2]. Исходя из условия электронейтральности транзисторной структуры с затвором, записано интегральное уравнение электростатики графенового канала [2], с помощью которого вычислены зависимости электрохимического потенциала, концентрации электронов и дырок, а также квантовой емкости от изменения потенциала полевого электрода, емкости подзатворного диэлектрика, плотности интерфейсных состояний на границе графен / диэлектрик. Показано, что при определенной величине плотности интерфейсных состояний зависимости электрофизических параметров графена от потенциала полевого электрода претерпевают скачкообразный переход из одного устойчивого состояния в другое. Также рассмотрены особенности спин-орбитального взаимодействия, индуцированного тяжелыми атомами в графене, которые обусловливают спин-зависимые процессы переноса в графеновой транзисторной структуре, определяющие функционирование спинового транзистора.

Литература

1. Schwierz F. Graphene Transistors // Nature Nanotech. 2010. Vol. 5. P.487–496.

2. Zebrev G.I. Graphene Field Effect Transistors: Diffusion-Drift Theory / in “Physics and Applications of Graphene-Theory”. InTech, 2011. P. 476–498.

АЛГОРИТМ КОДИРОВАНИЯ ИНФОРМАЦИИ В ЗАШУМЛЕННОМ ШИРОКОВЕЩАТЕЛЬНОМ КАНАЛЕ

А.И. Митюхин, А.В. Цык

Рассматривается алгоритм кодирования информации, позволяющий повысить уровень информационной безопасности системы передачи данных на основе информационного подхода. Представлен анализ оптимальных возможностей помехоустойчивых кодов при их применении в зашумленном широковещательном канале. Такой преднамеренно ухудшенный широковещательный канал описывается заданными переходными характеристиками (шумом). В качестве связной модели использовался двоичный симметричный канал. Сущность алгоритма основывается на применении основного уравнения помехоустойчивого кодирования [1] для формирования информационной неопределенности в канале перехвата. Предлагается в процесс кодирования ввести дополнительный этап преобразования источника информации. Данное преобразование формирует взаимно однозначное соответствие между векторами сообщений и синдромами. В этом случае размер анализа в канале перехвата определяется не разрешенным подпространством кода, а размером полного евклидова пространства, зависимым от длины кода. При этом дополнительное кодирование характеризуется свойством апериодичности, что важно, при решении задач минимизации информации в канале перехвата [2]. Кроме того, из-за воздействия шума, ошибки в принятом сигнале увеличивают неопределенность передаваемого сообщения в канале перехвата. В исследованиях основное уравнение кодирования задавалось в виде произведения порождающего и проверочных полиномов соответствующих степеней с коэффициентами над двоичным полем Галуа. В качестве исходного кода использовался симплексный m-код. Так как этот код дуален коду Хэмминга (относится к классу высокоскоростных), вычислительные затраты на анализ входного процесса в канале перехвата резко возрастают с увеличением длины кода. С использованием программного приложения MATLAB проводилась экспериментальная оценка вычислительных (программных) затрат на декодирование по стратегии максимального правдоподобия [3]. Например, для сравнительно малой длины кода, равной 31, вычислительная сложность анализа сводится к проведению более 2 млрд сравнений двоичных векторов по mod 2 на один входной сигнал (кодовое слово). Такой же вычислительный порядок необходим для выполнения операций сложений при нахождении коэффициентов корреляции, по множеству значений которых выносится решение о входном сигнале. Обеспечение требуемой информационной определенности приема информации в канале перехвата за реальное время передачи кодированного сигнала с высокой тактовой частотой чипов кода становится технически сложно реализуемым.

Литература

1. Митюхин А.И. Прикладная теория информации. Минск, БГУИР, 2018. 168 с.

2. Smart N. Cryptografhy: An Introduction. McGraw-Hill, 2003. 436 p.

2. Mac Willams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. Oxford, 1977. 762 p.

ОБ ОПРЕДЕЛЕНИИ МИНИМАЛЬНОГО РАССТОЯНИЯ НЕПРИМИТИВНЫХ КОДОВ ХЭММИНГА

Л.В. Михайловская, Е.В. Валаханович

Современная информационная эпоха характеризуется всеобщей компьютеризацией и стремительным развитием телекоммуникационных средств.

Современные компьютерные технологии позволяют решать задачи, недоступные для решения ранее. Созданы пакеты MathCAD, MATLAB, Maple, Mathematica, разрабатываются современные их версии, рассчитанные на преодоление растущих объемов вычислений. Современные физика, генетика, средства защиты информации требуют освоения новых вычислительных сред, в частности, успешного проведения вычисления не только в рамках нулевой характеристики, но и переход к вычислениям в полях, характеристика которых конечна. Лишь новые версии пакета Mathematica содержат разделы, посвященные некоторым видам вычислений в полях положительной характеристики [1]. Однако потребности практики требуют существенного расширения этих вычислительных возможностей.

В докладе излагается опыт компьютерного формирования больших полей Галуа с предельно широким варьированием формирующих примитивных полиномов, практической организации вычислений в этих полях для решения различных задач помехоустойчивого кодирования.

В помехоустойчивом кодировании важное место занимают коды Хэмминга – циклические совершенные коды из класса БЧХ-кодов [2]. Непримитивные коды Хэмминга потенциально могут иметь минимальное расстояние больше трех. Конкретное определение расстояния связано с решением громоздкой переборной задачи и сопряжено с определенными проблемами организации компьютерных вычислений.

В докладе подводятся итоги систематического исследования непримитивных кодов Хэмминга на длинах от 9 до 99. Известно, что минимальное расстояние кода зависит от количества линейно-зависимых и линейно-независимых столбцов в проверочной матрице кода. Точное значение расстояния каждого рассматриваемого кода устанавливалось построением проверочной матрицы кода и исследованием систем ее столбцов на линейную зависимость.

Наиболее же удачным среди исследованных авторами кодов следует считать код Хэмминга C_X^{79}, задаваемый над полем $GF(2^{39})$. Для этого кода точное значение минимального расстояния равно 15. Следовательно, данный код способен корректировать не только одиночные, но и любые ошибки кратностью до 7 включительно; всего 3200838655 ошибок, что в 40516945 раз больше количества корректируемых одиночных ошибок, исправление которых гарантировано конструктивным расстоянием кода Хэмминга C_X^{79}.

Литература

1. Wolfram Research, Inc., System Modeler, Version 13.0.0. Champaign, IL. 2021.

2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: Издательский центр БГУ, 2007. 240 с.

О ПРИМЕНЕНИИ МЕТОДОВ ТЕОРИИ ПОЛУГРУПП В КРИПТОГРАФИИ

В.А. Молчанов, В.Н. Кутин

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

Настоящая работа посвящена применению в криптографии методов теории полугрупп [3], которые не только позволяют естественно обобщать известные криптосистемы, но и разрабатывать принципиально новые криптосистемы на основе неразрешимых и трудноразрешимых алгоритмических проблем теории полугрупп [4].

Например, одной из таких проблем теории полугрупп является известная проблема равенства слов [3].

Целью данной работы является разработка и программная реализация алгоритмов вычисления конечных полугрупп с целью их дальнейших приложений в структурном анализе таких полугрупп и в криптографии. С помощью результатов [5] разработаны алгоритмы генерации конечных полугрупп преобразований и полугрупп квадратных матриц над конечным полем. На основании описанных алгоритмов реализован программный комплекс с доступным и простым интерфейсом для генерации конечных полугрупп. Программа также проводит статистический анализ процесса генерации полугрупп и на основе таких полугрупп реализует ряд криптосистем с открытым ключом. В частности, проанализированы размеры генерируемых конечных полугрупп и сложность их вычислений, получены распределения порядков элементов таких полугрупп. Помимо этого, программный комплекс на основе сгенерированных полугрупп реализует следующие криптосистемы: обобщенную криптосистему Эль-Гамаля, базирующуюся на полугруппе матриц или группе перестановок, а также криптосистему, базирующуюся на проблеме равенства слов в полугруппах. Программа зарегистрирована Федеральной службой интеллектуальной собственности, номер свидетельства 2021619325.

Литература

1. Романьков В А. Алгебраическая криптография. Омск: Изд-во Ом. гос ун-та, 2013. 136 с.

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

3. Lallement G. Semigroups and combinatorial applications. New York, Wiley, 1979. 376 p.

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

5. Froidure V., Pin J.-E. Algorithms for computing finite semigroups / in “Foundations of Computational Mathematics”. Berlin, Springer, 1997. P. 112–126.

О ВЕРОЯТНОСТНОМ ШИФРОВАНИИ

В.А. Молчанов, А.К. Минуситов

В работе рассматриваются криптосистемы на основе вероятностного шифрования. Главная особенность вероятностного шифрования заключается в том, что один и тот же открытый текст, зашифрованный на одном и том же ключе, порождает различные шифротексты.

Первой схемой вероятностного шифрования с открытым ключом является хорошо известный алгоритм Гольдвассера-Микали [1]. В стандартной реализации данного алгоритма при генерации ключей выбираются два случайных числа, удовлетворяющих лишь условию, что они в двоичном представлении имеют одинаковую длину. В нашей работе предлагается выбирать в качестве закрытого ключа пару простых чисел p, q, удовлетворяющих условию $p, q \equiv 3 \pmod 4$, чтобы использовать их также в генераторе псевдослучайных чисел BBS [1, с. 524–528.].

Предлагается также введение в зашифрованный текст случайных данных, которые затруднят использование методов выявления статистических закономерностей путем подбора открытых или шифрованных сообщений. Случайные данные генерируются с помощью генератора псевдослучайных чисел BBS, причем выходные данные будут зависеть от N-части открытого ключа, чтобы их присутствие в зашифрованном тексте нельзя было выявить.

Была разработана программа, реализующая предлагаемый алгоритм и имеющая пользовательский интерфейс. Программа позволяет сгенерировать пары открытого и закрытого ключей, помещая их в текстовые файлы, шифровать и расшифровывать данные из выбранных пользователем файлов.

Литература

1. Мао В. Современная криптография: Теория и практика. М.: Вильямс, 2005. 768 с.

МОДЕЛИРОВАНИЕ ИЗ ПЕРВЫХ ПРИНЦИПОВ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК ГИДРИРОВАННОГО ГРАФЕНА

В.В. Муравьев, В.Н. Мищенко, А.Д. Митрофанов, Н.Н. Павлюченко, Д.А. Филоненко

Рассмотрены вопросы моделирования из первых принципов параметров и характеристик гидрированного графена. Графен стал предметом многих исследований ввиду того, что он обладает особыми механическими, электрическим и другими свойствам. Но его использование для полупроводниковой электроники сдерживается из-за существующих проблем, связанных с отсутствием зазора между валентной зоной и зоной проводимости в зонной диаграмме. Химическая модификация графена под названием графан недавно стала предметом исследования как возможный кандидат для решения этих проблемы. Графан – это соединение, состоящее из двумерного графена, ковалентно связанного с атомами водорода. Он представляет собой перспективную основу для фундаментальных исследований и возможных технологических приложений при создании разнообразных электронных приборов. Было выполнено моделирование из первых принципов параметров и характеристик гидрированного графена с применением программного комплекса Quantum Espresso. В рамках теории функционала электронной плотности с использованием обменно-корреляционных функционалов вида PBE (Perdew-Burke-Ernzerhof) были получены зонные диаграммы, а также значения основных электрофизических параметров графана в составе гетероструктурного прибора при наличии внешнего электрического поля. Применение отмеченного подхода позволяет проектировать полупроводниковые приборы с регулируемым зазором между зоной проводимости и валентной зоной и добиваться улучшения коммутационных и выходных характеристик. Реализация гетероструктурных приборов с использованием графена и его модификаций позволит реализовать новые устройства, которые найдут широкое применение в системах передачи и обработки сигналов в диапазонах СВЧ и КВЧ.

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ BYOD В БЕЛАРУСИ

И.Г. Некрашевич, Ю.Ю. Петрович, Д.К. Дедович

Технология Bring Your Own Device (BYOD, принеси свое собственное устройство) с 2004 года получила широкое распространение в мире. Модификацию BYOD с аббревиатурой COBO (Corporate-Owned Business-Only, сотрудник использует служебный смартфон предприятия, защищенный отделом безопасности от проникновения вирусов и вредоносных программ) применяют в основном крупные корпорации – IBM, Cisco, Oracle и др. В докладе [1] задачу выбора руководством средней и мелкой компании варианта выбора смартфонов сотрудников (личные или служебные) на рабочих местах предлагается решать путем оценки экономической эффективности внедрения BYOD–COBO. Проведенные исследования показали, что внедрение BYOD–COBO даже на средних предприятиях информатики и телекоммуникаций Беларуси (например, Белтелеком) пока малоэффективно. Возможно, экономический эффект для таких и более мелких белорусских предприятий

даст внедрение модификации BYOD с аббревиатурой POCE (Personally-Owned Company Enabled, смартфон принадлежит сотруднику, но защита информации в нем поддерживается предприятием за счет установки отделом безопасности фирмы на этот смартфон MDM (Mobile device management) приложения, защищающего его от проникновения вирусов и вредоносных программ). Эта модель похожа на BYOD–COBO, при этом предприятие берет на себя ответственность за часть возможностей смартфона, используемых в бизнес-целях. Доступ со смартфона к корпоративной сети предприятия при этом осуществляется через портал, программно отделенный от частной части смартфона. Исследование применения BYOD–POCE в части возможных MDM-приложений и перспектив применения BYOD–COBO и BYOD–POCE в республике продолжается.

Литература

1. Григорьева Ю.Ю, Дедович Д.К., Бахтизин В.В. BYOD и защита информации: экономический аспект // Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 34.

ЗАЩИТА ТЕКСТОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ДОБАВЛЕНИЯ КОНТУРА К СИМВОЛАМ ТЕКСТА

О.А. Нистюк

Описывается метод стеганографии, основанный на использовании параметров текста, в котором в качестве контейнера применяется документ формата .doc или .docx. При помощи указанного метода предлагается скрывать тайное сообщение в файлах различного формата. Новизна рассматриваемого метода заключается в размещении тайного сообщения в контейнерах с помощью определенных параметров настройки характеристики текста, такой как контур. Среди множества известных на данный момент методов защиты текстовой информации ни один не дает полной гарантии сокрытия сообщения в носителе. В последние годы появляется все больше методов сокрытия информации на основе стеганографии. При этом защита или передача информации может производиться путем ее тайного размещения в документ.

Процесс размещения тайного сообщения (или цифрового водяного знака) подразумевает изменение некоторых параметров контейнера. Компьютерная графика добавила символам текста еще одну существенную характеристику – контур, который также может быть использован для размещения тайной информации в текст по аналогии с известными методами графической стеганографии.

Для внедрения информации в файл с расширением .docx необходимо иметь два документа. Один любого текстового формата, в котором будет находится тайное сообщение, а другой документ формата .doc либо .docx, который будет являться контейнером либо носителем. Далее переводим весь текст из документа с тайным сообщением в бинарную последовательность *C*. Необходимо вычислить количество символов бинарной последовательности *C* и документа-контейнера *M*, не учитывая знаки препинания, так как при применении контура к знакам препинания визуально заметна деформация символов. Если размер бинарной последовательности подходит к размеру документа-контейнера, то есть выполняется условие $N_C > N_M /2$, то документ подходит для внедрения информации. Необходимо взять первые два бита сообщения М. Если сочетание символов «11» или «10», то находим первый символ файла-контейнера *C* и изменяем в нем толщину контура символа, если «01» или «00» –

изменяем прозрачность параметра. Разместить информацию в документе-контейнере с применением метода.

Предложенный и проанализированный метод тайной передачи информации в тексте-контейнере основан на реализации текстовой стеганографии путем изменения такого параметра символов текста-контейнера, как контур символа. В результате анализа различных модификаций метода получен более оптимальный алгоритм, исследованы наиболее уязвимые характеристики контура символов.

Литература

1. Electronic Marking and Identification Techniques to Discourage Document Copying / J. Brassil [et al.] // IEEE Journal on Sel. Areas in Commun. 1995. Vol. 13, No. 8. P. 1495–1504.

2. Урбанович, П.П., Юрашевич Д.Э. Использование системных свойств и параметров текстовых файлов в стеганографических приложениях // Материалы международной научной конференции «Теоретическая и прикладная криптография», Минск, 20–21 октября 2020 г. С. 68–73.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДА ТЕКСТОВОЙ СТЕГАНОГРАФИИ ПОСРЕДСТВОМ ИЗМЕНЕНИЯ ПАРАМЕТРОВ КОНТУРА СИМВОЛОВ

О.А. Нистюк

Описывается метод стеганографии, основанный на использовании параметров текста, в котором в качестве контейнера применяется документ формата .doc или .docx. Излагаются возможности использования стеганографического метода в электронных изданиях для осаждения тайной информации с целью защиты документов-контейнеров от несанкционированного копирования и распространения. Представлено разработанное программное средство, демонстрирующее работу стеганографического метода. Описана технология разработки, а также основные структурные элементы его архитектуры. Программное средство работает с электронным документом формата .doc и .docx, изменяя его характеристики начертания символов для создания стеганографического контейнера.

Создано приложение, которое демонстрирует работу предложенного метода. Данное программное средство написано на языке программирования C# 10 (платформа .NET6) с использованием фреймворка Windows Presentation Foundation (WPF). Для работы с Word-файлами использовалась библиотека Open XML 2/16, в которой представена возможность работа с четкими параметрами контура, такими как цвет, толщина, прозрачность, тип точки, тип соединения; для работы с pdf-файлами – iText 7, которая использовалась для чтения тайного сообщения из файлов формата .pdf.

В приложении представлен следующий функционал: внедрение и извлечение информации. При осаждении информации в файл необходимо ввести сообщение или выбрать документ с текстом, затем выбрать файл-контейнер и проверить, подходит ли сообщение под размеры файла-контейнера. При извлечении сообщения из файла необходимо выбрать документ с сообщением и нажать на кнопку «Извлечь сообщение». В окне вывода появится внедренное сообщение, также можно выбрать в каком формате сохранить извлеченное сообщение.

Литература

1. Agarwal, M. Text steganographic approaches: a comparison // International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, No. 1. P. 91–103.

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

МЕТОДИКА АНАЛИЗА ВЗАИМОСВЯЗЕЙ ПОЛЬЗОВАТЕЛЕЙ TELEGRAM

Е.М. Новицкая

Для обеспечения информационной безопасности личности, общества, государства одним из важнейших мероприятий является мониторинг социальных сетей, включая данные которые передаются с помощью различных мессенджеров, например, Telegram. Необходимость мониторинга передаваемой информации, заключается в том, что программное обеспечение реализующее передачу мгновенных сообщений используется для деструктивных воздействий, что обуславливает необходимость проведения соответствующих мероприятий.

Для анализа взаимосвязей пользователей необходимо выполнить ряд этапов в соответствии со следующей методикой. На первом этапе устанавливается и настраивается необходимое для этого программное обеспечение. На следующем этапе необходимо выбрать группы пользователей, взаимосвязь которых необходимо проанализировать Telegram. На этом этапе используется утилита Telegram Scraper, который взаимодействует с Telegram через соответствующий API. Третий этап заключается в формировании списка групп, для этого можно использовать Excel. После того, как такие списки созданы можно перейти к завершающему этапу методики – визуализации результатов. Для практической реализации такого этапа использовалась утилита Gephi, которая позволяет отобразить взаимосвязи пользователей в рамках одной группы на основе учета тех сообщений, которыми они обмениваются. Визуальное представление взаимосвязей пользователей реализуется в виде информационной модели, имеющей вид ориентированного графа. Такое представление упрощает процесс дальнейшего анализа полученной таким образом информации.

Предложенная методика позволяет упростить задачу анализа взаимосвязей пользователей Telegram, за счет построения информационной модели, имеющей вид ориентированного графа. Анализ такой информации может помочь в определении наиболее активных пользователей.

ТЕОРЕТИКО-КОДОВАЯ СИСТЕМА ЗАЩИТЫ МАКЭЛИС С ПЕРЕСТРАИВАЕМЫМ КОДОМ ГОППЫ

В.В. Панькова, С.Б. Саломатин

Теоретико-кодовая система защиты использует высокую сложность решения задачи декодирования случайного кода над конечным полем. Система защиты задается совокупностью множеств: открытых текстов, криптограмм, прямых отображений, обратных отображений, ключей, параметризирующих прямые отображения, ключей, параметризирующих обратные отображения, таких, что сложность обратного отображения без знания ключа сопряжена с решением теоретико-сложностной задачи декодирования случайного кода [1, с. 47–62]. К недостаткам кодовых криптосистем можно отнести детерминизм генераторной матрицы, что делает их уязвимыми для атак с использованием алгоритмов распознавания кодовых структур.

В настоящей работе рассматривается теоретико-кодовая система, использующая рандомизированные коды Гоппа. В основе построения коды лежат полином Гоппы $g(x)$ над расширенным конечным полем, конечное подмножество L расширенного поля, а также функцию R, удовлетворяющая конгруэнтности нулю по модулю $g(x)$. Элементы L не являются корнями полинома $g(x)$. Декодирование кода Гоппы может быть выполнено различными методами [2].

Рассматриваются схемы кодирования и декодирования кода Гоппы с возможностью перестройки структуры путем автоматной рандомизации функции L, выбора требуемой формы функции распределения веса и алгоритма декодирования Патерсона. Анализ статистических свойств криптосистемы МакЭлис с рандомизированными кодами Гоппы показывает близость спектрально-корреляционных характеристик системы к характеристикам случайного процесса при заданной корректирующей способности кода. Применение рандомизированного кодов Гоппа в криптосистеме МакЭлис (Нидерайтер) расширяет область неопределенности задачи криптоаналитика распознавания кодовых конструкций, что в свою очередь повышает уровень защиты криптосистемы.

Литература

1. Biswas B., Sendrier N. McEliece Cryptosystem Implementation: Theory and practice / in “Post-Quantum Cryptography. Lecture Notes in Computer Science”. Berlin, Springer. 2009. 5299 p.

2. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. М.: МЦНМО. 2003. 504 с.

ПЛАЗМОХИМИЧЕСКОЕ НАНЕСЕНИЕ ТОНКИХ ПЛЕНОК В ПОВЫШЕНИИ НАДЕЖНОСТИ ЭЛЕМЕНТНОЙ БАЗЫ ЭЛЕКТРОННЫХ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Р.В. Пигаль

В работе с использованием источников [1–3] обобщены сведения о методах плазмохимического осаждения из газовой фазы тонких слоев диэлектриков на основе нитрида, углерода и диоксида кремния, а также фосфор- и борсодержащих материалов. Описаны процессы роста слоев и приведены данные об основных физико-химических свойствах тонкослойных диэлектрических материалов.

В настоящее время технология плазмохимического нанесения тонких пленок применяется при создании гибридно-пленочных микросхем, коммутационных плат микросборок, а также при получении диэлектрических слоев полупроводниковых интегральных микросхем. Установлено, что совершенствование технологии, улучшение качества и химической чистоты наносимых тонких пленок позволяет заметно повысить надежность элементной базы электронных устройств, в том числе применяемых для защиты информации. Исследовано влияние плазмохимических технологий осаждения тонких пленок на надежность полупроводниковых изделий (полупроводниковые приборы, интегральные микросхемы), а также на изменение эксплуатационных характеристик конструктивных частей технических средств.

В работе установлено влияние и значимость технологии плазмохимического нанесения тонких пленок для повышения надежности элементной базы и улучшения некоторых эксплуатационных характеристик конструктивных частей электронных устройств, используемых для обеспечения информационной безопасности.

Специалисты, которые заинтересовались данной работой, могут обращаться по e-mail: pigal.roman@yandex.ru.

Литература

1. Васильев В.Ю., Репинский С. М. Осаждение диэлектрических слоев из газовой фазы // Успехи химии. Новосибирск: Российская академия наук, 2005. С. 453–483.
2. Seshan, K. Handbook of Thin-Film Deposition Processes and Techniques. NY: Norwich, 2002. 646 с.
3. Прудникова Е.Л. Углеродные нанотрубки для сверхбыстродействующих транзисторов – элементной базы информационных систем будущего поколения // Доклады БГУИР. 2005. № 5. С. 72.

МНОГОФОНОННАЯ И ТУННЕЛЬНАЯ ИОНИЗАЦИЯ ЛОВУШЕЧНЫХ СОСТОЯНИЙ В ОКСИДЕ ГАФНИЯ ПРИ ЭЛЕКТРИЧЕСКОМ ПРОБОЕ

Д.А. Подрябинкин

Актуальность разработки элементов резистивной памяти в настоящее время весьма высока. Несмотря на существенный прогресс в этом направлении, остаются еще нерешенные проблемы, связанные с пониманием особенностей механизмов локализации и ионизации носителей заряда, их переноса в филаментах, сформированных при обратимом электрическом пробое, влиянием спиновой поляризации электронов и электрон-фононных взаимодействий. В работе представлены результаты моделирования процессов ионизации ловушечных состояний в оксиде гафния в составе элемента резистивной памяти. С помощью модели [1], модифицированной в [2], проведены расчеты туннельной и многофононной туннельной ионизации заряженных и нейтральных центров. Для туннельной ионизации с учетом многофонных переходов расчеты показали, что возникают неустойчивости в распределении электрического поля в филаментах в области внешних смещений 0,2–0,6 В. Стабильное состояние наблюдается при внешнем смещении 0,6 В и более, при этом плотность тока уменьшается с увеличением внешнего смещения. Это связано с нелинейным изменением вероятности ионизации с увеличением напряженности поля. Ее величина возрастает при напряженности поля менее $6 \cdot 10^7$ В/м, а затем уменьшается. Показано, что устойчивое состояние токопереноса через филаменты оксида гафния с ловушечными состояниями наблюдается для механизма Пула-Френкеля многофононной ионизации и туннельного механизма ионизации. В случае многофононных переходов с туннелированием электронов и нейтральными ловушками возникают нестабильности в распределении напряженности электрического поля, а также токопереноса, что может быть использовано для управления свойствами элементом резистивной памяти на основе оксидов переходных металлов.

Литература

1. A.L. Danilyuk [et al.] // Physica Status Solidi, ser A. 2013. Vol. 210, No. 2. P. 361–366.
2. Trafimenko A.G., Danilyuk A.L. // Materials Physics and Mechanics. 2018. Vol. 39, P. 75–80.

АНАЛИЗ МЕТОДОВ КОМПЛЕКСИРОВАНИЯ ИЗОБРАЖЕНИЙ В ОПТИКО-ЭЛЕКТРОННЫХ СИСТЕМАХ

К.Е. Прасолович, В.Ю. Горшанов

При осуществлении мероприятий разведки, предусматривающих, в первую очередь, обнаружение объекта, используются различного рода оптико-электронные системы (ОЭС). Как показывает практика, обычные ОЭС, работающие по уже

разработанным алгоритмам функционирования, не обеспечивают требуемой точности обнаружения объекта, что зачастую приводит к невыполнению боевой задачи.

В решении подобной проблемы в настоящее время активно используются алгоритмы комплексирования, за счет которых осуществляется объединение информации, получаемой от датчиков ОЭС, построенных на различных физических принципах.

Обработка информации в ОЭС чаще всего ведется автоматизированным способом, что накладывает определенные трудности, поскольку оператору сложно одновременно воспринимать информацию от нескольких источников. Таким образом, актуальным становится вопрос комплексирования информации для уменьшения ее объемов без потери информативности.

Анализ проблем обнаружения объектов на сложном фоне позволяет выделить ряд недостатков существующих оптико-электронных систем (ОЭС). Среди них можно выделить:

- малую дальность обнаружения;
- зависимость от погодных условий;
- искажение изображений;
- чувствительность к маскировочным средствам;
- зависимость от выбранного порога обнаружения.

Особенно сложными объектами обнаружения являются малоразмерные и малоконтрастные объекты. Основным из направлений повышения качества обнаружения малоразмерных и малоконтрастных объектов является комплексирование нескольких оптических каналов многоканальных ОЭС.

В работе проведен анализ существующих методов комплексирования изображений, среди которых можно выделить:

- метод максимума;
- метод маски;
- метод усреднения;
- метод степенного преобразования;
- метод чересстрочного комплексирования;
- метод весовой функции;
- метод усиления спектрозональных отличий;
- разновидности дискретного вейвлет-преобразования;
- анализ главных компонент.

Результаты исследования были промоделированы в среде Matlab. Каждый из рассмотренных методов комплексирования имеет свои достоинства и недостатки. Однако точного ответа об однозначности выбора лучшего из данных методов, для выполнения задачи обнаружения малоконтрастных и малоразмерных объектов, дать нельзя. Также в некоторых случаях использование комбинации методов является лучшим. Это подтверждает требование ситуативного подбора методов комплексирования для повышения вероятности обнаружения малоразмерных и малоконтрастных объектов на сложном фоне.

МОДИФИКАЦИЯ ФОНОННОГО СПЕКТРА В НАНОСТРУКТУРИРОВАННЫХ СВЕРХПРОВОДНИКАХ

С.Л. Прищепа, В.Н. Кушнир, И.В. Комиссаров

Для надежного и устойчивого функционирования элементов сверхпроводниковой спинтроники возникает необходимость в контроле и управлении эксплуатационными параметрами устройств. Одним из основных направлений в этом смысле является контроль и изменение критической температуры перехода в сверхпроводящее

состояние T_c. Учитывая, что все основные элементы сверхпроводниковой спинтроники базируются на «обычных» сверхпроводниках типа Nb, Al, Pb, у которых спаривание электронов обусловлено фононным механизмом, возникает задача управления фононным спектром сверхпроводников. При смягчении фононных мод константа электрон-фононного взаимодействия повышается, что приводит к росту T_c [1]. Анализ литературы показывает, что повышение критической температуры возможно осуществить разными способами:

- уменьшение размеров образца до значений, приводящих к дискретизации квантовых уровней энергии (характерные значения размеров составляют 2–3 нм);
- формирование сэндвичей типа сверхпроводник-диэлектрик-сверхпроводник, приводящее к экситонному механизму спаривания электронов;
- использование тонких пленок с гранулированной структурой, у которых роль поверхностных фононов значительна;
- использование внешней накачки низкочастотными фононами наноразмерных пленок сверхпроводников.

С технологической точки зрения наиболее перспективным методом является последний [2]. При этом возникает проблема поиска источника низкочастотных (частоты порядка единиц терагерц) акустических фононов. Как показывают многочисленные исследования, графен является хорошим материалом для этих целей. Варьируя параметры синтеза графена, можно управлять его фононным спектром. В данной работе мы демонстрируем что, при определенных условиях, существует возможность локальной накачки тонкой пленки сверхпроводника низкочастотными фононами из графена, что приводит к повышению T_c в отдельных участках пленки.

Литература

1. Transient Superconductivity from Electronic Squeezing of Optically Pumped Phonons / D.M. Kennes [et al.] // Nature Physics. 2017. Vol. 13. P. 479–483.

2. Superconducting Critical Temperature and Softening of the Phonon Spectrum in Ultrathin Nb and NbN/Graphene Hybrids / S.L. Prischepa [et al.] // Superconductor Science and Technology. 2021. Vol. 34. 115021.

ЗАДАЧА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Задача обеспечения информационной безопасности и кибербезопасности – обеспечение непрерывности, безопасности и эффективности технологических и производственных процессов АЭС.

Решением рассмотренных проблем можно считать использованием моделей информационной безопасности, построенной на основе модели МАГАТЭ, которая определяет, как основной элемент информацию, представленную в цифровой форме, и системы, используемые для ее обработки и хранения на уровне технологического управления, т. е. АСУ ТП АЭС.

Кибербезопасность АСУ ТП АЭС, как составная часть информационной безопасности АЭС, заключается в поддержании значений рисков для АЭС (экономических, экологических, социальных), связанных с возможным нарушением (умышленным и не умышленным) доступности, целостности или конфиденциальности информации (программ, данных и их потоков) в АСУ ТП АЭС, в заданных пределах.

При этом АСУ ТП имеет достаточно большое количество уязвимых мест, способных привести к нарушению корректной работы технологического процесса

и реализации угроз несанкционированного доступа к информации в системах диспетчерского управления и сбора данных, отдельных интерфейсах управления автоматизированными комплексами разного назначения, элементах телеметрических систем управления производством. АСУ ТП может быть реально защищена только при решении задач защиты на всех возможных уровнях, угрозы для которых принято определять в виде трех основных групп: угрозы техногенного характера; угрозы антропогенного характера; угрозы несанкционированного доступа.

Техногенные угрозы рассматриваются как физическое влияние на компоненты АСУ ТП. К антропогенным относятся ошибки персонала, преднамеренные и непреднамеренные действия людей, занятых обслуживанием АСУ ТП, ошибки в организации работ с компонентами АСУ ТП. Угрозы несанкционированного доступа для АСУ ТП возникают при взаимодействии компонентов АСУ ТП с локальной вычислительной сетью предприятия при необходимости передачи информации о состоянии технологической среды и управления воздействиями на технологические объекты.

В заключении можно отметить, что особенность задачи состоит в том, что информация, как предмет, безопасность которого определяется, должен быть определен как по внутренней структуре, так и по внутренним свойствам и связям с внешними устройствами, которые необходимы для формирования требований к его безопасности.

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Все указанные факторы в совокупности влияют на общую защищенность системы АСУ ТП. Это и отказ даже от минимальных мер безопасности, и использование Windows, как основной операционной системы для рабочих станций и серверов, и слабая дисциплина сотрудников, а также тот факт, что на каждом из этапов жизненного цикла должны быть определен свой набор мероприятий по выделению актуальных угроз и объектов защиты в АСУ ТП.

Литература

1. Общие положения обеспечения безопасности атомных станций (ОПБ АС). Минск: Министерство по чрезвычайным ситуациям Республики Беларусь, 2009. 28 с.

СНИЖЕНИЕ ЭФФЕКТИВНОЙ ПЛОЩАДИ РАССЕЯНИЯ ЭКРАНАМИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ВЛАГОСОДЕРЖАЩИХ КОМПОЗИТОВ С ПОРИСТЫМИ И ВОЛОКНИСТЫМИ НАПОЛНИТЕЛЯМИ В КРЕМНИЙОРГАНИЧЕСКОМ СВЯЗУЮЩЕМ

Г.А. Пухир, Н.В. Насонова

Эффективную площадь рассеяния (ЭПР) объекта можно использовать в качестве показателя защищенности от утечки информации через средства радиоэлектронной разведки и позволяет рассчитать дальность обнаружения цели (защищаемого объекта). Одним из способов снизить ЭПР объектов является использование экранов электромагнитного излучения (ЭМИ). Проведены исследования радиолокационных характеристик (ЭПР) образцов конструкций экранов на основе влагосодержащих композитов в частотном диапазоне 8–12 ГГц по стандартной методике с использованием сверхширокополосного автоматизированного измерительно-вычислительного комплекса. Для испытаний были изготовлены образцы экранов электромагнитного излучения, представляющих собой гибкую конструкцию из кремнийорганического связующего, внутри которого в предельном объеме

равномерно распределен наполнитель из силикагеля или измельченной древесины с максимальным влагосодержанием.

Результаты измерений показывают, что использование рассматриваемых конструкций экранов позволяет снижать ЭПР цели по сравнению с металлическим отражателем (плоская пластина) до 1 м^2 на частотах в диапазоне 8–10 ГГц.

Конструкции гибких экранов ЭМИ на основе влагосодержащих силикагеля или измельченной древесины в кремнийорганическом связующем обладают средними значениями ЭПР, равными 12–15 м^2 (конструкция из композита на основе влагосодержащей измельченной древесины), 7–12 м^2 (конструкция из композита на основе влагосодержащего силикагеля) и 5–14 м^2 (двухслойная конструкция из представленный материалов) в диапазоне 8–12 ГГц.

На основании экспериментально полученных данных по ЭПР, рассчитана максимальная дальность обнаружения объекта, при его укрытии разработанными экранами ЭМИ. Для представленных конструкции экранов ЭМИ максимальная дальность обнаружения объекта по сравнению с металлическим отражателем снижается в 0,8–1,0 раз. Увеличение количества слоев позволит снизить дальность обнаружения объекта по сравнению с металлическим отражателем за счет согласования волновых свойств слоев с аналогичными свойствами свободного пространства, в котором распространяется ЭМИ, путем снижения коэффициента отражения от поверхности электромагнитного экрана.

ПРОГРАММНАЯ МОДЕЛЬ ДЛЯ СТАТИСТИЧЕСКОГО МОДЕЛИРОВАНИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. Радюкевич

Аналитический анализ процессов, протекающих в синхронизируемых искусственных нейронных сетях (СИНС) представляет очень сложную задачу. В [1] сделана попытка ее решения в упрощенном варианте, позволяющем оценивать лишь общие тенденции влияния параметров.

В связи с этим разработана программная модель для статистического моделирования результатов исследования СИНС. При программной реализации наиболее эффективным инструментом ее исследования является метод имитационного моделирования, а точнее метод статистического моделирования, т.к. случайные процессы, имеющие место в реальной технологии, полностью совпадают с процессами, организованными в модели. Имитационная модель СИНС отличается от реальной программной реализации лишь наличием дополнительных функций, позволяющих анализировать свойства технологии такие как эффективность, безопасность, быстродействие.

Программная модель позволяет смоделировать методы, описанные в [2–4], а также выполнять исследования с учетом действий криптоаналитика. В программной модели существует возможность изменения начальных параметров СИНС, а также объема моделирования. Результаты моделирования представляются в виде таблиц и графиков для наглядного восприятия результатов.

Метод статистического моделирования позволяет вычислять вероятностные характеристики случайных величин и процессов в задачах практически любой сложности и широко применяется в настоящее время в физике, информатике, экономике и других областях науки и техники.

Литература

1. Neural Synchronization and Cryptography. Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades der Bayerischen Julius-Maximilians-Universitat Wurzburg vorgelegt von Andreas Ruttor aus Wurzburg, 2006. 120 p.

2. Радюкевич М.Л., Голиков В.Ф. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей // Информатика. 2020. Т. 17, № 1. С. 75–81.

3. Радюкеви М.Л., Голиков В.Ф. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей // Доклады БГУИР. 2021. № 19 (1). С. 79–87.

4. Радюкевич М.Л. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей // Системный анализ и прикладная информатика. 2021. № 3. С. 51–58.

ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. Радюкевич

Проведенный анализ технологии формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей [1–3] показывает, что данная технология может быть использована в условиях компрометации методов, базирующихся на применении классических односторонних функций. Однако, уровень конфиденциальности формируемого секрета, быстродействие предлагаемой технологии нуждается в серьезном повышении и обосновании.

В работах [4–6] предложены методы повышения конфиденциальности формируемого общего секрета и уменьшения количества обменов информации по сравнению с технологией Neural key generation. Первым был предложен метод усиления секретности, суть которого заключалась в смешивании некоторого числа результатов отдельных синхронизаций (свертки). В качестве функции смешивания использовалась свертка векторов весовых коэффициентов сетей побитовым сложением по модулю 2 всех результатов отдельных синхронизаций. Данный метод позволил экспоненциально уменьшить успех криптоаналитика. При дальнейших исследованиях был предложен комбинированный метод, который состоял из двух этапов: формирование частично совпадающих бинарных последовательностей с помощью синхронизируемых искусственных нейронных сетей и устранение несовпадающих битов путем открытого сравнения четностей пар битов. Данный метод позволил существенно сократить количество обменов информации. Проанализировав возможные атаки на комбинированный метод было предложено добавить досрочное прерывание процесса синхронизации на первом этапе и внесение изменений в полученную бинарную последовательность путем инвертирования случайным образом некоторого количества бит. Эти изменения получили название комбинированного метода формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей, который обеспечивает высокую его криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации.

Литература

1. Kinzel W., Kanter I. Neural Cryptography // 9th International Conference on Neural Information Processing. Singapore, 2002.

2. Kanter I., Kinzel W., Kanter E. Secure exchange of information by synchronization of neural networks. arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.

3. Kanter I., Kinzel W. The Theory of Neural Networks and Cryptography // Quantum Computers and Computing. 2005. Vol. 5, No. 1. P. 130−140.

4. Радюкевич М.Л., Голиков В.Ф. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей // Информатика. 2020. Т. 17, № 1. С. 75–81.

5. Радюкеви М.Л., Голиков В.Ф. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей // Доклады БГУИР. 2021. № 19 (1). С. 79–87.

6. Радюкевич М.Л. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей // Системный анализ и прикладная информатика. 2021. № 3. С. 51–58.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНЫХ ПРОДУКТОВ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ ЗНАНИЙ СТУДЕНТОВ

Н.В. Ржеутская

На сегодняшний день существует огромное количество программных продуктов и оболочек для проведения тестирования в различных сферах деятельности. Для проведения исследования были выбраны двенадцать наиболее востребованных в нынешнее время программных продуктов: TestMaker, RichTest, UniTest System, Hyper Test version 2.0, SunRav TestOfficePro, VeralTest Express, Ассистент II, eTest, MyTest X, Moodle, Microsoft Teams, Indigo.

Используя международный стандарт ISO/IEC 9126 «Информационная технология. Оценка программного продукта. Характеристики качества и руководство по их применению» были оценены все вышеназванные программные продукты. На основании данного стандарта были выделены шесть таблиц и проведена сравнительная характеристика по следующим критериям: 1. Функциональность; 2. Надежность; 3. Удобство использования; 4. Эффективность; 5. Удобство сопровождения; 6 Портативность.

При проведении сравнительного анализа вышеперечисленных программных продуктов выяснилось, что все они полностью соответствуют требованиям функциональности и надежности. Эффективность использования ресурсов в некоторых программах неоднозначна за счет способов установки программ. Удобство использования в программных продуктах Test Maker, HyperTest, Assistant II снижено, за счет возможности создания тестов только на выбор одного или нескольких правильных ответов, а также сложностью установки. Программы Indigo, Microsoft Teams, eTest и Moodle сложны в изучении для пользователя программных продуктов, однако это компенсируется большим количеством методических разработок по этим программам.

Программный рынок для тестирования очень широк. Что касается программ, рассмотренных в данной работе, можно выделить общие достоинства и недостатки в целом:

- высокий уровень функциональности;
- эффективность использования времени и затраченных ресурсов;
- совместимость программного обеспечения;

- наличие сетевых версий и удобство использования;
- высокая степень защиты.

Недостатки:

- отсутствие адаптивности под различные сферы аттестации;
- также самым главным недостатком во всех рассмотренных в данной работе программах остается невозможность отслеживания процесса списывания при проведении удаленного тестирования студентов.

Литература

1. Software Quality ISO Standards // Описание стандарта качества программного обеспечения ISO [Электронный ресурс]. – Режим доступа: http://www.arisa.se/compendium/node6.html/. –Дата доступа: 30.04.2022.

2. Андросов К.Ю. Сравнительный анализ программ-конструкторов тестов и возможность их использования в учебном процессе // Эргодизайн. 2019. № 2. С. 75–80.

ЭТИЧЕСКАЯ СТОРОНА ВОПРОСА ПРОВЕДЕНИЯ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ

Н.В. Ржеутская

Важнейшим этапом изучения любого предмета или дисциплины является процент усвоения студентом знаний, предложенных ему. Традиционно считается, что экзамен является окончательным вердиктом. Однако не менее важным этапом контроля знаний является промежуточное тестирование студентов с целью определения уровня усвоения материалов. Рассматривая этическую сторону вопроса можно отметить, что тестирование должно быть не предвзятым. Личное мнение преподавателя не должно отражаться на оценке студента. Поэтому при выборе вариантов тестирования оптимальным будет является компьютерное тестирование.

В пользу проведения компьютерного тестирования говорит и сложившаяся в настоящее время эпидемиологическая обстановка.

Несправедливость отметок – самый актуальный аспект взаимоотношения преподавателя с учащимися и самая частая причина конфликтов. Данные проблемы поможет эффективно решить внедрение компьютерного тестирования знаний в учебный процесс на всех его этапах.

В научной литературе много статей посвящено правилам составления и требованиям к содержанию тестов. Однако в данной работе хотелось бы рассмотреть создание тестов с точки зрения эффективности всесторонней оценки качества усвоения знаний студентами. Многим студентам психологически тяжело отвечать тет-а-тет преподавателю. В момент волнения даже хорошо известный ответ может вылететь из памяти. На проведенных экспериментах можно удостовериться в эффективности компьютерного тестирования: результаты компьютерного тестирования студентов выше, чем при ответе устно, отсутствует нервное напряжение у испытуемых в силу того, что они сами могут контролировать время ответа на каждый вопрос теста.

Немаловажным достоинством использования тестов является не только процесс контроля подготовленности студентов, но также и их обучение по дисциплине. В качестве примера можно рассмотреть случай, когда студент, проходя тестирование по определенной теме дисциплины, самостоятельно может обнаружить «пробел» в собственных знаниях. При условии самостоятельной ликвидации данных пробелов студентом можно утверждать, что тестовая система проверки знаний имеет еще и обучающий потенциал.

Компьютерное тестирование – наиболее справедливый метод оценки знаний,

как на этапе контроля знаний, так и на этапе выставления результатов. Все студенты находятся в равных условиях изначально и полностью исключается субъективизм преподавателя. Использование компьютерного тестирования знаний является качественным инструментом при оценке уровня усвоения студентом полученных материалов. Ведь когда студент осознает, что его оценка зависит только от его знаний, умений и навыков, тогда процесс подготовки к занятиям становится более ответственным, как вариант с использованием дополнительных источников информации.

Литература

1. Ларина Л.В. Компьютерные системы тестирования знаний студентов на различных этапах оценки успеваемости // Омский научный вестник. 2013. № 1. С. 43–46.

ТРЕБОВАНИЯ К СИСТЕМАМ ЭЛЕКТРОСНАБЖЕНИЯ, ВАЖНЫМ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

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

В связи с вводом в эксплуатацию Белорусской АЭС в Республике Беларусь высокими темпами проводится работа по расширению номенклатуры нормативных правовых актов (НПА), в том числе технических НПА, устанавливающих регулирующие требования к различным видам деятельности, связанным с этапами жизненного цикла АЭС, а также к системам и оборудованию АЭС, поскольку нормативное регулирование является одним из основных принципов обеспечения безопасности АЭС, в том числе информационной безопасности [1]. Разрабатываемые НПА должны отражать накопленный международный опыт в области проектирования и эксплуатации АЭС, а также соответствовать национальному законодательству, в том числе в области использования атомной энергии.

Представлены результаты анализа развития регулирующих требований к системам электроснабжения АЭС на протяжении последних 20 лет. Если документ МАГАТЭ [2] устанавливал требования только к системам аварийного электроснабжения (САЭ), то после аварии на АЭС «Фукусима-дайити» появился новый документ [3], который определяет требования ко всем системам электроснабжения важным для безопасности АЭС (СЭВБ): САЭ, которые являются системам безопасности; системам электроснабжения нормальной эксплуатации, а также системам электроснабжения оборудования контроля и управления запроектными авариями.

С учетом выполненного анализа был подготовлен проект норм и правил по обеспечению ядерной и радиационной безопасности, учитывающий опыт Российской Федерации [4], Украины [5] и рекомендации МАГАТЭ [3] по требованиям к структуре, характеристикам, элементам и условиям эксплуатации, а также к организационным требованиям, направленным на обеспечение ядерной и радиационной безопасности при проектировании, сооружении, вводе в эксплуатацию и эксплуатации систем электроснабжения важных для безопасности АЭС.

Литература

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

2. Design of Emergency Power Systems for Nuclear Power Plants. IAEA Safety Standards Series. Safety Guide. № NS-G-1.8. Vienna, IAEA, 2004. 62 p.

3. Design of Electrical Power Systems for Nuclear Power Plants. IAEA Safety Standards. Specific Safety Guide. № SSG-34. Vienna, IAEA, 2016. 122 p.

4. НП-087-11 «Требования к САЭ атомных станций», утвержденные приказом Федеральной службы по экологическому, технологическому и атомному надзору Российской Федерации от 30.11.2011 № 671. [Электронный ресурс]. – Режим доступа: https://docs.secnrs.ru/documents/nps/НП-087-11/НП-087-11_conv.pdf. Дата доступа: 22.04.2022.

5. НП 306.2.205-2016. Вимоги до систем електропостачання, важливих для безпеки атомних станцій. Затверджено наказом Державної інспекції ядерного регулювання України від 24.12.2015 № 234. [Электронный ресурс]. – Режим доступа: https://zakon.rada.gov.ua/laws/show/z0078-16#Text. Дата доступа: 22.04.2022.

ШИРОКОДИАПАЗОННЫЕ КОНСТРУКЦИИ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ

С.Э. Саванович, Т.В. Борботько

Современный уровень развития средств технической разведки (СТР), обеспечивающих несанкционированные получение информации о местоположении и характеристиках наземных объектов посредством электромагнитного канала, выдвигает в число приоритетных задачу противодействия получения таких сведений [1]. Решение указанной задачи состоит из комплекса мер, включающих снижение интенсивности излучений, отраженных от поверхности наземных объектов ниже или сравнимого с порогом их обнаружения СТР, за счет применения конструкций экранов электромагнитного излучения (ЭМИ), наносимых или закрепляемых на поверхности наземных объектов. Учитывая, что для ведения технической разведки используется диапазон частот 2–12 ГГц [2], актуальным представляется разработка широкодиапазонных конструкций экранов ЭМИ на основе псевдоовальных рассеивающих элементов, линейный размер которых в поперечине составляет 10…20, 2…4, 1…4 и 1…2 мм, содержащих растворы хлорида натрия (NaCl).

Для установления влияния взаимного расположения указанных элементов на ширину рабочего диапазона частот конструкций экранов ЭМИ предложены пять вариантов их конструктивного решения:

1) многослойная конструкция экрана ЭМИ;

2) конструкция экрана ЭМИ с геометрическими неоднородностями поверхности;

3) конструкция экрана ЭМИ дифракционного типа

4) конструкция экрана ЭМИ в виде монослоя псевдоовальных элементов;

5) конструкция экрана ЭМИ в виде комбинации монослоя псевдоовальных рассеивающих элементов и двух- трехслойных структур, выполненных на их основе.

В результате исследований установлено, что оптимальным вариантом является конструкция экрана ЭМИ дифракционного типа и конструкция, выполненная в виде комбинации монослоя псевдоовальных рассеивающих элементов и двух- трехслойных структур. В диапазоне частот 2–12 ГГц указанные конструкции экранов ЭМИ характеризуются значениями коэффициентов отражения до –21 дБ, что соответствует, в случае нанесения или закрепления их на поверхность наземных объектов, значениям ЭПР в пределах 0,08…11,8 м^2, что свидетельствует о существенном затруднении перехвата информации о местоположении и характеристиках наземных объектов СТР.

Литература

1. Модели технических разведок и угроз безопасности информации / под ред. Е.М. Сухарева. Кн. 3. М.: Радиотехника, 2003. 144 с.

2. Перунов, Ю.М. Зарубежные радиоэлектронные средства / Ю.М. Перунов [и др.]. Кн. 2. М.: Радиотехника, 2010. 336 с.

АЛГОРИТМ ВЫБОРА ПИКСЕЛЕЙ ДЛЯ СТЕГАНОГРАФИЧЕСКОГО ВНЕДРЕНИЯ ИНФОРМАЦИИ В WEB-ДОКУМЕНТЫ

М.Г. Савельева

Поскольку аудио, видео и другие работы доступны в цифровой форме, легкость, с которой могут быть сделаны идеальные копии, может привести к крупномасштабному несанкционированному копированию и/или модификации исходных файлов. Эти опасения по поводу защиты авторских прав вызвали значительные исследования, направленные на поиск способов сокрытия авторских сообщений и серийных номеров в цифровых носителях. Одним из основных направлений разработки упомянутых средств является стеганография [1].

Важным этапов любого стеганографического алгоритма является выбор массива пикселей для внедрения информации. В данном докладе предлагается алгоритм создания массива пикселей для внедрения секретного сообщения в web-документ, представленный как файл растровой графики. Для внедрения информации необходимо выбрать массив пикселей *Z*, где совпадает значение одного или двух цветовых каналов. Для выбора пикселей в изображениях с большим количеством полутонов, монохроматических или черно-белых целесообразно осуществлять выбор по двум цветовым каналам, а для внедрения тайной информации в выбранные пиксели использовать один канал. В остальных изображениях можно ограничиться одним каналом для выбора пикселей. Осуществлять внедрение информации в канал, использующийся для выбора пикселей, нельзя.

Для реализации алгоритма примем c_{RGB} как цветовой канал с повторяющимися значениями пикселя, $c_{RGB} \in R, G, B$, φ как ключевое значение канала c_{RGB}, $\varphi \in \{0, 1, \ldots, 255\}$. Начальным шагом является определение размеров изображения-контейнера. Следующим этапом является поэлементная обработка пикселей контейнера, являющихся двумерным массивом. Если значение канала c_{RGB} имеет значение φ, то пиксель предварительно вносится в массив *Z*. Так как стеганографическое преобразование основано на неспособности органов чувств человека различить незначительные изменения в цвете изображения (изменение значений наименее важных битов, отвечающих за цвет пикселя, не приводит к сколь-нибудь заметному для человека изменению цвета, что также объясняет невозможность использовать изменение значений яркости для внедрения секретной информации), то для выбора пикселей для внедрения некоторых алгоритмов следует провести дополнительную выборку из получившего массива.

Для увеличения пропускной способности при выборе изображения-контейнера следует провести анализ, в каком цветовом канале больше пикселей с повторяющимися значениями (одно из 256) и непосредственно само значение, которое встречается в этом канале наиболее часто. Рекомендуется использовать канал как c_{RGB} и значение как φ. Канал для внедрения выбирается произвольно из оставшихся двух или оба.

Литература

1. Шутько Н.П. Особенности и формальное описание процесса осаждения секретной информации в текстовые документы на основе стенографии // Труды БГТУ. 2014. № 6 (170). С. 121–124.

СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ПРИЛОЖЕНИЙ В РАСТРОВОЙ ГРАФИКЕ НА ОСНОВЕ МОДЕЛИ RGB

М.Г. Савельева, П.П. Урбанович

Актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. Современные компьютерные технологии, прогресс в области глобальных компьютерных сетей и средств мультимедиа обеспечивает возможность разработки и реализации новых методов, предназначенных для обеспечения защиты электронного контента от несанкционированной модификации или использования [1, 2].

В докладе представлены метод и реализующие его алгоритмы стеганографического преобразования, использующие в качестве контейнера элементы web-приложения на основе растровой графики. В данном случае под контейнером понимается защищаемый документ. Эта защита реализуется размещением в указанном документе тайной информации, выполняющей функцию невидимого водяного знака. В качестве базового элемента контейнера, цветовые параметры которого модифицируются в модели RGB при осаждении информации, выступает пиксель изображения. Внедрение/извлечение информации происходит в пикселях, имеющих одинаковое значение (одно из 256) в одном или нескольких цветовых каналах. Особенностью разработанного метода является то, что процессы внедрения/извлечения информации осуществляются при сравнительном анализе значений одного или двух цветовых координат базового пикселя и пикселя для внедрения. Количество каналов для выбора пикселей и для внедрения сообщения зависит от цветовых характеристик изображения и длины сообщения. В изображениях с большим количеством полутонов, монохроматических или черно-белых изображений для выбора пикселей, в которых будет происходить внедрение тайной информации, целесообразно осуществлять выбор по двум цветовым каналам. При этом непосредственно для внедрения информации в выбранные пиксели использовать один канал. В полноцветных изображениях можно ограничиться одним каналом для выбора пикселей. Использовать одни и те же каналы для внедрения и выбора пикселей нельзя, их суммарное количество также не должно превышать трех.

Данный метод может использоваться для защиты текстовых документов, представленных как объект растровой графики. Пропускная способность (емкость внедрения) метода зависит от характеристик изображения-контейнера: количества пикселей с одинаковыми значениями одного или нескольких цветовых каналов.

После проведенного сравнительного анализа с методом LSB можно сказать, что предложенный метод может уступать по максимальной пропускной способности, но выигрывает в устойчивости к некоторым видам атак.

Литература

1. Шутько Н.П., Урбанович П.П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов // Материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов «Информационные технологии», Минск, 4–15 февраля 2019 г. С. 41–43.

2. Шутько Н.П., Урбанович П.П. Особенности использовании параметров апроша в методах текстовой стеганографии // Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 103–104.

ФОРМИРОВАНИЕ ОБРАЗОВАТЕЛЬНОГО КОНТЕНТА ПО ОТКРЫТЫМ ИСТОЧНИКАМ МЕТОДАМИ АНАЛИТИЧЕСКОЙ РАЗВЕДКИ

И.М. Салей, Г.В. Щиглинский

События последнего времени, связанные с приостановкой работы на белорусском рынке некоторых ведущих ИТ-компаний, остро ставят вопрос о поддержке организаций, пользовавшихся их продуктами и сервисами. Так уход с белорусского рынка компании Cisco, привел к внезапной блокировке ресурсов программы Сетевых академий Cisco, участником которой белорусские университеты были почти 20 лет. Поэтому эксперты все активнее выступают за снятие ограничений на использование интеллектуальной собственности в современных условиях, предупреждая одновременно о рисках для участников рынка легального программного обеспечения.

В докладе представлен подход, использующий методы аналитической разведки, позволяющий на основе открытого контента интернет-ресурсов образовательного характера (наборы связанных веб-страниц, интерактивные учебные веб-ресурсы) формировать контент в традиционном академическом «бумажном» представлении (книги, методические пособия).

Использованный метод проведения аналитической разведки и извлечения информации предполагает выполнение ряда этапов. 1. Исследование технической составляющей сайта: анализ доменного имени, изучение структуры сайта, изучение использованных способов адресации и структуры ссылок на страницы сайта. 2. Исследование контента сайта: используемого шаблона страницы; структуры и стилей текстовой информации; принципов формирования графического контента сайта; идентификации тегов текстовой и графической части, элементов шаблона страницы; наличия дополнительных разделов. 3. Использование пакета скриптов на языке Python с доступом к библиотекам requests, bs4, selenium для извлечения контента. 4. Использование скриптов на языке Visual Basic for Application пакета MS Office для формирования «бумажных» аналогов полученного образовательного контента.

Работа проводилась в академических целях. Авторы разделяют авторитетное мнение, что «чтобы обеспечить защиту от атак, специалисты по кибербезопасности должны обладать теми же навыками, что и хакеры» [1].

Литература

1. Cybersecurity Essentials / Cisco Networking Academy [Electronic resource]. – Access mode: https://contenthub.netacad.com/ legacy/CyberEss/1.0/ru/course/module1/ 1.5.2.2/1.5.2.2.html. – Date of access: 03.05.2022.

ОБЗОР ОБОРУДОВАНИЯ FORTINET ДЛЯ ВНЕДРЕНИЯ В ЛОКАЛЬНЫЕ СЕТИ С ЦЕЛЬЮ ЭФФЕКТИВНОГО ВЫЯВЛЕНИЯ УГРОЗ

Е.А. Семак

Компания Fortinet специализируется на разработке и продвижении программного обеспечения, решений и сервисов в области информационной безопасности: межсетевых экранов, антивирусных программ, систем предотвращения вторжений и обеспечения безопасности конечных точек и других продуктов. Компания Fortinet наиболее известна благодаря семейству средств обеспечения безопасности FortiGate, которые сочетают множество функций по защите информации. Семейство физических и виртуальных решений FortiGate в области унифицированного управления угрозами включает такие функции обеспечения безопасности, как межсетевые экраны,

средства предотвращения вторжений, веб-фильтры и защита от вредоносного программного обеспечения или нежелательной почты. Программное обеспечение FortiAnalyzer предоставляет функции создания отчетов для продуктов Fortinet, включая ведение журналов событий, создание отчетов безопасности и функции анализа [1, 2].

Литература

1. Martín H. Hoz Salvador; Ken McAlpine; Rick Basile; Bruce Matsugu; Josh More. UTM Security with Fortinet: Mastering FortiOS Syngress, 2012.

2. Fortinet Fortiguard Security Services | AVFirewalls.com [Electronic resource]. – Access mode: https://www.avfirewalls.com/Fortiguard-Security-Services.asp. – Date of access: 06.05.2022.

К ВОПРОСУ О МЕТОДИКЕ ПРЕПОДАВАНИЯ ТЕМЫ «ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ»

А.И. Серый

Учебные планы некоторых физико-математических специальностей (в частности, «Компьютерная физика») предусматривают, среди прочих дисциплин, изучение дисциплины «Технические средства и методы защиты информации» [1]. Важное место в этой дисциплине занимают вопросы, связанные с техническими каналами утечки информации и мерами по борьбе с утечкой информации по таким каналам. Несмотря на бурное развитие указанной дисциплины и довольно быструю потерю актуальности сведений о некоторых конкретных технических устройствах, общие принципы формирования каналов утечки информации и выбора мер борьбы с ними можно считать относительно устойчивыми.

Каждый отдельно взятый технический канал утечки информации можно охарактеризовать по следующим пунктам. 1.1. Тип сигнала (акустический, электрический, электромагнитный). 1.2. Для каждого типа сигнала – подкласс канала (например, акустические каналы бывают воздушными, вибрационными и другими). 1.3. Разновидность устройства съема информации и ее дальнейшей передачи. 2.1. Меры по недопущению проникновения информации в канал утечки (иными словами – меры по устранению или уменьшению демаскирующих признаков (ДП) охраняемого объекта), связанные: а) с понижением уровня исходного сигнала (в том числе путем изоляции); б) с зашумлением сигнала. 2.2. Меры по поиску устройств съема информации: а) по внешним ДП (даже если устройство закамуфлировано); б) по наличию полупроводниковых соединений (с помощью нелинейных локаторов); в) по электромагнитному излучению во время работы (с помощью, технических средств радиомониторинга и других устройств). 2.3. Меры противодействия работе устройств съема информации после обнаружения таких устройств: а) отключение; б) блокировка канала дальнейшей передачи информации; в) вывод устройства из строя. Таким образом, требуется ослабить ДП своих устройств и усилить ДП устройств противника (чьи задачи сформулированы почти или точно так же, но противоположны с точки зрения перечня устройств)

Приоритеты при выборе конкретных мер из перечисленных выше, как правило, обусловлены: а) принципиальными физико-техническими возможностями; б) допустимостью с точки зрения действующего законодательства; в) стремлением к минимуму финансовых издержек. Руководствуясь данным алгоритмом, можно составлять план по реализации мер противодействия утечке информации в конкретных ситуациях. Составление подобных планов можно предлагать учащимся в качестве самостоятельных творческих заданий. Данная публикация является дополнением к [2].

Литература

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

2. Серый, А.И. К вопросу о методике преподавания дисциплины технические средства и методы защиты информации» Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 86–87.

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ МОБИЛЬНОГО РОБОТА С ОГИБАНИЕМ ПРЕПЯТСТВИЙ ПРИ ИСПОЛЬЗОВАНИИ МАШИННОГО ОБУЧЕНИЯ

А.В. Сидоренко

При внедрении мобильных роботов в космическую, военную, производственную сферы деятельности человека возникает одна из актуальных задач, заключающаяся в управлении движением мобильного робота в среде с обеспечением его безопасного движения и огибанием препятствий, встречающихся на его пути.

При решении подобных задач используются алгоритмы машинного обучения. Использование указанных алгоритмов основано на принципах моделирования. Критерием оптимизации в моделях машинного обучения является определение количества эпизодов для достижения цели обучения при использовании определенного алгоритма обучения.

В предлагаемой работе программно-реализованные алгоритмы обучения, примененные нами для системы мобильных роботов, позволили провести вычислительный эксперимент. В модели, описывающей движение робота, применяется пакет Mobile Robotics Simulation Toolbox на операционной системе Linux при использовании пакета визуализации Gazebo. Взаимодействие роботов обеспечивается через пакет для MatLab ROS Toolbox. При реализации эксперимента использовалась модель поверхности размером 17×17 блоков с препятствием размером 1×12 блоков, определяемая пакетом Gazebo. В процессе эксперимента при перемещении робота достижение значения вознаграждения в численном выражении равное 500, определялось как целевое. В ином положении отмечалось как «–1». Обучение прекращалось, когда суммарное среднее значение вознаграждения достигало «480».

Анализ полученных результатов показал, что для рассмотренной модели среды обучение производится при использовании алгоритма Q-обучения за 73 эпизодов, а для алгоритма SARSA понадобилось, соответственно, 58 эпизодов.

Результаты анализа показали, что быстрее всего обучается робот при использовании алгоритма SARSA, более медленно – алгоритм при применении Q-обучения.

ИССЛЕДОВАНИЯ УТЕЧКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК В ИНТЕРФЕЙСАХ ВИДЕОПОДСИСТЕМ МОНИТОРОВ

Е.А. Симахин, Г.П. Гавдан, А.П. Дураковский

Решение проблем по противодействию утечке информации ограниченного доступа за счет побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники (СВТ) сегодня не утратили своей актуальности. Проведение анализа работы различных интерфейсов передачи данных СВТ позволяет злоумышленнику получить не только доступ к защищаемой информации,

но и выполнить ее восстановление с требуемым качеством. А с учетом того, что рассматриваемый технический канал утечки информации (ТКУИ) работает фактически в реальном масштабе времени и является пассивным, то задача обнаружения нарушителя для владельца информации является практически невыполнимой. Вместе с тем ряд исследований показывает наличие трудностей при анализе компонентов архитектуры интерфейсов передачи данных [1, 2], подходов к обеспечению требуемого уровня защищенности объектов информатизации [3], а также при разработке программно-аппаратных комплексов, решающих задачи автоматизированного тестирования интерфейсов передачи данных [4]. Совокупность выполненных исследований по данной тематике и наличие неконтролируемого распространения информативного сигнала от СВТ через физическую среду до технического средства, осуществляющего перехват информации, подтверждают актуальность защиты информации от утечки по каналу ПЭМИН, в особенности для критически важных объектов. В последние годы с возросшим объемом обрабатываемой информации обширное распространение получили устройства с высокоскоростными интерфейсами передачи данных, например, жидкокристаллические мониторы с интерфейсами HDMI и DisplayPort. В качестве решения поставленной задачи для рассматриваемых интерфейсов требуется проведение лабораторных исследований [2]. Входной информацией для такого рода исследований являются сведения об архитектуре интерфейса, о технологии формирования последовательности данных, их порядке передачи от источника к приемнику, результаты проведения инструментальной проверки на сформированном исследовательском стенде. В результате работы полученные данные позволят сформировать критические условия эксплуатации интерфейса с точки зрения возможности перехвата, и, как следствие, получить более точные значения при выполнении контроля защищенности обрабатываемой в СВТ (защищаемой) информации.

Литература

1. Durakovskiy A.P., Kessarinskiy L.N., Simakhin E.A. Detection of compromising radiation from modern data transfer interfaces using the example of high definition multimedia interface // IOP Conference Series: Materials Science and Engineering. 2021. Vol. 1069 (1). P. 012026.

2. Анализ компонентов архитектуры интерфейса DisplayPort, влияющих на побочное электромагнитное излучение / Е.А. Симахин [и др.] // Безопасность информационных технологий. 2022. Т. 29, № 1. С. 108–124.

3. Голяков А.А., Дураковский А.П., Симахин Е.А. Применение генератора замещения для определения реального затухания информативных сигналов побочных электромагнитных излучений // Безопасность информационных технологий. 2018. Т. 25, № 2. С. 38–53.

4. Development of a Software Package for the Analysis of Compromising Emanation Using LabVIEW / I.I. Kagin [et al.] // Proccedings of 2021 International Siberian Conference on Control and Communications (SIBCON). 2021. P. 1-5.

РАСПОЗНАВАНИЕ ЧЕЛОВЕКА ПО ГОЛОСУ НА ОСНОВЕ ВЕЙВЛЕТА МОРЛЕ

Н.А. Слышанков

Выполнить распознавание человека по голосу является довольно сложной задачей, которая включает в себя затраты многих ресурсов, однако, выполнение данной задачи позволяет наиболее эффективно защищать конфиденциальную информацию.

Распознавание происходит считыванием характеристик человека и сравнения с теми, что хранятся в базах с данными пользователей. Для получения характеристик голоса применяют различные технологии, одной из таких технологий является вейвлет-преобразование.

Вейвлет-преобразование – эффективная технология, позволяющая проводить обработку сигналов различного типа. Кроме того, существует множество исследований по использованию вейвлет-преобразований для сжатия звука, в ходе которых было показано, что данный вид функций позволяет выделять различные характеристики аудиосигналов. Это свойство обусловливает возможность применения вейвлет-преобразований для анализа звуковых данных с последующим использованием полученных сведений для выделения звукового отпечатка человека.

Целью исследования является определение возможности применения вейвлета Морле для систем распознавания человека по голосу. Вейвлет Морле представляет собой непрерывное вейвлет-преобразование, которое применяется для проведения локального спектрального анализа.

В ходе данной работы была разработана программа, производящая трехсекундные записи голоса с выбранного микрофона, а также вейвлет-анализ и сравнение представленных записей.

Было проведено 200 опытов на одном и том же записанном фрагменте, и точность распознавания составила 93 %. Признание вейвлета Морле значительно сократило время обработки входного сигнала при распознавании человека по голосу [1].

Литература

1. Гребнов С.В. Аналитический обзор методов распознавания речи в системах голосового управления [Электронный ресурс]. – Режим доступа: http://ispu.ru/files/%2083-85.pdf. – Дата доступа: 12.05.2021.

УЯЗВИМОСТИ VPN-ТЕХНОЛОГИЙ

Т.И. Солонович

В работе [1] рассмотрены назначение, принцип действия и разновидности Virtual Private Network (VPN). В настоящее время в связи с быстроразвивающейся сферой технологий и ростом популярности использования, среди VPN-сервисов, кроме безопасных и технологичных, появились мошенники. «Второй стороной медали» являются многочисленных атаки на VPN, кража данных пользователей и их продажа рекламодателям, с целью последующего использования в своих целях. Наиболее простой является дактилоскопия трафика веб-сайта. Шифрование трафика определенных веб-сайтов происходит по шаблону, в результате чего злоумышленник может догадаться, какой сайт посещается, хоть и не видит содержание передачи этого трафика.

Атаки на такие известные криптографические алгоритмы как DES, TripleDES, RSA, AES практически бессильны, ведь стойкость алгоритма определяется не его секретностью, а надежностью ключа, именно поэтому наиболее популярными являются атаки на криптографические ключи. Для того, чтобы обезопасить сервис от атак, в зависимости от необходимости времени хранения информации, ключ должен обладать достаточной длиной.

Механизм генерации ключей – еще одна уязвимость, составляющая алгоритм шифрования (для получения доступа к данным иногда достаточно атаковать всего один элемент алгоритма). Для предупреждения фактора предсказания ключа злоумышленников, необходимо отдавать предпочтения аппаратным системам генерации ключей.

Не стоит пренебрегать и возможными атаками на оборудование VPN, атаками на пользователей и ПО. Существует множество сервисов и приложений, изучив специфики которых, можно выделить наиболее оптимальные и безопасные для использования. Surfshark VNP использует метод шифрования AES-256-GCM. Он предоставляет конфиденциальность и аутентификацию переданных данных, является высоко эффективным и производительным. Имеет функции защиты от фишинга, различных вредоносных программ и утечек, благодаря частному DNS. Позволяет подключаться через несколько стран или с нескольких устройств одновременно при необходимости. Имеет строгую политику отсутствия журналов, обладает функцией раздельного туннелирования и аварийного выключателя, а также уникальной функцией Spoofing GPS. Однако из недостатков можно выделить наличие статических IP-адресов и неравномерности географического расположения серверов, что сказывается на скорости соединения.

Сервис NordVPN использует тот же метод шифрования, ведет политику полного отказа от ведения логов и хранения любой персональной информации пользователей. Так же отличается своей производительностью от конкурентов на рынке других приложений, но уступает им в стоимости ежемесячной подписки. Протоколы – IKEv2/IPsec и OpenVPN.

Сервис ExpressVPN в отличие от вышеперечисленных имеет функцию speed test, которая позволяет тестировать скорость в зависимости от точки подключения. Как и NordVPN поддерживает P2P, благодаря чему можно достаточно быстро загружать файлы. Построен на базе протоколов IKEv2, OpenVPN и L2TP/IPsec, для обеспечения безопасности данных пользователей, а также начал развертывание своего собственного протокола Lightway.

В результате проведенного анализа можно отдать преимущество сервису NordVPN. Немногим от него отличается Surfshark, однако с точки зрения безопасности является более не надежным. Безопасность всей системы равна безопасности самого слабого звена, именно поэтому стоит задумываться даже о самых мелких возможных уязвимостях, ведь даже они могут нанести значительный ущерб как отдельному пользователю, так и крупной компании.

Литература

1. Солонович Т.И. Использование технологии VNP как средства защиты информации // Материалы XVIII Международной научно-практической конференции «Управление информационными ресурсами», Минск, 24 февраля 2022 г. 4 с.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

К.О. Станкевич

Современный этап развития системы обеспечения информационной безопасности государства и общества, а также политики государства в области защиты информации характеризуется осознанием необходимости защиты любых информационных ресурсов и информационных технологий от неправомерного обращения, которое может нанести ущерб их собственнику, владельцу, пользователю или иному лицу.

Под защитой информации понимают комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Основным законом, регламентирующим нормативно-правовое регулирование в сфере защиты информации в Республике Беларусь, является Закон РБ 10 ноября 2008 г.

№ 455-З (далее-Закон), в соответствии с которым, целями защиты информации являются:

- обеспечение национальной безопасности, суверенитета Республики Беларусь;
- сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;
- обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий [1].

Владельцы программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъекты информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями при организации и планировании своей деятельности должны руководствоваться нормами, регламентированными статьей 38 Закона.

Нарушение законодательства об информации, информатизации и защите информации влечет ответственность в соответствии с законодательными актами Республики Беларусь:

- ответственность за совершение административных правонарушений в области информации предусмотрена главой 23 Кодекса Республики Беларусь об административных правонарушениях;
- ответственность за совершение преступлений против информационной безопасности предусмотрена главой 31 Уголовного кодекса Республики Беларусь.

Литература

1. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: http://www.pravo.by. – Дата доступа: 29.04.2022.

ТЕХНОЛОГИИ ТРЕХМЕРНОЙ КОМПЬЮТЕРНОЙ ГРАФИКИ ДЛЯ РЕШЕНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ ЗАДАЧ

В.А. Столер

В последнее время разработчиками инженерных проектов все чаще применяются технологии, связанные с последовательным использованием нескольких пакетов графических программ трехмерной графики при создании объектов и изделий технического назначения. Программных пакетов, реализующих трехмерную графику, довольно много. Среди них, такие как Lightwave 3D, Blender 3D, Cinema 4D, 3ds Max, Maya, а также САПРы Inventor, AutoCAD, SolidWorks, T-FLEX CAD др. Использование трехмерной графики объясняется большей реалистичностью полученного в ней изображения, когда появляется возможность изучения объекта со всех сторон для выбора лучшего варианта. Недостатком трехмерной графики является повышенные требования к оперативной памяти и быстродействию компьютера, которые следует учитывать при разработке проекта.

В работе рассматривается технология трехмерного моделирования и визуализации объектов и сцен на основе двух графических программ фирмы Autodesk. Предлагаемая технология заключается в использовании AutoCAD

для разработки технического проекта с последующим применением 3ds Max для создания трехмерного изображения изделия в составе сцены. AutoCAD является наиболее распространенным и эффективным инструментом в области проектирования и выполнения чертежей. Современные версии AutoCAD содержат в своем арсенале достаточно полезных инструментов для решения многих инженерно-технических задач. Выбор программы 3ds Max обусловлен ее большими графическими возможностями при создании трехмерных изображений. Так называемые фотореалистичные изображения, созданные в 3ds Max, позволяют получать наиболее полную визуальную характеристику на разных стадиях разработки проекта.

В заключение необходимо отметить, что применение рассмотренной технологии позволит создавать различные реалистичные объекты, в том числе системы и устройства защиты информации, обеспечивая их быстрое моделирование и разработку с использованием современных компьютерных программ.

УТОЧНЕННАЯ МЕТОДИКА ФОРМИРОВАНИЯ РЕЧЕПОДОБНЫХ ПОМЕХ

А.В. Сусов, А.А. Гавришев

Для защиты речевых сигналов (РС) от утечки по техническим каналам широко применяются активные средства защиты – генераторы акустического и виброакустического шума. Такие генераторы обычно построены на основе использования белого или розового шума. Вместе с тем известно, что белый или розовый шум, с точки зрения восприятия человека, не являются «близкими» к РС [1–3]. Поэтому для эффективного маскирования РС помеха должна иметь структуру, близкую к РС. Кроме того, используемый вид шума должен вносить минимальный дискомфорт при проведении переговоров. Многочисленные исследования показывают [1–3], что одним из самых перспективных видов помех в указанных условиях является речеподобная помеха (РП), схожая с настоящими РС. При этом более эффективной является помеха типа «речевой хор», состоящая из суммы нескольких РС [1–3]. Также известно, что одними из наиболее лучших свойств обладают РП, сформированные тем же голосом, каким был сформирован исходный РС. Указанные принципы положены в основу различных методик формирования РП, например, описанных в работах [1–3] и списках литературы к ним. Исследования, проводимые в данном направлении, несомненно являются актуальными и требуют дальнейшей проработки.

В данной работе авторами предлагается, с учетом работ [1–3], уточнение методики формирования РП в реальной обстановке, представленной в работе [3]. Уточненная методика формирования РП состоит из следующих шагов:

1) руководитель и его заместители, участвующие в конфиденциальных переговорах (не более 5 человек), одновременно зачитывают открытые документы, которые записываются в виде звуковых файлов с расширением .wav. В случае, если записываемая речь является исключительно мужской, то к ней необходимо добавить женскую речь, а в противном случае – мужскую. Кроме того, необходимо, чтобы непосредственно рядом с местом записи на достаточной громкости работал радиоприемник FM-диапазона, настроенный на одну из радиостанций;

2) в полученных записях программным методом удаляются паузы между словами;

3) программным методом звуковой файл разрезается на небольшие файлы со случайной длиной;

4) эти короткие файлы, выбранные случайным образом со случайным временным сдвигом, микшируются и стыкуются между собой, тем самым позволяя создавать файлы РП произвольной длины;

5) сформированные файлы РП сжимаются, переписываются на mp3-плейер и после усиления могут подаваться на средства активной защиты, например, на генератор шума «Барон», акустический подавитель «Троян 2» и др., либо использоваться совместно с ними.

Литература

1. Авдеев В.Б., Трушин В.А., Кунгуров М. А. Унифицированная речеподобная помеха для средств активной защиты речевой информации // Информатика и автоматизация. 2020. Т. 19. № 5. С. 991–1017.

2. Хорев А.А., Царев Н.В. Способ и алгоритм формирования речеподобной помехи // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2017. № 1. С. 57–67.

3. Куницын И.В., Лобашев А.К. Применение методов математического моделирования для оценки эффективности активной защиты акустической (речевой) информации [Электронный ресурс]. – Режим доступа : http://www.bnti.ru/showart.asp?aid=867&lvl=04.03.01. – Дата доступа: 02.05.2022.

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ IOT УСТРОЙСТВ

И.С. Терех, Е.А. Криштопова

В современных IoT экосистемах огромное количество датчиков, машин и других объектов отправляют данные по беспроводной связи на облачные сервера. Несмотря на множество возможностей для бизнеса, использование IoT-инфраструктуры несет риски информационной безопасности для компании и для отдельных пользователей.

Опросы западных потребителей показывают, 90 % из них не уверены в безопасности устройств IoT.

Проблемы информационной безопасности использования IoT делятся на две группы:

- повышение устойчивости подключенных устройств к кибератакам;
- защита конфиденциальности переедаемых персональных данных.

Разнообразие типов данных, мощностей и типов устройств IoT не позволяет создать универсальное техническое решение для любой инфраструктуры IoT и делает особенно важным правовые и организационные методы обеспечения безопасности.

Анализ имеющейся литературы, рекомендаций и практических реализаций показывает, что для обеспечения минимального уровня безопасности инфраструктуры IoT и данных ее пользователей необходимы уникальные пароли для подключенных устройств, сетевой адрес производителя для сообщений об уязвимостях, минимально требуемый срок обновления безопасности при продаже и эксплуатации устройств.

В дальнейшем необходимо развернуть работы над национальными, региональными и глобальными системами сертификации устройств IoT.

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТИ СТИРАНИЯ ДВОИЧНЫХ ДАННЫХ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

А.М. Тимофеев

Квантово-криптографические каналы связи в последние годы получают все большее развитие, поскольку они позволяют обеспечивать абсолютную скрытность и конфиденциальность передаваемых данных [1]. Это становится возможным при наличии высоконадежного оборудования, способного регистрировать оптические сигналы со средним числом фотонов не более десяти в расчете на каждый

передаваемый бит (символ) [2]. Поскольку в известных литературных источниках оценка надежности квантово-криптографических каналов связи отсутствует, это являлось целью данной работы. Объект исследования – квантово-криптографический канал связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа. Предмет исследования – оценка влияния интенсивности регистрируемого оптического излучения при передаче двоичных символов «0» J_0 на вероятность стирания этих символов $P(-/0)$. Установлено, что с увеличением J_0 зависимости $P(-/0)$ от J_0 спадают и, достигая своего наименьшего значения, переходят в насыщение. Получено, что минимальная вероятность ошибочной регистрации двоичных символов «0» для исследованного канала связи равна $0{,}11 \cdot 10^{-2}$ и соответствует $J_0 \geq 98{,}94 \cdot 10^{-2}$ отн. ед. и напряжению питания приемного модуля $U_{\text{пит}} = 52{,}54$ В, при которых мертвое время счетчика фотонов минимально, а его квантовая эффективность регистрации максимальна.

Литература

1. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]. Минск, Белорусская наука, 2007. 392 с.

2. Тимофеев А.М. Измерение вероятности стирания двоичного символа «0» в однофотонном асинхронном канале связи с приемником на основе счетчика фотонов // Приборы и методы измерений. 2021. Т. 12, № 2. С. 156–165.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КВАНТОВО-КРИПТОГРАФИЧЕСКОГО КАНАЛА СВЯЗИ С ПРИЕМНЫМ МОДУЛЕМ НА ОСНОВЕ СЧЕТЧИКА ФОТОНОВ

А.М. Тимофеев, Ю.В. Злобина

В настоящее время для защиты информации достаточно широко используют квантово-криптографические каналы связи, характеризующиеся абсолютной скрытностью и конфиденциальностью передаваемых данных [1]. Одной из наиболее важных характеристик этих каналов связи является пропускная способность $C_{\max}$, которая определяет максимальную скорость передачи информации [1, 2]. Для оценки пропускной способности квантово-криптографического канала связи необходимо построить его математическую модель, учитывающую мертвое время приемного модуля. Поскольку в известных литературных источниках математические модели указанного типа отсутствуют, это являлось целью данной работы. Объект исследования – квантово-криптографический канал связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа. Предмет исследования – построение математической модели асинхронного двоичного несимметричного однородного квантово-криптографического канала связи без памяти и со стиранием. На базе приемо-передающих устройств [3] создан квантово-криптографический канал связи, для которого построена математическая модель. По результатам выполненного математического моделирования установлено, что при прочих равных параметрах приема в диапазонах средних скоростей счета сигнальных импульсов при передаче двоичных символов «1» n_{s1}, на которых зависимости $C_{\max}(n_{s1})$ растут, увеличение средней длительности мертвого времени продлевающегося типа приводит к уменьшению пропускной способности канала связи.

Литература

1. Тимофеев А.М. Оценка влияния мертвого времени счетчика фотонов на скорость передачи информации в канале однофотонной связи // Вестник связи. 2019. № 6. С. 55–61.

2. Биккенин Р.Р., Чесноков М.Н. Теория электрической связи. М., Издательский цент «Академия», 2010. 336 с.

3. 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.

ОСОБЕННОСТИ ЭКРАНИРОВАНИЯ АППАРАТУРЫ, ПОДВЕРЖЕННОЙ ДЕЙСТВИЮ ВЧ- И СВЧ-ПОМЕХ

Н.А. Титович

При проектировании специальной аппаратуры, работающей в сложной электромагнитной обстановке. важно не только обеспечить ее защиту от воздействия ВЧ и СВЧ электромагнитных помех (ЭМП), но и исключить ее электромагнитные излучения, позволяющие извлечь информацию об особенностях работы. Отказы в работе быстродействующих и восприимчивых к воздействию ЭМП систем чаще всего являются обратимыми и поэтому трудно прогнозируемыми. Для сбоя в работе аппаратуры не требуется очень мощных источников помех.

Проведенные ранее исследования показали, что по характеру воздействия на полупроводниковые приборы (ПП) и интегральные микросхемы (ИМС) частотный диапазон ЭМП можно разделить на три области: 1) частота ВЧ помехи $f_п$ ниже граничной рабочей частоты $f_{гр}$ ПП и ИМС и в этом случае происходят функциональные сбои в их работе; 2) $f_п$ уже превышает $f_{гр}$ и поэтому времени воздействия помехи не всегда достаточно для переключения, а результат ее воздействия во многом зависит от соотношения фаз сигнала и помехи, происходят так называемые «перемежающиеся» сбои в работе микросхем; 3) в этой области уже начинает сказываться эффект детектирования огибающих СВЧ помех, появляются дополнительные напряжений смещения и изменения всех параметров: уровней логического нуля и единицы, времени задержки распространения при включении и выключении ИМС.

В ряде случаев вторая область отмеченного диапазона представляет наибольший интерес. В области «перемежающихся» сбоев под действием ЭМП могут происходить частые функциональные переключения. Известно, что наибольшее излучение ИМС наблюдается на частотах их переключения. В связи с этим потенциальному противнику может быть интересна информация о частоте этих излучений, которые проникают через отверстия для вентиляции и индикации в электромагнитных экранах. Следует учесть, что в момент переключения ИМС значительно возрастают потребляемые ими токи. Это может привести к изменению температурного режима микросхемы и сбою в ее работе. Очевидно, что, воздействуя на аппаратуру с частотой радиопомехи, равной частоте переключения ИМС, можно значительно удешевить решение задачи радиопротиводействия.

С учетом вышеизложенного возрастают требования к проектированию электромагнитных экранов для радиоаппаратуры. Важно учесть отмеченную особенность при расчетах размеров отверстий для вентиляции и индикации. Размер отверстия должен быть больше или меньше критического, при котором частота максимального проникновения ЭМП через экран равна граничной рабочей частоте переключения ИМС. Одновременно с повышением защитных свойств экрана к помехе уменьшается и излучение с частотой переключения ИМС. В ряде случаев эта задача решается с помощью применения специальных дополнительных тканых экранов.

ФОРМИРОВАНИЕ ПОРИСТОГО АЛЮМИНИЯ И ЕГО АНОДНОГО ОКСИДА ДЛЯ ИЗГОТОВЛЕНИЯ СЕНСОРНЫХ СТРУКТУР

Л.П. Томашевич, Н.А. Казимиров, Н.Н. Стешиц, К.А. Антипов

В последнее время большое внимание уделяется разработке новых материалов для чувствительного слоя и новых конструкций химических сенсоров, позволяющих измерять малые концентрации активных газов в окружающей среде. В последние несколько лет определилось новое направление в разработке данного типа химических сенсоров. Это направление связано с разработкой физических и химических методов увеличения удельной поверхности газочувствительных слоев сенсорных систем. Сенсорные устройства являются составной частью систем защиты электронной базы от нежелательных воздействий.

Поверхность наноструктурированного пористого алюминия, полученного методом электрохимического анодирования, может быть использована для создания на ней сенсорной структуры, электрофизические свойства которой зависят от влажности окружающей среды. В качестве исходного материала использовались пленки алюминиевой фольги толщиной 500 мкм. Наноструктурирование алюминиевой поверхности проводили с помощью метода электрохимического анодирования в 1 % водном растворе NaCl при анодном напряжении 50 В. Сам процесс длился 5 минут. Исследования, полученные с помощью растрового электронного микроскопа, показали, что в результате эксперимента были сформированы пленки пористого алюминия толщиной примерно 40-60 мкм. Данные пленки имеют пористую структуру кораллообразной формы. Диаметр пор варьируется от 0,8 до 2 мкм, минимальный размер на поверхности алюминиевого электрода составляет 50 нм. Далее на пористой алюминиевой поверхности формировали слой анодного оксида алюминия толщиной 100 нм при помощи электрохимического анодирования в 1 % водном растворе лимонной кислоты. Поверх анодного оксида алюминия осаждали никелевые электроды при помощи магнетронного распыления с использованием теневой маски.

Сформированные структуры показали чувствительность к изменению влажности окружающей атмосферы. При увеличении влажности окружающего воздуха на 10 % сопротивление структуры уменьшалось на 5–8 %.

Таким образом, проведенные исследования показали, что сформированные наноструктуры на основе пористого алюминия и его анодного оксида обладают сенсорными свойствами при изменении влажности окружающего воздуха, что позволяет их использовать в качестве сенсоров влажности.

ОСОБЕННОСТИ ЛАТЕРАЛЬНОГО ТОКОПЕРЕНОСА МЕЖДУ КОНТАКТАМИ МЕТАЛЛ-ПОЛУПРОВОДНИК

А.Г. Трафименко, А.Л. Данилюк

Актуальность исследований свойств контактов металл–полупроводник с барьером Шоттки в настоящее время не снижается в связи с их широким использованием в современной микро- и наноэлектронике. Наиболее часто при конструировании микроэлектронных устройств и моделировании токопереноса в контактах металл-полупроводник рассматривается только площадь контакта. Однако рост степени интеграции наноэлектронных приборов и уменьшение размеров активных элементов приводит к усилению влияния периферийных областей контактов металл-полупроводник. В ряде работ было показано, что даже на микроуровне нельзя полностью пренебречь влиянием периферии контакта на его приборные характеристики. При формировании контакта металл–полупроводник с барьером Шоттки возникает встроенное в контакт электрическое поле, распространяющееся

вокруг контакта на расстояние (ореол), в десятки раз превышающее размеры области пространственного заряда (ОПЗ). Это поле понижает электростатический потенциал контакта на значительную величину. Размер ореола и величина понижения электростатического потенциала в общем случае определяются величиной и знаком ОПЗ, которые зависят от диаметра контакта, а также концентрации и типа проводимости полупроводника [1, 2]. Данный круг вопросов в настоящее время все еще остается недостаточно изученным. Нет полной ясности о величине периферийной области, ее роли в общем токопереносе через контакт при прямых и обратных смещениях, мало исследована физическая природа периферийной области контакта металл–полупроводник с барьером Шоттки. Особый интерес представляют механизмы латерального токопереноса вдоль поверхности полупроводника между контактами металл-полупроводник [1].

В данной работе рассмотрены вопросы влияния периферийных областей двух металлических контактов, расположенных на поверхности кремния, на токоперенос между ними по приповерхностной области. Рассчитана глубина проникновения электрического поля в кремний в центральной части и периферийных областях контактов, распределение потенциала в окружающих контакты ореолах, установлены закономерности компенсации периферийного поля зарядом ОПЗ. Показано, что распределение потенциала в направлении нормальном к поверхности является немонотонным, сопровождающимся возникновением седловой точки, в которой напряженность поля равна нулю. В области периферии контактов распределение электрического поля становится неоднородным из-за наличия концентраторов поля на углах контактов, действия заряда ОПЗ и перепада потенциала, вызванного переходом к свободной поверхности кремния. Это приводит к неоднородности в распределении потенциала и ведет к нарушению равновесного состояния электронной системы полупроводника. Исследования токов растекания показали, что за счет электрических полей ореола по периметру контактов возникает проводящая область (периферия), приводящая к появлению токов утечки. Результаты расчетов тока из периферийной области инжектирующего контакта (эмиттера) в кремний показали, что
из-за неоднородного распределения напряженности поля периферии и ореола токоперенос вдоль поверхности является неустойчивым.

Литература

1. Торхов Н.А. Влияние периферии контактов металл–полупроводник с барьером Шоттки на их статические вольт-амперные характеристики // Физика и техника полупроводников. 2010. Т. 44, № 5. С. 615–627.

2. Tung R.T. The Physics and Chemistry of the Schottky Barrier Height // Applied Physics Reviews. 2014. Vol. 1. 011304.

$W_{18}O_{49}$ – НОВЫЙ ПРОЗРАЧНЫЙ ПРОВОДНИК С ЭКРАНИРОВАНИЕМ В ИК-ДИАПАЗОНЕ

Д.С. Федосеев, С.В. Гранько, Д.Б. Мигас

С помощью методов из первых принципов исследованы электронные и оптические свойства субстехиометрического оксида вольфрама ($W_{18}O_{49}$). Установлено, что это соединение является вырожденным полупроводником, так как уровень Ферми находится в зоне проводимости. Особенностью энергетического спектра $W_{18}O_{49}$ является наличие локализованного состояния в запрещенной зоне, вызванного формированием биполяронов из-за взаимодействия двух соседних атомов

вольфрама, и, как следствие, локализацией заряда. Расчет коэффициентов оптического поглощения и отражения указывает на наличие значительного поглощения и отражения при энергии фотонов менее 1 эВ, вызванного свободными носителями заряда с концентрацией ~10^{22} $см^{-3}$, за которым следует хорошо видимый пик около 1,1 эВ, обусловленный переходами с биполяронного состояния на свободные состояния в зоне проводимости. В районе энергий фотонов 1,2 – 2,8 эВ значения коэффициентов оптического поглощения и отражения падают практически до нуля, указывая на окно прозрачности в видимом диапазоне у $W_{18}O_{49}$. Для энергий фотонов, превышающих 3,0 эВ, происходит интенсивное поглощение за счет межзонных переходов. Таким образом, $W_{18}O_{49}$ представляет собой прозрачный в видимом диапазоне проводник, у которого наблюдается экранирование в ИК диапазоне за счет переходов, использующих биполяронные стояния.

УЯЗВИМОСТИ ФОТО- И ВИДЕОМАТЕРИАЛОВ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ DEEPFAKE

И.И. Фролов

Технологии машинного обучения получили уже достаточно широкое распространение не только в научно-исследовательской среде, но также стали применяться во многих сферах реальной экономики: многие бизнесы используют нейронные сети для анализа исторических данных (например, данные о продажах) [1] и прогнозирования развития будущей деятельности, основываясь на результатах анализа. В последние годы в определенной степени снизился порог входа в область анализа данных и работы с нейронными сетями за счет создания и продвижения отдельных готовых высокоуровневых библиотек, реализующих сложные алгоритмы машинного обучения.

Получив широкое распространение среди пользователей, появились и новые области применения нейросетевых алгоритмов: стали популярными приложения по обработке и синтезу изображений, видеопотоков. Одним из популярных направлений стали приложения, позволяющие моделировать и заменять изображения лица человека не только на статичном фотоизображении, но и для видеопотока. Появился даже отдельный термин «DeepFake» [2] для описания такого рода технологий. Поначалу подобные эксперименты использовались в развлекательных целях большинством пользователей сети, а также открывали более широкие перспективы развития киноиндустрии. Однако вскоре стало понятно, что подобное программное обеспечение может использоваться и в целях дискредитации популярных личностей шоу-бизнеса и политики, подготовки видео- или аудиосообщений для оказания влияния как на отдельные процессы в бизнесе (например, телефонный звонок, имитирующий указание руководителя перевести денежные средства на указанный банковский счет), так и на финансовые рынки (например, смонтированное видео-сообщение крупных игроков о слиянии компаний). Несмотря на краткосрочность таких действий (реальные личности быстро опровергают подделки), эффект может быть использован в корыстных целях.

Кроме перечисленных уязвимостей в видео- и аудиосообщениях более простым вариантом использования технологии DeepFake может быть имитация/моделирование изображения лица для несанкционированного доступа к, например, мобильным устройствам, предоставляющим доступ по биометрическим параметрам владельца.

Таким образом, актуальными является не только разработка алгоритмов машинного обучения и обработки фото- и видеоизображений для построения качественных моделей, используемых для реализации технологии «DeepFake», но исследования в области распознавания результатов применения технологии «DeepFake».

Литература

1. Прогнозирование спроса с помощью автоматизированного машинного обучения без кода в студии машинного обучения Azure [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/azure/machine-learning/tutorial-automated-ml-forecast. – Дата доступа: 02.05.2022.
2. What are deepfakes – and how can you spot them? [Электронный ресурс] – Режим доступа: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them. – Дата доступа: 02.05.2022.

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ ТЕХНОЛОГИИMOVING TARGET

О.А. Хацкевич, А.Д. Михейчик

На сегодняшний день некоторые атаки на сеть происходят из-за недоработки системных администраторов, специалистов по информационной безопасности, разработчиков. В качестве причин таких атак можно выделить: ошибка кода; пропуск критически важных обновлений средств защиты информации, либо телекоммуникационных средств; неправильная настройка оборудования. Данными недостатками могут воспользоваться злоумышленники, что может привести к серьезным последствиям. В данной работе предлагается использовать защиту сети с помощью подвижных целей (Moving Target Defense, далее – MTD). Технология MTD осуществляет постоянно меняющуюся (динамическую) поверхность атаки, из-за чего злоумышленники тратят большое количество времени на выбор цели атаки, а специалистам сети позволяет сфокусироваться на внутренних процессах. MTD создает ложную инфраструктуру, где динамически изменяются IP-адреса хосты, операционные системы, приложения и т.п. На сегодняшний день можно выделить три уровня защиты MTD.

1. Уровень сети. На данном уровне происходит изменение трафика путем рандомизации назначения портов, IP-адресов, а также подмена другой информации о хосте.
2. Уровень хоста. Здесь происходит модификация в узлах, в хостовых настройках, а также в операционных системах.
3. Уровень приложения. На этом уровне осуществляется изменения адресного пространства, исходного кода, типов приложений, а также непосредственно происходит изменение маршрутизации.

Таким образом, технология MTD является эффективным средством для обеспечения информационной безопасности благодаря тому, что позволяет уменьшить потребность в нахождении новых угроз, так как доступная поверхность для атаки все время динамически изменяется.

ТЕХНОЛОГИИ НЕЧЕТКОЙ ЛОГИКИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ПОЛНОТЫ И ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

А.В. Хижняк, Е.И. Хижняк

События сегодняшнего дня свидетельствуют о том, что риски вооруженной конфронтации передовых стран становятся, к сожалению, все более реальными. Отличие складывающейся ситуации от локальных конфликтов последних десятилетий состоит в том, что высокотехнологичные виды оружия будут как никогда востребованы. Их эффективное применение невозможно без современных автоматизированных систем управления (АСУ), характеризующихся углублением

интеграции в единый контур автоматизированного управления новых средств информационного обеспечения и огневого поражения. Совершенствование противником средств, форм и методов вооруженной борьбы обусловливает перманентное усложнение решаемых в АСУ задач (например, сбора и обработки информации, целераспределения и др.) и обусловливает функционирование в условиях существенной неопределенности. При этом неопределенности обычно делят на две группы: случайные и неопределенности нестохастической природы (например, поведенческая, целевая и (или) др.). Первая группа хорошо изучена и эффективно подлежит обработке на практике, обычно, когда закон распределения нормальный с априорно известными математическим ожиданием и дисперсией (или корреляционным моментом). Формализация второй группы факторов значительно более сложная ввиду отсутствия общей теории. Поэтому подходы к решению таких задач носят проблемно-ориентированный характер, который предполагает пошаговое выстраивание решения, отличное от уже известных. В таких задачах находят широкое применение современные популярные методы. Например, для преодоления трудностей, вызванных обработкой неопределенных знаний, широко используются технологии нечеткой логики. Многопараметрические задачи нелинейной оптимизации для адаптивного управления могут решаться на основе концепции обучения с помощью искусственных нейронных сетей. В рамках общей технологии системного моделирования может применяться комплексирование нескольких различных моделей для взаимного усиления достоинств каждой из них. Обязательным условием верификации при создании новых моделей и алгоритмов является наличие научно-исследовательского инструментария, обычно, представляющего собой аппаратно-программный комплекс.

В Военной академии Республики Беларусь разработан программно-аппаратный комплекс, позволяющий вычислять показатели качества решения задачи сбора и обработки информации о воздушной обстановке в многоуровневых иерархических структурах АСУ. Модульность его построения дает возможность количественно оценивать показатели качества траекторной (третичной) обработки не только различных алгоритмов в целом, но и контроля и оценки качества отдельных его этапов. Созданный инструментарий способствовал не только разработке, но и обоснованию эффективности нового способа обработки траекторных измерений в условиях высокой плотности воздушных объектов, основанный на многоэтапной оптимизационной процедуре нечеткой автоматической классификации, что позволило повысить значение точности определения текущих координат до двух раз, а быстродействие не менее, чем на два порядка, обеспечив значения полноты и достоверности близкими к единице.

Литература

1. Хижняк А.В. Оптимизационный метод нечеткой автоматической классификации в задаче объединения оценок траекторных измерений в радиолокационной системе. // Доклады БГУИР. 2020. Т. 18, № 2. С. 89–95.

2. Белоус А.А., Хижняк А.В., Шевяков А.В. Метод объединения радиолокационной информации на основе нечеткой классификации // Инженерный вестник. 2010. № 3 (29). С. 38–43.

СТЕГАНОГРАФИЧЕСКИЙ ПРОГРАММНЫЙ МОДУЛЬ

О.Д. Чкоидзе

Актуальность стеганографии заключается в том, что этот метод передачи информации является наиболее скрытным в реалиях новых информационных технологий. Основной задачей стеганографического программного средства является встраивание в цифровое изображение данных, предназначенных для передачи по стегоканалу, таким образом, чтобы исходное изображение было максимально схожим с результирующим. Стеганографическое программное средство должно использовать наиболее эффективные и актуальные стеганографические методы. Такими методами являются: метод наименьшего значащего бита (НЗБ) и метод дискретного косинусного преобразования (ДКП) [1]. Главным преимуществом НЗБ является достаточное количество бит, которое возможно записать в одно цифровое изображение, однако этот метод весьма неустойчив при сжатии изображения. ДКП в свою очередь достаточно устойчив к сжатию, но доступное количество бит для записи в разы меньше по сравнению с НЗБ. Важным элементом любого стеганографического программного средства является шифрование. В связи с возможной частичной потерей данных, алгоритмы симметричного шифрования наиболее применимы для задач стеганографии. Потеря данных обычно связана с особенностью сжатия некоторых форматов цифровых изображений.

Необходимо отметить, что при использовании вышеперечисленных стеганографических методов, возникает проблема извлечения встроенных данных, так как в случае разработанного программного средства, они могут быть распределены по нескольким цветовым каналам цифрового изображения и иметь разный размер. Поэтому, обязательной процедурой будет протоколирование процесса извлечения данных. Для этого был разработан отдельный алгоритм, отвечающий за определение размера и количества сегментов данных в каждом цветовом канале.

Литература

1. Global Journal of Computer Science and Technology. An Analysis of LSB & DCT based Steganography [Электронный ресурс]. – Режим доступа: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.178.7157&rep=rep1&type=pdf – Дата доступа: 30.04.2022.

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ КОМПЛЕКСИРОВАНИЯ ИЗОБРАЖЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ ЗЕНИТНЫХ УПРАВЛЯЕМЫХ РАКЕТ С ОПТИЧЕСКИМИ ГОЛОВКАМИ САМОНАВЕДЕНИЯ

Д.С. Шарак, А.О Гирко

Проводимые военные операции в ходе военных конфликтов подразумевают массированное применение средств воздушного нападения (СВН), которые рассматриваются в качестве основной ударной силы [1].

Одним из рубежей применения зенитных ракетных средств в системе ПВО является рубеж сверхмалой дальности (непосредственного прикрытия) – до 5 км, на котором активно применяются зенитные ракетные комплексы (ЗРК), использующие зенитные управляемые ракеты (ЗУР) с оптической головкой самонаведения (ОГСН).

Проведенные исследования показывают, что применение комплексирования изображений при стрельбе ЗРК, оснащенного ОГСН, приводит к повышению показателей эффективности данного ЗРК [2].

В соответствии с разработанной методикой на первом этапе задаются условия проведения моделирования и расчетов, которые являются исходными данными и в дальнейшем используются при расчетах соответствующих вероятностей.

На втором этапе определяются вероятности устойчивого сопровождения для работы ЗРК в различных режимах ($P_{\text{сопр}}^{\text{тв}}$, $P_{\text{сопр}}^{\text{ик}}$, $P_{\text{сопр}}^{\text{компл}}$).

Далее с использованием исходных данных определяются вероятности пуска ракеты в различных режимах работы ($P_{\text{П}}^{\text{тв}}$ $P_{\text{П}}^{\text{ик}}$, $P_{\text{П}}^{\text{компл}}$).

На пятом этапе с использованием исходных данных определяется вероятность обнаружения цели для заданных условий ($P_{\text{обн}}^{*}$).

Далее с учетом данных блока 1 определяются вероятности выполнения огневой задачи подразделением в различных режимах работы ($P_{\text{о.з}}^{\text{тв}}$, $P_{\text{о.з}}^{\text{ик}}$, $P_{\text{о.з}}^{\text{компл}}$).

Стоит также отметить что при расчетах принимается:

$P_{*}^{\text{тв}}$, $P_{*}^{\text{ик}}$, $P_{*}^{\text{компл}}$ – вероятности при работе ЗРК в видимом, ИК-диапазонах, а также в случае применения комплексирования изображений, соответственно.

Вывод о предпочтительном режиме работы ЗРК для заданных условий делается на основании сравнения соответствующих значений вероятностей выполнения огневой задачи.

Проведенное моделирование показало, что эффективность ЗРК, использующего ЗУР с ОГСН можно повысить в случае применения комплексирования изображений видимого и ИК-диапазонов. Комплексирование в сложных условиях обеспечивает повышение вероятностей устойчивого сопровождения захваченной цели ($P_{\text{сопр}}$), пуска ракеты ($P_{\text{П}}$), что, в конечном итоге, приводит к увеличению вероятности выполнения огневой задачи ($P_{\text{о.з}}$), являющейся общим показателем эффективности стрельбы огневой единицы.

Литература

1. Справочник офицера воздушно-космической обороны / Ю. Г. Аношко [и др.]; под общ. ред. С. К. Бурмистрова. Тверь: ВА ВКО, 2005. 564 с.

2. Шарак Д.С., Липлянин А.Ю., Хижняк А.В. Комплексирование изображений в следящем координаторе целей головки самонаведения для повышения эффективности стрельбы зенитно-ракетного комплекса типа «Стрела-10М2» // Доклады БГУИР. 2018. № 8 (118). С. 108–115.

ВЛИЯНИЕ УСЛОВИЙ АНОДИРОВАНИЯ НА ПРЕДЕЛ ПРОЧНОСТИ СВОБОДНЫХ ПЛЕНОК АНОДНОГО ОКСИДА АЛЮМИНИЯ

М.А. Шахвердиев, С.А. Биран, К.В. Гарифов, Д.А. Короткевич, А.В. Короткевич

Микроэлектромеханические системы (МЭМС) находят широкое применение в высокочастотных системах связи. Большинство радиочастотных компонентов, таких как катушки индуктивности, переменные конденсаторы и переключатели, являются решающими элементами для производительности беспроводных устройств, работающих на высоких частотах [1]. Эксплуатационные характеристики МЭМС устройств определяются механическими свойствами материала, на основе которого они изготовлены. Анодный оксид алюминия позволяет контролировать свои механические свойства в процессе получения, за счет изменения параметров анодирования, что делает его отличным выбором при изготовлении МЭМС устройств.

Образцы для исследования предела прочности представляли собой свободные пленки анодного оксида алюминия длиной 50 мм и шириной 9 мм. Для исследования были выбраны следующие режимы анодирования: двухстороннее сквозное анодирование, одностороннее сквозное анодирование, не сквозное двухстороннее

анодирование (время анодирование варьировали от 1 до 3 часов). Для исследования придела прочности полученных образцов, к ним прикладывали механическую нагрузку. Придел прочности образцов с двухсторонним сквозным анодированием составил 1,7 Н, для образцов с односторонним сквозным анодированием 1,45 Н. При исследовании придела прочности образцов, которые анодировались с двух сторон не насквозь, было замечено, что в зависимости от толщины оксида их механические свойства различаются. Образцы с толщиной оксида 50 и 85 мкм (2 и 3 часа анодирования соответственно), при достижении своего предела прочности (нагрузка в 1,55 Н), ломались, а образец с толщиной оксида 30 мкм вел себя иначе. При нагрузке массой 0,75 Н оксид потрескался, но при этом при снятии нагрузки образец возвращался в исходное состояние. При нагрузке в 0,9 Н происходила уже пластичная деформация образца, и он не возвращался в исходное состояние.

Литература

1. Eloe J.C. MEMS and Nano Divrgence: Status of MEMS industry. Yole development, 2021.

ДЛЯ ЗАМЕТОК

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XX Белорусско-российской научно-технической конференции
(Республика Беларусь, Минск, 7 июня 2022 года)

В авторской редакции
Ответственный за выпуск *Т. В. Борботько*
Компьютерная верстка *О. В. Бойправ*

Подписано в печать 23.05.2022. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 13,25. Уч.-изд. л. 10,8. Тираж 100 экз. Заказ 64.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий №1/238 от 24.03.2014, № 2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск