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

# ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Тезисы докладов**
**XVIII Белорусско-российской научно–технической конференции**
**(Минск, 9 июня 2020 г.)**

**Минск БГУИР 2020**

УДК 004.56.5
ББК 32.972.5
Т38

**Редакционная коллегия**

**Т.В. Борботько, Л.А. Шичко, В.Ф. Голиков, Г.В. Давыдов,
В.К. Конопелько, Л.М. Лыньков**

**НАУЧНЫЙ ПРОГРАММНЫЙ КОМИТЕТ**

| | |
|---|---|
| Богуш В.А. | ректор БГУИР, председатель |
| Борботько Т.В. | зав. кафедрой защиты информации БГУИР, зам. председателя |
| Осипов А.Н. | проректор по научной работе БГУИР |
| Шелупанов А.А. | президент ТУСУР (Российская Федерация) |
| Филиппович А.Г. | Оперативно-аналитический центр при Президенте Республики Беларусь |
| Горбач А.Н. | директор Государственного предприятия «НИИ ТЗИ» |
| Голиков В.Ф. | профессор кафедры информационных технологий в управлении БНТУ |
| Маликов В.В. | Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь |
| Иванов А.В. | зав. кафедрой защиты информации НГТУ (Российская Федерация) |
| Харин Ю.С. | директор НИИ прикладных проблем математики и информатики БГУ |
| Хижняк А.В. | начальник научно-исследовательской лаборатории кафедры автоматизированных систем управления войсками Военной академии Республики Беларусь. |
| Хорев А.А. | зав. кафедрой информационной безопасности МИЭТ (Российская Федерация) |

**ОРГАНИЗАЦИОННЫЙ КОМИТЕТ**

| | |
|---|---|
| Борботько Т.В. | зав. кафедрой защиты информации БГУИР, председатель |
| Бойправ О.В. | доц. кафедры защиты информации БГУИР, зам. председателя |
| Белоусова Е.С. | доц. кафедры защиты информации БГУИР |
| Шичко Л.А. | нач. ОМНК НИЧ БГУИР. |

Т-38 **Технические** средства защиты информации : тез. докл. XVIII Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 9 июня 2020 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2020. – 88 с.
ISBN 978-985-543-513-7

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

**УДК 004.56.5**
**ББК 32.972.5**

**ISBN 978-985-543-513-7**

© УО «Белорусский государственный университет информатики и радиоэлектроники», 2020

# ОГЛАВЛЕНИЕ

**SMILE BIOMETRIC IMPRINT CREATION WITH THE USE OF AUTOENCODER**

B.A. Assanovich, N.N. Bich, A.F. Pronevich

Non-contact biometric identification and autentification methods with high reliability and security have become very popular in recent years in both social and financial areas. A new biometric imprint was proposed, which is obtained from smile video using stacked autoencoder that allows to build a biometric cryptosystem based on fuzzy commitment [1]. Despite the fact that there are a number of techniques that use facial dynamics to identify a person with the use of various spatio-temporal parameters of face, the deep learning methods are increasingly being exploited for various recognition tasks. Classical linear methods of image processing and feature extraction based on principal components analysis (PCA) are replaced by non-linear transformations. Compared with PCA, the use of an autoencoder significantly increases the classification accuracy, especially with a large number of items [2]. In our setup we applied so-called stacked autoencoder (SAE) that is a neural network including several layers of sparse autoencoders where output of each hidden layer is connected to the input of the successive hidden layer. In this case the hidden layers are trained in an unsupervised way and then fine-tuned by a supervised method.

The use of SAE will allow the use of the trained data of the output layer of the neural network as features for biometric separation of users into genuine and imposters (persons who pretends to be somebody else). The effectiveness of user comparisons depends on similarity rates, which are often determined by the distribution of root mean square (RMS) distances of their characteristics. The more the two distributions are separated and the smaller the standard deviation for each distribution, the better the separation of the classified classes. This property of distributions is estimated by such a parameter as decidability index

Recent research has shown that neural networks like autoencoders have better performance in feature separation compared to PCA technique. Inspired by a possible improvement in the classification characteristics, we used an auto-encoder to obtain biometric data on a person's smile and bind them to a secure user key. Due to the fact that biometric data has instability, error correction codes (ECCs) should be adopted to ensure that fuzziness of biometric data can be alleviated.

According to our knowledge, the use of auto-encoders to create a biometric imprint from face dynamics the context of implementing Biometric Cryptosystem (BC) and linking the secret key to a human smile have not been considered before. We have introduced the term smile-imprint of the user for biometric data $Y$ obtained from the SAE output layer and then used to obtain the personal key with the use of error correcting codes (ECC),

Despite the widespread use of binary BCH codes, recently, interest has grown in non-binary ECC, which also found the application in the creation of Physical Unclonable Function (PUF) for secure storage of cryptographic keys and tamper-detection systems.

Using the designed FaceAnalizer program [3] video was obtained with a person's smile and its three phases: 1.onset (neutral to expressive) phase; 2.apex; and 3.offset phase (expressive to neutral), describing the state of a smiling person's face, were detected and analyzed.

A series of experiments with different dimensions of the intermediate layers were performed with SAE to get good compact biometric features. To reduce time spent, in these experiments the subsets of 40 subjects randomly selected from the entire UvA-NEMO Database were used, reproducing a posed smile. Then normalized grayscale images of from corresponding video of 112x112 pixels in size, scaled to 50%, creating a vector length of the input layer of 0.5x112x112=6272 elements have been used for unsupervised learning of SAE. The results obtained have shown much better performance compared to baseline methods.

**References**

1. Juels A., Wattenberg M. A fuzzy commitment scheme // Proc. ACM Conf. on Computer and Communications Security. – 1999. – P. 28–36.

2. Mei Wang, Weihong Deng. Deep Face Recognition: A Survey // Computer Vision and Pattern Recognition. – arXiv:1804.06655 https://arxiv.org/abs/1804.06655.

3. Assanovich B., Veretilo Yu. Biometric database based on HOG structures and BCH codes // Proc. ITS. – 2017. – P. 286–287.

## ALGORITHMS OF IMAGE PROCESSING BASED ON GAUSSIAN AND LAPLACIAN PYRAMIDS

I. Baryskievic, M. Hussein

The rapid development of sensor technologies has given impetus to the widespread use of multisensory systems in computer vision applications, remote monitoring of objects, as well as for medical and military purposes. The result of using multisensory systems has been a rapid increase in the amount of information to be processed and stored. To provide an effective method of reducing data flow, algorithms for combining images are developed that ensure the preservation of useful information obtained from the source images [1].

An algorithm for the significance map synthesis based on the analysis of low-level image properties (intensity, color, orientation), the formation of a Gaussian pyramidal structure, the calculation of characteristic maps and visibility maps by intensity, color and orientation, and the calculation of the resulting significance map of the original image is developed. It is shown that the multisensory image representation as a pyramidal structure is effective for detecting low-contrast objects.

An algorithm for image enhancement based on combining source images using the Laplacian pyramid is proposed. The developed algorithm is efficient for use in both single-sensor and multi-sensor systems.

The simulation of the algorithms was performed in Matlab programming environment. It was found that the best results for significance map synthesis could be achieved for Laplacian pyramid. For image enhancement algorithm, the smallest standard error is ensured by using a three-level pyramidal structure.

**References**

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

## DEVELOPMENT RELIABILITY NODE FAULT-TOLERANT COMPUTING SYSTEMS BY PARALLEL TECHNICS.

Kamil Iehab Abduljabbar Kamil, M.B. Abrosimov

Reliability and availability have become increasingly important in today's computer-dependent world. In many applications where computers are used, outages or malfunction can be expensive, or even disastrous. Which includes high availability, improved throughput and response time. Due to the complexity of such systems, it is impossible to improve computer performance using a single processor, the system must be able to operate correctly despite the presence of certain faults. Fault-tolerance the important technique used to the ability of a system to continue performing its intended function, in spite of faults maintains dependability in these systems. In a broad sense, fault tolerance is associated with reliability. The theory of fault tolerance in graphs as a mathematical model for fault tolerance in computers was introduced in a seminal paper by Hayes [1]. In fault-tolerant systems, spare components are needed so that when some basic component fails, their tasks are dynamically transferred to the spare component. The problem here is to minimize the number of spare components that are needed for the network to become fault-tolerant and deciding whether graphs are isomorphic. In general, the implementation of a serial based graph algorithm is time-consuming as the number of vertex and edge in graph increases as the size of the graph increases [2]. Recently there have been increasing graph applications with large sizes because of increasing big data provided [3, 4]. Due to these large data, the parallel implementation of graph algorithms is more effective than serial-based implementation. we need to parallel algorithm and special approach for contemporary massively parallel computers that run efficiently and general technique for generating families of combinatorial objects without isomorphs. In our theses, we used random graphs from vertices of small size to up to 9 vertices. The experimental results show that the proposed approach brings a considerable improvement in performance and efficiency compared to the CPU-based results. Our result also shows high performance, especially on large graphs.

**References**

1. Hayes J.P. A graph model for fault-tolerant computing system // IEEE Transactions on Computers. – 1976. – Vol. C-25, no. 9. – P. 875–884. – DOI: 10.1109/TC.1976.1674712.

2. Ullmann J.R. An algorithm for subgraph isomorphism // Journal of the ACM (JACM). – 1976. – Vol. 23. – P. 31-42.

3. A (sub)graph isomorphism algorithm for matching large graphs / L.P. Cordella [et al.] // Pattern Analysis and Machine Intelligence. – 2004. – Vol. 26. – P. 1367–1372.

4. An Improved Algorithm for Matching Large Graphs / L.P. Cordella [et al.] // 3rd IAPR-TC15 workshop on graph-based representations in pattern recognition. – 2001. – P. 149–159.

## ИЗУЧЕНИЕ ВОПРОСОВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТИ «ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

В.М. Алефиренко

Учебный план специальности «Электронные системы безопасности» [1] включает в себя как компонент учреждения высшего образования дисциплину «Методы и технические средства обеспечения безопасности», которая читается на 3 курсе в 2-х семестрах и состоит из 2-х частей: «Методы и технические средства обеспечения безопасности информации» и «Методы и технические средства обеспечения безопасности объектов». Первая часть и посвящена изучению вопросов, связанных, в первую очередь, с техническими методами и средствами защиты информации. Эта часть делится на 3 самостоятельных, но логически взаимосвязанных раздела. В первом разделе – «Общие вопросы защиты информации», рассматриваются вопросы, связанные с понятием и видами информации, обеспечением ее безопасности, рассматривается концептуальная модель информационной безопасности и ее компоненты, модель построения системы информационной безопасности предприятия, угрозы, источники угроз и уязвимости конфиденциальной информации, действия, приводящие к неправомерному овладению конфиденциальной информацией, а также основные направления обеспечения информационной безопасности. Во втором разделе – «Каналы утечки и технические методы скрытого съема информации», рассматриваются вопросы, связанные с причинами и условиями утечки информации, рассматриваются средства переноса информации, дается понятие канала утечки, приводится классификация и общая характеристика каналов утечки, рассматриваются методы и технические средства скрытого съема аудио- и видеоинформации, а также методы и технические средства скрытого съема информации в электромагнитных и оптических каналах передачи информации. В третьем разделе – «Методы и технические средства защиты информации», рассматриваются методы и технические средства защиты, обнаружения и противодействия в акустических каналах передачи информации, в телефонных линиях связи, в электромагнитных и оптических каналах передачи информации, основные методы защиты информации в персональных компьютерах и сетях ЭВМ, криптографические и стеганографические методы защиты информации, включая компьютерную стеганофонию, а также защита электронных документов с помощью электронной цифровой подписи.

Как показала практика, изучение этих вопросов, связанных с технической защитой информации и подкрепленных лабораторными и практическими занятиями, позволяет студентам-дипломникам выполнять дипломные проекты не только по тематике обеспечения безопасности объектов, но и по обеспечению безопасности информации.

**Литература**

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

## ИССЛЕДОВАНИЕ СТЕГАНОФОНИЧЕСКИХ МЕТОДОВ СКРЫТИЯ ИНФОРМАЦИИ

В.М. Алефиренко, Д.А. Никитенко

Компьютерная стеганофония позволяет не только скрывать текст и графические изображения в аудиофайлах, но и преобразовывать сам текст и изображения в аудиофайлы, в которых, при необходимости, также может быть скрыта соответствующая информация. Эти возможности позволяют использовать стеганофонические методы для скрытой передачи текстовой и графической информации, встроенной в аудиофайлы, по открытым каналам связи. Постановка подписи или специальных графических меток в аудиофайлах позволяет осуществить защиту авторских прав текстового, графического или музыкального произведения.

Для проведения исследований использовались такие программные средства, как Virtual ANS, позволяющее представлять аудиофайлы в виде сонограммы и Sonic Visualiser, позволяющее просматривать и анализировать содержимое аудиофайлов в виде фонограммы, спектрограммы и сонограммы. Для анализа были выбраны два аудиофайла, представляющие собой речь (стихотворение) и музыку (музыкальное произведение), а также графическое изображение, представляющее собой цветную репродукцию картины. Исходные файлы и графическое изображение импортировались в программное средство Virtual ANS, после чего на различные участки полученной сонограммы наносился короткий текст. Затем аудиофайл экспортировался в формат .jpeg или .png и вновь импортировался в Virtual ANS. Проводилось сравнение исходных и полученных аудиофайлов на слух и изображений их сонограмм. Для более детального исследования с помощью программного средства Sonic Visualiser проводился анализ спектрограмм файлов.

Как показали исследования, при импортировании исходных аудиофайлов происходят искажения в области нижних частот, что при их прослушивании несколько отражается на качестве (более глухое, удаленное звучание). Искажения наблюдаются и в нижней части картины, соответствующей на сонограмме нижним частотам. Это обусловлено особенностью программы Virtual ANS, так как она является симулятором фотоэлектронного синтезатора АНС [1]. Поэтому постановка текста или графических изображений в области нижних частот приводила к их искажению. В то же время их постановка в области верхних частот практически не влияла на качество прослушивания аудиофайлов и не приводила к их искажению на картине. Исследование спектрограмм пиковых частот с помощью программы Sonic Visualiser позволяло определять диапазон частот, в которых постановка текста или графических изображений приведет к заметному искажению качества воспроизведения аудиофайлов.

**Литература**

1. Апресов С. Полновластные правители звуков // Популярная механика. – 2015. – № 4.

## ПРОЦЕССЫ ВОССТАНОВЛЕНИЯ БЛАГОРОДНЫХ МЕТАЛЛОВ НА ПОВЕРХНОСТИ ПИРОГЕННОГО КРЕМНЕЗЕМА

М.Ф.С.Х. Аль-Камали

Введение соединений металлов в структуру объемных силикатных матриц возможно с применением различных технологических приемов, основные из которых включают в себя сплавление исходных материалов (применяется при получении глазурей, стекол и стеклокерамических веществ) или компактированием исходных реагентов из шихты с последующей термообработкой сформированной заготовки в контролируемой газовой среде (используется при получении керамики и металлокерамики). В нашем случае, проводились исследования по модификации поверхности высокопористого пирогенного кремнезема (аэросила) солями металлов – путем введения их в водную дисперсию аэросила с последующим преобразованием золя в ксерогель (сушкой гелей на воздухе по заданному температурному режиму). Получившиеся ксерогели обладали оптимальной однородностью распределения

соединений металлов по всему объему сформированной высокопористой матрицы (в качестве соли-допанта использовался нитрат меди). Дальнейшая термообработка на воздухе упрочняла кремнийкислородный каркас ксерогеля и приводила к трансформации нитрата меди в оксид меди (II). Последующая обработка композиционных материалов состава $SiO_2$:CuO в среде осушенного водорода позволяла получать системы состава $SiO_2$:$Cu^o$. Во всех случаях конечная температура формирования матриц составляла 800 ºС (время выдержки на указанной температуре – 1 ч). Получившиеся ксерогели размалывались до состояния микропорошков, которые методом одноосного прессования компактировались в таблетированные мишени различного геометрического размера ($d \sim 13$–$83$ мм). Изучение поверхности микропорошков, прошедших структурирующую термообработку, методом сканирующей электронной микроскопии позволило установить, что оксид меди формируется в $SiO_2$-матрице в виде отдельной микродисперсной фазы, а восстановленная медь «обволакивает» поверхность $SiO_2$-глобул, образуя, фактические, сплошную тонкую 2-D структуру по всему внутреннему объему ксерогеля. Проведенные исследования показали возможность использования полученных таблетированных материалов в качестве мишеней для напыления в вакууме: система $SiO_2$:$Cu^o$ использовалась для распыления электронным пучком, а $SiO_2$:CuO – для магнетронного распыления. Структура покрытий получалась достаточно однородной с высокой адгезией сформировавшееся тонкой пленки к поверхности подложки, в качестве которой использовались полированные кремниевые пластины.

## ПОМЕХОУСТОЙЧИВЫЙ КАНАЛ ПЕРЕДАЧИ ДАННЫХ ДЛЯ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Е.И. Асауляк, Т.Н. Дворникова

В системах цифровой передачи информации при прохождении сигнала по каналу передачи данных сигнал подвергается различным изменениям (искажениям) под действием шумов. Это ведет за собой нарушение целостности передаваемой информации и может привести к сбоям в работе различных систем, например, получение ложной информации со спутника, принятие не правильных решений при наведении на цель, не корректный обмен информацией между системами и т. д. В связи с этим, введение помехоустойчивого кодирования является актуальной задачей при разработке системы передачи цифровой информации.

Для противодействия шуму, которому подвигается информация при передаче ее через канал передачи данных используются различные методы борьбы с ним. Одним из методов – это введение в систему передачи цифровой информации помехоустойчивое кодирование.

Помехоустойчивое кодирование канала – кодирование с исправлением ошибок, представляющее собой метод обработки сигналов, предназначенный для увеличения надежности их передачи по цифровым каналам за счет специальной вводимой избыточности [1]. Используя правильный метод помехоустойчивого кодирования и декодирования можно добиться практически полного исправления всех ошибок, возникающих в канале передачи данных.

Большую популярность помехоустойчивое кодирование получило с развитием БИС. Данный метод позволил более чем на 10 дБ повысить производительность при значительно меньших затратах по сравнению с другими методами, например, методами увеличения мощности передатчика или размера антенны [2].

В помехоустойчивом кодировании широкое применение нашли сверточные коды. Сверточный код происходит от того, что в результате кодирования на выходе кодера образуется свертка кодируемой информации с импульсной реакцией кодера. Основная суть сверточного кодирования состоит в последовательном преобразовании информационной последовательности в кодовую последовательность, которое происходит непрерывно. Также они занимают меньшую полосу частот и могут использоваться как одной из основ конструкции для других кодов.

Для оценки достоверности передачи с использованием сверточного кодера и без него использовалась среда имитационного моделирования MATLAB. Установлено, что применение

сверточного кодера позволяет повысить достоверность при передаче информации через канал передачи данных. Преимуществами использования сверточного кодирования являются: простота реализации, кодирование и декодирование потоков данных непрерывно во времени, не нуждаются в блоковой синхронизации, путем моделирования можно определить оптимальные коды.

**Литература**

1. Рихтер С.Г. Кодирование и передача речи в цифровых системах подвижной радиосвязи. – М.: Горячая линия – Телеком, 2018. – 302 с.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

## АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ

Ф.А. Бабенко, Т.П. Тынкович

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был невелик, так как зависимость мировой экономики от информационных технологий была мала. В настоящее время в условиях значительной зависимости бизнеса от электронных средств доступа и обмена информацией и постоянно растущего числа атак ущерб от самых незначительных атак, приводящих к потерям машинного времени, исчисляется миллионами долларов, а совокупный годовой ущерб мировой экономике составляет десятки миллиардов долларов.

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации, сосредоточение в базах данных информации различного уровня важности и конфиденциальности, расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети, увеличение числа удаленных рабочих мест, широкое использование глобальной сети Internet и различных каналов связи, автоматизация обмена информацией между компьютерами пользователей.

Корпоративная информационная система представляет собой сложную структуру, в которой объединены различные сервисы, необходимые для функционирования компании. Эта структура постоянно меняется – появляются новые элементы, изменяется конфигурация существующих. По мере роста системы обеспечение информационной безопасности и защита критически важных для бизнеса ресурсов становятся все более сложной задачей.

Для того чтобы выявить недостатки защиты различных компонентов и определить потенциальные векторы атак на информационные ресурсы, проводится анализ защищенности. Эффективный способ анализа – тестирование на проникновение (пентест), в ходе которого моделируется реальная атака злоумышленников. Цель тестирования – обнаружить возможные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу от обслуживания, а также спрогнозировать возможные финансовые потери и экономические риски.

Технологии информационной безопасности очень быстро устаревают, решение, оптимальное для предприятия заказчика на данный момент, не будет таковым через некоторое время. Поэтому многие специалисты по информационной безопасности рекомендуют проводить penetration test на регулярной основе, наилучшее решение – ежегодно.

**Литература**

1. Конеев И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с

2. Олифер В.Г. Олифер Н.А. Компьютерные сети: 2-ое изд. – М.: Вильямс, 2007. – 1410 с.

3. Коллинз М. Защита сетей. Подход на основе анализа данных. – М.: ДМК, 2019. – 308 с.

## ФОКУСИРОВКА СВЧ-ЭНЕРГИИ С МАКСИМАЛЬНОЙ ЭФФЕКТИВНОСТЬЮ

И.В. Баженова

В работе предлагается технология проверки, настройки с целью идентификации элементов-фазовращателей цифровой управляемой фазированной антенной решетки (ФАР) СВЧ диапазона малопараметрической РТС, предназначенной осуществлять фокусировку СВЧ-энергии электромагнитного поля с максимальной эффективностью. Измерительная установка позволяет выполнять измерения и давать оценку разброса параметров цифровых фазовращателей с высокой точностью и контролировать качество их настройки.

Управляемая антенная система типа фазированной антенной решетки является весьма важной системой в малопараметрической адаптивной РТС фокусировки СВЧ-энергии, выполняя роль пассивной проходной радиолинзы круговой поляризации, начиненной фазовращателями с цифровым управлением. Применение системы такого типа с достаточно большой апертурой с целью получения сформированного электромагнитного поля вблизи раскрыва и диаграммы фокусировки позволяет реализовать основные принципы и работоспособность РТС. Для этого фазированная антенная решетка должна быть предварительно настроена. В данном случае такая антенна представляет собой непрерывную управляемую антенную систему, способную обеспечить достижение максимально возможной эффективности фокусировки и плотности концентрированной СВЧ энергии в заданной точке пространства. С этой целью необходимо использовать по всему раскрыву фазовращатели ФАР с идентичными техническими характеристиками. Такие требования вполне выполнимы с помощью проведения предварительных настроечных юстировочных работ, направленных на идентифицирование фазовращателей по техническим характеристикам.

Основными характеристиками фокусирующей антенной решетки являются диаграмма фокусировки и плотность потока мощности в фокальном пятне при заданной мощности передатчика. Первое характеризует распределение СВЧ мощности в пространстве, а второе коэффициент передачи всей системы.

**Литература**

1. Охрименко А.Е. Основы извлечения, обработки и передачи информации. Ч. 1. Обнаружение и временная обработка одиночных сигналов. Мн.: МРТИ, 1994. – 138 с.

2. Охрименко А.Е. Основы обработки и передачи информации. // Мн.: МВИЗРУ ПВО, 1990. – 180 с.

## МЕТОДИКА ЗАКРЕПЛЕНИЯ ИНКОРПОРИРОВАННЫХ ЧАСТИЦ АЛЛОТРОПНЫХ ФОРМ УГЛЕРОДА В ВОЛОКНИСТОМ МАТЕРИАЛЕ ДЛЯ ПОЛУЧЕНИЯ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Е.С. Белоусова, О.В. Бойправ, М.С.Х. Аль-Махдави

Тематика исследований, результаты которых представлены в данной работе, соответствует одному из приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг. и посвящена разработке новых композиционных материалов на основе аллотропных форм углерода. В работе [1] представлена методика создания гибких углеродосодержащих поглотителей электромагнитного излучения на основе волокнистых материалов с включением частиц технического углерода. Особенность данной методики заключается в пропитке волокнистого материала водным углеродосодержащим раствором. Однако в ней не предусмотрен способ закрепления частиц углерода в структуре волокнистого материала. Это обуславливает нестабильность значений коэффициентов отражения и передачи электромагнитного излучения поглотителей, изготовленных в соответствии с рассматриваемой методикой, ввиду перераспределения частиц углерода в объеме волокнистого материала.

В связи с этим была разработана методика закрепления инкорпорированных частиц аллотропных форм углерода в волокнистом материале. Отличительной особенностью данной методики является использование углеродосодержащего нанокомпозита на основе смеси порошка технического углерода и поливиниацетатного клея. В соответствии с разработанной

методикой изготовлены образцы композиционных поглотителей электромагнитного излучения. Исследованы частотные характеристики передачи и отражения электромагнитного излучения в СВЧ-диапазоне изготовленных образцов (далее по тексту – образцов группы 1). Выполнен сравнительный анализ указанных характеристик с аналогичными им, полученными для образцов композиционных поглотителей электромагнитного излучения, изготовленных в соответствии с методикой, представленной в работе [1] (далее по тексту – образцов группы 2). На основе результатов такого анализа установлено, что значения коэффициента передачи электромагнитного излучения образцов группы 1 ниже, чем значения аналогичного параметра, полученные для образцов группы 2 и изменяются в пределах от –10,1 до –16,1 дБ. Значения коэффициента отражения электромагнитного излучения образцов групп 1 и 2 являются практическими схожими.

Следует отметить, что такие характеристики передачи и отражения образцов группы 1 по сравнению с образцами группы 2 характеризуются более высокой стабильностью.

**Литература**

1. Белоусова Е.С., Аль-Махдави М.С.Х., Бойправ О.В. Экспериментальное обоснование способа получения гибких экранов электромагнитного излучения, основанного на инкорпорировании углерода аллотропных форм в волокнистые матрицы // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. Физика. – 2019. – № 12. – С. 15–20.

## СТРАХОВАНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.Н. Беляцкая, В.С. Князькова

По данным МВД РБ за 2018 г. количество выявленных преступлений в Беларуси против информационной безопасности увеличилось на 48 % (по сравнению с 2017 г.); в том числе количество преступлений, связанных с несанкционированным доступом к компьютерной информации, увеличилось на 97,4 %. Ущерб, понесенный в результате таких преступлений, может быть различным, от хищения денежных средств до имиджевых потерь. Частично компенсировать ущерб (главным образом юридическим лицам) призван инструмент страхования рисков информационной безопасности. На сегодняшний день мировой рынок т. н. киберстрахования оценивается в 3,5 млрд долларов США; к 2025 г. ожидается, что его объем достигнет 21,4 млрд. долларов США. В условиях развития информационного общества в Республике Беларусь, а также мерах, принятых правительством по развитию цифровой экономики (например, Декрет Президента Республики Беларусь № 8 «О развитии цифровой экономики», регулирующий, в частности, обращение цифровых знаков (токенов), позволяющий нашей стране стать крупным игроком на криптовалютных биржах), представляется важным формирование и развитие нормативно-правовой базы, регулирующей осуществление деятельности по страхованию рисков информационной безопасности. Страхование информационных рисков главным образом распространяется на следующие объекты: а) программное обеспечение; б) базы данных; в) финансовые активы в электронной форме. Данные объекты чаще всего страхуются от наступления следующих событий: 1) нарушение целостности, доступности и конфиденциальности данных; 2) нарушение работоспособности ЭВМ; 3) незаконное вмешательство в функционирование программно-технических комплексов. Полисы киберстрахования (cyber insurance policy, cyber risk insurance, cyber liability insurance coverage) позволяют организациям минимизировать затраты, возникшие в результате нарушения информационной безопасности. В Республике Беларусь на данный момент времени не существует нормативно-правовой базы в данной области. Тем не менее, ряд страховых организаций (например, РУСП «Белгосстрах») предлагают заключить договора добровольного страхования, которые (возможно, с определенной степенью условности) можно отнести к договорам страхования рисков ИБ. Так, «Белгосстрах» предлагает застраховать портативные устройства от хищения, пожара, взрыва, удара молнии и пр.; нарушение имущественных прав на объекты интеллектуальной собственности (которыми являются, например, базы данных), незаконного их использования третьими лицами. Разработка

комплекса нормативно-правовых актов, регулирующих данный вид деятельности, будет способствовать успешной цифровой трансформации белорусской экономики.

**Литература**

1. Статистика УРПСВТ за 2018 год [Электронный ресурс]. – Режим доступа: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt. – Дата доступа: 21.03.2020.

2. The cyber insurance market in 2019 [Electronic resource]. – Mode of access: https://www.atlas-mag.net/en/article/the-cyber-insurance-market-in-2019. – Date of access: 21.03.2020.

3. Global Cyber Insurance Market Report 2019-2025 [Electronic resource]. – Mode of access: https://www.businesswire.com/news/home/20191213005215/en/Global-Cyber-Insurance-Market- Report-2019-2025-Market. – Date of access: 21.03.2020.

4. Измалкова С.А., Тарасов А.В. Страхование информационных рисков как эффективный способ управления информационной безопасностью предприятий // Национальный интересы: приоритеты и безопасность. – 2006. – № 5. – С. 69–72.

5. Правила страхования / Белгосстрах [Электронный ресурс]. – Режим доступа: http://bgs.by/eventinsurance/12514/. – Дата доступа: 21.03.2020.

## РАДИОПОГЛОЩАЮЩИЕ КОМПОЗИЦИОННЫЕ СТРУКТУРЫ НА ОСНОВЕ ВЛАГОСОДЕРЖАЩИХ ПОРОШКООБРАЗНЫХ МАТЕРИАЛОВ

О.В. Бойправ, Н.В. Богуш

Радиопоглощающие материалы представляются перспективными для использования не только в целях скрытия объектов от обнаружения в радиолокационном диапазоне длин волн, но и в целях защиты информации от утечки по каналу побочного электромагнитного излучения и наводок, в связи с тем, что амплитуда электромагнитных волн, отражаемых такими материалами, характеризуется невысокими значениями и, как следствие, эти материалы не создают пассивные помехи, влияющие на процессы функционирования устройств обработки данных и другого радиоэлектронного оборудования. Для изготовления радиопоглощающих материалов весьма перспективным представляется использование воды и водных растворов, что экспериментально обосновано в работе [1]. В связи с вышеизложенным, авторами доклада были проведены исследования, направленные на разработку методики изготовления радиопоглощающих влагосодержащих композиционных структур, которые могут быть использованы в процессе строительства выделенных помещений.

Разработанная методика заключается в реализации следующих действий.

1. Подготовка водного раствора хлорида кальция.

2. Пропитывание до насыщения подготовленным раствором порошкообразных материалов, содержащих оксиды переходных металлов. Выбор указанных материалов обусловлен тем, что они характеризуются высокой пористостью, а также диэлектрическими или магнитными свойствами. Пропитывание этих материалов водным раствором хлорида кальция обуславливает возможность обеспечения как диэлектрических (магнитных) свойств для формируемых композиционных структур, так и свойств электропроводности.

3. Смешивание пропитанных раствором порошкообразных материалов, содержащих оксиды переходных металлов, с гипсовым связующим в объемном соотношении 1:1.

4. Помещение полученной смеси в пресс-формы.

5. Выдерживание в пресс-формах смеси при стандартных условиях до момента ее перехода их жидкой фазы в твердую.

6. Извлечение смеси из пресс-форм.

Получаемые в соответствии с предложенной методикой радиопоглощающие композиционные структуры характеризуются следующими преимуществами:

– стабильное влагосодержание и, как следствие, стабильные значения коэффициентов отражения и передачи электромагнитного излучения;

– прочность.

Указанные преимущества рассматриваемых структур обусловлены тем, что водный раствор хлорида кальция содержится не в объеме их связующего вещества, а в порах их порошкообразного наполнителя, и по сути, связующее вещество «герметизирует» этот раствор в порах порошкообразного наполнителя.

Установлено, что радиопоглощающие композиционные структуры, изготовленные в соответствии с разработанной методикой, характеризуются значениями ослабления электромагнитного излучения в диапазоне частот 0,7…150,0 ГГц не менее 20 дБ.

**Литература**

1. Водосодержащие капиллярно-пористые экраны электромагнитного излучения. Теория и практика / Н.Н. Гринчик [и др.] – Мн.: Бестпринт, 2016. – 238 с.

## ВЛИЯНИЕ РАЗМЕРА ПОР ВЛАГОСОДЕРЖАЩЕЙ МАТРИЦЫ НА ЗНАЧЕНИЯ КОЭФФИЦИЕНТА ОТРАЖЕНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Т.В. Борботько, С.Э. Саванович

Один из эффективных методов, обеспечивающий исключение неконтролируемого распространения информации о наземных подвижных объектах (военной технике) в диапазоне частот 2–12 ГГц [1], заключается в снижении их отражающих свойств и реализован в экранах ЭМИ, выполняемых на основе влагосодержащих материалов. Известно [2], что значения коэффициента отражения таких экранов в пределах их рабочего диапазона частот определяется значениями действительной $\varepsilon'$ и мнимой $\varepsilon''$ составляющих диэлектрической проницаемости растворов, вводимых в поры матрицы, и ее влагосодержанием. Можно предположить, что значения коэффициента отражения экранов ЭМИ в рассматриваемом диапазоне частот также определяются размерами пор матрицы и их распределением в ее структуре.

В результате обзора экранирующих свойств экранов ЭМИ, выполненных на основе влагосодержащих материалов, установлено, что для разработки экранов, обеспечивающих противодействие перехвату информации по электромагнитному каналу (ЭМК), предпочтительно использование матриц, характеризующихся порами, размеры которых изменяются от $5\cdot10^{-6}$…1 мм, например, керамзита. Размеры пор керамзита варьируются в пределах $4\cdot10^{-6}$…2,2 мм, значения коэффициентов отражения экранов ЭМИ, выполненных на его основе, составляют от –1,6 до –19,5 дБ в диапазоне частот 2–12 ГГц, что показывает перспективность его использования для разработки конструкций экранов ЭМИ, обеспечивающих блокирование информации от утечки по ЭМК.

**Литература**

1. Перунов Ю.М., Фомичев К.М., Юдин Л.М. Радиоэлектронное подавление информационных каналов систем управления оружием. – М. :«Радиотехника», 2003. – 416 с.

2. Электромагнитные излучения. Методы и средства защиты / В. А. Богуш [и др.] ; под ред. Л.М. Лынькова. – Мн.: Бестпринт, 2003. – 406 с.

## НАПРАВЛЕНИЯ РАЗВИТИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В 2020 ГОДУ

А.А. Виноградов

Какие основные направления развития кибербезопасности следует знать в 2020 году?

TÜV Rheinland выпустил свой седьмой ежегодный отчет о тенденциях кибербезопасности на 2020 год [1]. В этом отчете представлены мнения многих экспертов в области компьютерной безопасности по всему миру. Анализируя публикацию, можно выделить основные негативные тенденции в защите информации.

1. Огромные темпы увеличения количества и производительности «умных» устройств в повседневной жизни человека являются угрозой персональной информационной безопасности.

2. Угрозы морским перевозкам и другим типам перевозок давно перестали быть теоретической угрозой и вошли в стадию реальной.

3. Транспортная инфраструктура становится все более связана программным обеспечением, что открывает широкое поле для кибератак.

4. В операционных системах реального времени (таких, как VxWorks) открывается все больше уязвимостей. Такие уязвимости могут подвергать ОС риску атак удаленного выполнения кода (RCE).

Так, развитие кибербезопасности в ближайшем будущем будет направлено именно на смягчение вышеописанных тенденций.

**Литература**

1. Cybersecurity Trends 2020 [Electronic resource]. – Mode of access: https://www.tuv.com/landingpage/en/cybersecurity-trends/. – Date of access: 10.05.2020.

## АСПЕКТЫ ИЗУЧЕНИЯ ПРОЦЕССНОЙ МОДЕЛИ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г.А. Власова

К базовым компетенциям при подготовке специалистов по информационной безопасности относится умение управлять информационными рисками, что подразумевает владение практическими навыками применения современных методов управления. В основе международных управленческих стандартов лежит модель Деминга-Шухарта. Преимуществом данной модели является ее универсальность: модель применима и к высокоуровневым стратегическим процессам, и к операционным действиям, то есть, применима для различных областей деятельности и различных организаций. Помимо этого модель характеризуется наглядностью и системностью.

Модель определяет 4 группы процессов: Планирование – Реализация – Проверка – Действие (ПРПД, PDCA, PDSA). Непрерывная деятельность по управлению рисками, согласно Демингу, должна осуществляться на основании следующих аксиом: любая деятельность может рассматриваться как технологический процесс и, следовательно, может быть улучшена; результат решения конкретных проблем определяется состоянием системы; высшее руководство предприятия должно во всех случаях принимать на себя ответственность за деятельность предприятия.

Важно на практических примерах показать учащимся преимущества, которыми обладают организации, в которых существует система управления информационными рисками. К ним относятся: стабильные и высокие (выше среднестатистических показателей) результаты деятельности на протяжении многих лет; максимизация возврата инвестиций в информационную безопасность; способность к самовосстановлению и самосовершенствованию, что особенно значимо в переходные периоды. Практикоориентированный подход вызывает интерес у учащихся, формирует понимание значимости изучаемой дисциплины для их дальнейшей профессиональной деятельности.

**Литература**

1. СТБ ISO/IEC 27005-2012 Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности.

2. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management.

## МЕРОПРИЯТИЯ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАК В БАНКОВСКОЙ СФЕРЕ

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

Возможность баснословных прибылей и невысокий уровень риска обнаружения благоприятствуют росту кибератак на финансовые организации. Банковская система Республики Беларусь по-прежнему остается в поле зрения злоумышленников и международных преступных группировок. Последние, как хамелеоны, приспосабливаются к изменениям обстановки в сфере информационной безопасности, тщательно отслеживают появление новых уязвимостей в программном обеспечении и появление брешей в информационных системах банков и финансовых организаций.

Для успешного предотвращения кибератак необходимо выполнение банками следующих мероприятий:

– использование современных аппаратных, программных и программно-аппаратных комплексов средств защиты информации;

– постоянное повышение квалификации работников, отвечающих за информационную безопасность в банке;

– обучение работников банков основам информационной безопасности;

– поддержание здорового климата в коллективе;

– информирование и обучение клиентов банков финансовой и цифровой грамотности;

– разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке;

– блокирование подключения к беспроводным сетям на территории банка;

– создание команды по расследованию инцидентов информационной безопасности в банке из числа наиболее подготовленных работников;

– скрупулезный подбор персонала в банковские учреждения с учетом их профессиональных, нравственных и моральных качеств;

– взаимодействие и обмен информацией о кибератаках между банками и правоохранительными органами.

## ОПРЕДЕЛЕНИЕ ПОЖАРНОЙ ОПАСНОСТИ ПО ДИНАМИКЕ ПРОПУСКАЮЩЕЙ СПОСОБНОСТИ СРЕДЫ

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

В основе работы дымовых пожарных извещателей (ДПИ) систем пожарной безопасности лежит измерение величины оптической плотности газодымовой среды. Для повышения информативности, формируемых ДПИ сигналов, предлагается переход от статических измерений оптической плотности к динамическим измерениям в пространстве задымления.

В работе исследовалась динамика пропускающей способности среды в помещении при тлении разного количества хлопчатобумажной ткани.

Из экспериментальных данных с применением методов наименьших квадратов и Евклидова расстояния получены характеристические кривые потоков прошедшего сквозь задымленную среду оптического излучения. Различия между кривыми проявляются в положении максимумов и интервале изменения Евклидового расстояния. При этом с увеличением количества топлива наблюдается тенденция снижения абсолютных значений максимумов и расширения интервала изменения Евклидового расстояния кривых.

Результаты исследования свидетельствуют о возможности соотношения формы и положения характеристических кривых с количеством тлеющего материала. Такой подход может быть использован для определения опасности пожара относительно количества горящего топлива.

## СИСТЕМА ЛОКАЛИЗАЦИИ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

В.Е. Галузо, А.В. Коваль, В.В. Мельничук

При проектировании автономных транспортных средств (АТС) и систем ассистирования вождению важнейшее место отводится системе автоматической локализации.

Среди подходов, применяемых для решения задач разработки систем локализации, принятия решений, а также системы управления и контроля все большее место занимают методы и алгоритмы, основанные на технологиях искусственного интеллекта и машинного обучения. При решении задачи локализации АТС необходимо определить его положение относительно дорожной разметки, других транспортных средств, пешеходов и окружающей среды, а также распознать дорожные знаки.

Сигналы от системы локализации принимаются и обрабатываются системой принятия решений, и передаются в систему управления и контроля. В качестве приемных устройств в системах локализации используются различные датчики и устройства типа LIDAR, однако центральное место отводится видеокамерам. Использование видеокамер обусловлено рядом преимуществ, среди которых низкая стоимость технологии, разнообразие доступных техник по обработке изображений, а также простота эксплуатации оборудования. В то же время, использование видеоданных имеет и свои недостатки, в частности, видеокамеры имеют разное качество выходного изображения, а также искажения, обусловленные кривизной линз и точностью их установки.

При моделировании системы локализации АТС необходимо с высокой степенью точности определить границы текущей полосы движения, что в свою очередь подразумевает, что система должна уметь распознавать линии дорожной разметки. Одним из подходов к распознаванию линий дорожной разметки может быть метод кусочной сегментации, позволяющий определять не только границы разметки, но и на основании данных о смещениях единичных сегментов вычислять кривизну полосы движения на участке пути. Используя данные о границах полосы движения, габаритах АТС и точки расположения видеорегистратора, можно определить горизонтальное смещение АТС относительно полосы движения. В то же время, на основании данных о смещении единичных сегментов элементов дорожной разметки на изображении можно рассчитать кривизну полосы движения на участке пути. Получив требуемые данные, при помощи средств обработки видеоряда можно аннотировать исходные обрабатываемые изображения или видеоряд целиком.

Таким образом, используя вышеупомянутые техники и инструменты, возможно получить относительно полную информацию о локализации АТС относительно полосы движения, что является весьма критичной частью решения задачи о локализации АТС в целом.

## ПОСТРОЕНИЕ СПАМ-ФИЛЬТРА НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

А.А. Григорьев, А.В. Галковский, Д.С. Совпель, Д.А. Клебанов

Безопасность и качество информации, поступающей из интернета один из ключевых вопросов его развития. Количество информации экспоненциально увеличивается каждый день и вопрос в том, как ее обрабатывать становится достаточно острым. Одним из подходов для анализа больших данных является алгоритмы машинного обучения. Машинное обучения применяется в том числе для фильтрации данных и защиты пользователя от нежелательного контента.

Существует множество подходов к построению алгоритмов для фильтрации спама:

– фильтры содержимого: анализ содержимого сообщений, поиск по словам, которые обычно используются в спам-письмах;

– фильтры черного списка: игнорирование электронных писем, приходящих с IP-адресов и e-mail адресов, находящихся в черных списках (некоторые фильтры также могут проверять IP-репутацию IP-адреса);

– фильтры на основе правил: применяют настраиваемые правила, разработанные организацией, чтобы исключить электронные письма от определенных отправителей или электронные письма, содержащие определенные слова в строке или тексте темы.

Наиболее эффективным является подход комбинированных систем, основным компонентом которого является фильтр содержимого, основанный на алгоритмах машинного обучения. Широко применяемым алгоритмом фильтрации спама является алгоритм наивного Байеса. Он возвращает вероятность того, что сообщение является спамом или не спамом при условии исходных данных. Расчет вероятности производится при помощи формулы Байеса [1]:

Таким образом при помощи этого алгоритма и набора исходных данных, представляющих размеченные на спам и не спам письма, можно построить систему спам фильтрации и использовать ее в системе почтовых клиентов.

**Литература**

1. Bishop C. Pattern Recognition and Machine Learning. – Springer: 2006. – 48 p.

## ПРИМЕНЕНИЕ СИСТЕМЫ T-POT ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

В.И. Грицкевич

Система T-Pot – это коллекция различных ханипотов, собранных компанией T-Mobile. Он представляет реализацию стека ELK (Elastic Search, Logstash, Kibana) для визуализации всех событий, захваченных различными ханипотами и некоторыми другими инструментами. Все ханипоты в T-Pot работают, используя docker (виртуальный контейнер), что значительно упрощает управление всеми настройками. Сам по себе ханипот не является средством обеспечения информационной безопасности. Это лишь приманка, ловушка для злоумышленника, целью которой является заставить его поверить в легитимность сервисов, которые имитирует ханипот. Однако такие приманки позволяют получить и проанализировать огромное количество информации, которая может оказаться полезной при планировании мероприятий повышения уровня информационной безопасности организаций. В частности, данная система содержит SSH и Telnet ханипоты, веб-ханипоты (эмулируют такие сервисы, как Redmine, Tomcat, Gitlab), ханипот, эмулирующий промышленный комплекс, SMTP-ханипот и многие другие. Система собирает информацию о методах, применяемых злоумышленниками, для проведения атак, что позволяет предотвратить атаку еще до попытки ее реализации. Помимо этого, появляется возможность оценить с каких территорий производятся атаки. Таким образом, система ханипотов T-Pot предоставляет информацию, с помощью которой можно значительно повысить уровень защищенности информационных систем.

**Литература**

1. Introduction to T-Pot - The all in one honeypot [Электронный ресурс]. – Режим доступа: https://northsec.tech/introduction-to-t-pot-the-all-in-one-honeypot/. – Дата доступа: 10.05.2020.

## О ПРАВОВОМ РЕГУЛИРОВАНИИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В ФОРМЕ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА

М.В. Губич

Тенденцию к увеличению внимания к государственно-частному партнерству (далее – ГЧП) при построении государственной политики в сфере безопасности можно проследить на примере анализа содержания Концепции национальной безопасности Республики Беларусь, принятой в 2010 году [1] и Концепции информационной безопасности Республики Беларусь, принятой в 2019 году [2]. Так, если в первом документе ГЧП рассматривается в качестве инструмента, обеспечивающего конструктивную направленность деятельности общественных объединений, повышение созидательной активности населения и основы формирования и развития белорусского гражданского общества [1, п. 49], то в Концепции информационной безопасности ГЧП в сфере

обеспечения информационной безопасности (далее – ИБ) посвящена целая глава [2, гл. 26].

В настоящее время рассматриваемый правовой институт регламентирован 201 нормативным правовым актом, в том числе Законом Республики Беларусь «О государственно-частном партнерстве» [3], постановлениями Совета Министров Республики Беларусь [5] и Министерства экономики Республики Беларусь [4], направленными на реализацию указанного закона. Проанализировав содержание данных и иных нормативных правовых актов можно выделить следующие положения законодательства, направленные на развитие ГЧП в сфере противодействия киберпреступности: создание условий для обеспечения национальной безопасности Республики Беларусь, а также совершенствование средств и систем защиты и охраны, используемых для противодействия противоправной деятельности отнесено к основным задачам ГЧП; ГЧП признано наиболее эффективной моделью обеспечения ИБ, что в полной мере относится и к области противодействия киберпреступности; основными целями рассматриваемой формы взаимодействия являются привлечение квалифицированных кадров, технологий, капитала частных предприятий, а также повышение эффективности использования бюджетных средств; ГЧП в рассматриваемой области обеспечения ИБ основывается на объединении ресурсов и распределении рисков между правоохранительными органами и субъектами хозяйственной деятельности; государство заинтересовано в обновлении и развитии механизмов противодействия киберпреступлениям, в том числе посредством проведения IT-аудита, мониторинга киберрисков, поиска уязвимостей и актуальных средств защиты.

**Литература**

1. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 нояб.2010 г. № 575 : в ред. Указ Президента Респ. Беларусь от 24.01.2014 Лукашенко // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета Безопасности Республики Беларусь, 18 марта 2019 № 1 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

3. О государственно-частном партнерстве [Электронный ресурс]: Закон Респ. Беларусь, 30 дек. 2015 г. № 345-З: в ред. от 17 июля 2018 г. № 134-З) // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

4. О мерах по реализации Закона Республики Беларусь от 30 декабря 2015 г. № 345-З «О государственно-частном партнерстве» [Электронный ресурс]: постановление Совета Министров Респ. Беларусь, 6 июля 2016 г., № 532: в ред. от 26.03.2019 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

5. О проектах государственно-частного партнерства [Электронный ресурс]: постановление Министерства экономики Респ. Беларусь, 27 июля 2016, № 49: в ред. от 28.03.2019 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

## АНАЛИЗ ЗАЩИЩЕННОСТИ ВЕБ-РЕСУРСОВ НА ОСНОВЕ МЕТРИКИ CVSS

Ш.Р. Давлатов

С развитием веб-технологий растет и число потенциальных уязвимостей в онлайн-ресурсах. Широкое использование инструментов для реализации угроз информационной безопасности в Интернете определяет актуальность использования систем для анализа безопасности веб-ресурсов. Специалисты по защите информации часто используют объективные количественные показатели защищенности, которые вычисляются на основе метрик открытой системы оценки CVSS (Common Vulnerability Scoring System). Метрика CVSS предлагает простой инструментарий для расчета числового показателя уязвимости по десятибалльной шкале. Чем выше значение метрики, тем более оперативная реакция требуется для исправления проблемы безопасности системы.

В рамках данной работы была разработана система для автоматического сбора информации о веб-ресурсах из открытых источников shodan.io и censys.io. В результате процесса сканирования удалось собрать данные более 19 тысяч наиболее популярных веб-ресурсов Беларуси. Для каждого отдельного домена была получена техническая информация в формате: IP-адреса, открытые порты, географическое расположение веб-серверов и заголовки ответов HTTP. В работе также представлена новая методика оценки безопасности веб-ресурсов на базе метрики CVSS. Установлено, что порядка 10% веб-ресурсов Беларуси из исходной генеральной выборки, в размере 19 тысяч доменов, имеют критическую усредненную оценку уязвимости. На основе данных об уязвимостях построено эмпирическое распределение оценки CVSS. С помощью критерия хи-квадрат проверена гипотеза о том, что данное распределение подчиняется закону Пуассона. В рамках данного исследования были также разработаны RegExp выражения на языке JavaScript для точного определения версий технологий, которые были использованы для создания веб-сайтов. Установлены процентные соотношения используемых технологий, доменов верхнего уровня и географическое расположение серверов, которые обслуживают данные веб-ресурсы.

## ОСОБЕННОСТИ ГЕНЕРАЦИИ И ПРИЕМА АКУСТИЧЕСКИХ СИГНАЛОВ С ЦИФРОВОЙ МЕТКОЙ ДЛЯ ИЗМЕРЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЙ

Г.В. Давыдов, А.И. Кухаренко

При измерениях уровня защищенности помещения от утечек информации по звуковому каналу часто требуется повышение отношения сигнал/шум принятого акустического сигнала после прохождения его через поглощающие среды. Поставленную задачу предлагается достичь путем метода встраивания цифровой метки особой формы, основанной на коде Баркера в звуковой сигнал.

Для исследований поведения такого сигнала с кодом Баркера в реальном окружении были проведены измерения. Сигнал создавался на персональном компьютере с помощью разработанной специальной программы, предназначенной для генерирования в реальном времени звуковых сигналов со встроенными метками в диапазоне частот от 100 до 8000 Гц. Для этого тестовый сигнал, сгенерированный в акустическом виде с амплитудно-импульсной модуляцией, был подан на цифровой осциллограф RIGOL DS1102D. При использовании ждущего режима триггера и запоминающей функции осциллографа, удалось в сигнале зафиксировать код Баркера. Определено, что из-за особенностей операционной системы и накладываемых из-за системных прерываний ограничений на генерацию акустических сигналов, стабильность обнаружения метки на высоких частотах может снижаться. Для повышения стабильности необходимо либо понижать частоту несущего сигнала, либо увеличивать число периодов сигнала, приходящихся на один элемент кода Баркера. Однако слишком сильное понижение несущей частоты может отрицательным образом сказаться на измерениях в реальных помещениях, так как на низких частотах начинают вносить существенные искажения акустические резонансы помещения, а также падает эффективность излучателей.

Таким образом, для дальнейшего приема и фильтрации слабого сигнала, прошедшего через поглощающие среды, целесообразно повышать количество периодов несущего сигнала на один кодирующий элемент, при этом спектральная полоса метки в сигнале (без учета высших гармоник) должна отстоять от полосы несущего сигнала по меньшей мере на 4 октавы, это необходимо для уверенного выделения меток из звуковых сигналах с применением фильтров нижних частот. Проводимые по теме работы и исследования осуществляются при поддержке программы ГПНИ «Информатика, космос и безопасность».

## МОДЕЛИ ЗВУКОВЫХ СИГНАЛОВ СО ВСТРОЕННЫМИ МЕТКАМИ ДЛЯ ОЦЕНКИ ЗВУКОИЗОЛЯЦИИ ПОМЕЩЕНИЙ

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

Разработана программа генерирования звуковых сигналов со встроенными метками в диапазоне частот от 100 до 8000 Гц. Метки встраивались в начале звукового сигнала и повторялись через каждые 10 секунд. Встраивание меток в звуковые сигналы осуществлялось путем скачкообразного изменения амплитуды несущего колебания в соответствии с кодом Баркера.

Моделирование заключалось в формировании гармонического сигнала, модулированного импульсными сигналами в соответствии с кодами Баркера и наложение на них шумового сигнала с уровнями в октавных полосах, соответствующих речевому сигналу. Таким образом, было выполнено моделирование работы диктора при оценке степени защищенности речевой информации.

Моделирование канала передачи акустического речевого сигнала заключалось в наложении на раннее сформированный сигнал, имитирующий работу диктора, шумового сигнала, характерного для акустических производственных шумов в ограждающих конструкциях защищаемого помещения. Кроме того, было введено и ослабление сигнала, что моделировало затухание акустического сигнала при распространении его за ограждающие конструкции помещения.

Результаты моделирования показывают, что с точки зрения помехоустойчивости, наиболее подходящим методом тестирования зондирующего сигнала является метод амплитудной манипуляции.

Определено число элементов кода Баркера и длины элемента при акустическом зондировании ограждающих элементов конструкций помещений с учетом явлений их механического резонанса в исследуемом диапазоне частот.

## ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ПО ПОКАЗАТЕЛЯМ РАЗБОРЧИВОСТИ РЕЧИ

Г.В. Давыдов, В.А. Попов, А.В. Потапович, Е.Н. Сейткулов

В данной работе представлены результаты экспериментальных исследований, направленные на оценку разборчивости речи при ее защите от утечки по акустическим каналам путем маскирования комбинированными акустическими сигналами, включающими «белый» шум и речеподобные сигналы. Рассмотрены особенности и факторы, влияющие на оценку защищенности речевой информации, и представлен программный продукт, позволяющий автоматизировать процесс оценки защищенности.

Оценка защищенности речевой информации тесно связана с условиями окружающей среды, как правило, наиболее часто встречающийся вариант – это определенное помещение с различными звукоизолирующими свойствами ограждающих элементов конструкций. Учесть влияние звукоизолирующих свойств ограждающих конструкций можно только на основании экспериментальных измерений передаточной характеристики речевых сигналов за пределы помещений и дополнительного пространства защиты. При этом следует иметь в виду, что и от методики проведения экспериментальных исследований в сильной степени зависят результаты оценки защищенности речевой информации. Важным явлением при проведении экспериментальных исследованиях является резонанс изгибных колебаний ограждающих элементов конструкций помещений.

Сложности в оценке защищенности речевой информации обусловлены неопределенностями, связанными с трудностями математической формулировкой задачи защиты с одной стороны и большим количеством факторов, влияющих на показатели защищенности речевой информации, с другой стороны. В данной работе оценку защищенности речевой информации предлагается определять по показателям разборчивости речи по предельным состояниям. Для правильной оценки защищенности речевой информации

по показателям ее разборчивости было принято ряд допущений и ограничений, которые основаны на опыте практической реализации и экспериментальных исследованиях по защите речевой информации.

## КРИТЕРИИ КЛАССИФИКАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК

А.Г. Давыдовский

Цель исследования – анализ критериев классификации социоинженерных атак на информационные социотехнические системы (ИСТС) и их пользователей.

В 2011 г. K. Ivaturi и L. Janczewski впервые предложили классификацию различных социоинженерных атак (СИА). В 2013 г. Algarni A., Xu Y., Chan T., Tian Y.-C. предложили подразделять все социоинженерные атаки на одно- и многоступенчатые. Krombholz K., Hobel H., Huber M., Weippl E. (2013, 2015) предложили классификация СИА на основе трех критериев: канала, оператора и типа. Причем каналы могут быть как техническим, так и нетехническими (психофизиологическими), операторы представлены людьми или программным обеспечением, а типы зависят от физических, технических, социальных и социотехнических способов и средств атаки. При этом могут быть использованы такие методы социальной инженерии, как «погружение в мусорные контейнеры», «спасательные работы», фишинг (вишинг), договоренности quid pro quo, «дорожное яблоко», претекстинг, «слежка». В зависимости от эксплуатируемых эмоций жертв все СИА можно классифицировать на негативно ориентированные (используют вину, сочувствие, невежество, двусмысленность и аффилированность) и позитивно ориентированные (используют дружелюбие, олицетворение, соответствие, предлога, диффузии ответственности и приманки). Для классификации СИА необходимо учитывать модели поведения социальных инженеров и их жертв, включая человеческие ошибки, особенности восприятия информации онлайн, способы восприятия и оценки низко- или высококонтекстуальных медиасообщений [1].

Критерии классификации СИА могут быть основаны на использовании технологических платформ (аппаратное и программное обеспечение, сетевая инфраструктура), атаки на мобильные устройства и их приложения, атаки рабочих столов, атаки физических инфраструктур [2]. Широко распространены методы атак, использующие мобильные телефоны, IP-технологии голосового обмена сообщениями, методы фишинга (вишинга). Отдельно можно выделить видео-СИА, а также СИА на основе использования ботнетов, руткитов (Gregio A.R.A., et al., 2015).

Учитывая вышеизложенное, впервые разработана многокритериальная классификация СИА, характеризующая динамику атаки как вектор в N-мерном гиперпространстве критериев, включающем причины и мотивацию, модели поведения социальных инженеров и их жертв, посредников, технологические платформы, информационные, социотехнические среды реализации атаки, время эффекта (быстрый, с отсрочкой, поздний), тип эффекта и его последствий. Для классификации атакующих воздействий предложен ряд базовых моделей: «человек (сообщество)→человек (сообщество)» и опосредованные «человек (сообщество)→медиасреда→человек (сообщество)», «человек (сообщество)→ИСТС→человек (сообщество)», «человек (сообщество)→ИСТС→медиасреда→ИСТС →человек (сообщество)».

**Литература**

1. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice/ K. Chen, [et al.] // J. of Hardware and Systems Security. – 2018. – Vol. 2, № 2. – P. 97–110.

2. Aldawood H.A., Skinner G. Taxonomy for Social Engineering Attacks via Personal Devices // Intern. J. of Comp. Appl. – 2019. – Vol. 178, N50. – P. 19–26.

## ФОРМИРОВАНИЕ ШАГОВОЙ ТРАЕКТОРИИ С ИСПОЛЬЗОВАНИЕМ ЭКСТРАПОЛИРОВАННЫХ ЗНАЧЕНИЙ ОЦЕНОЧНОЙ ФУНКЦИИ

И.В. Дайняк

Для расчета промежуточных участков траекторий в устройствах управления применяется аппаратный либо программный блок – интерполятор, выходные сигналы которого представляют собой распределенные во времени импульсы, поступающие на управляющие входы исполнительного устройства. Алгоритмы работы таких интерполяторов, как правило, строятся на основе анализа знака оценочной функции, однако непосредственная реализация такого алгоритма не обеспечивает максимальной точности приближения расчетной траектории к теоретической кривой.

Основное требование, предъявляемое к управлению движением объекта, состоит в том, что управляемый объект должен двигаться с минимально возможным отклонением от желаемой траектории. Координаты являются дискретными, а направление элементарного шага приращения выбирается в зависимости от знаков оценочной функции в узловых точках. Для повышения точности формирования плоской траектории в докладе предлагается применить алгоритм на основе использования экстраполированного значения оценочной функции. Суть алгоритма состоит в том, что направление элементарных шагов выбирается в зависимости от знака оценочной функции, вычисленной с экстраполяцией на половину шага сетки вперед по обеим координатам. Таким образом как бы предугадывается поведение линии $F(x,y) = 0$ в области каждого пересекаемого этой линией элементарного квадрата с учетом того, что выбор направления шага осуществляется из узловой точки. В докладе проанализированы различные возможные варианты пересечения линией $F(x, y) = 0$ элементарных квадратов и указаны направления элементарных шагов к узловым точкам, наиболее близко расположенным к этой линии. В результате была сформирована методика преобразования требуемой траектории в сеточную функцию, обеспечивающую процесс построения шаговой траектории и ориентированную на программно-аппаратную реализацию в контроллере шагового привода. Это позволяет повысить точность перемещений исполнительного элемента привода при малых затратах на выполнение вычислительных операций.

## КОМБИНИРОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ АТАК

В.А. Дмитриев, Е.П. Максимович

К характерным недостаткам разных отдельных методов обнаружения атак относятся: недопустимо высокий уровень ложных срабатываний и пропусков атак; слабые возможности по обнаружению новых атак; частая невозможность определения атаки на начальных этапах; трудность определения атакующего, цели атаки; отсутствие оценок точности и адекватности результатов работы; невозможность определения «старых» атак, использующих новые стратегии; слабые возможности по автоматическому обнаружению сложных координированных атак. В виду этого актуальным подходом к повышению эффективности систем обнаружения атак является использование комбинации нескольких методов обнаружения атак, нивелирующих недостатки друг друга.

В настоящее время подавляющее большинство реальных систем обнаружения атак делятся по способам выявления атак на системы обнаружения аномалий и системы обнаружения злоупотреблений. Обнаружение злоупотреблений позволяет идентифицировать несанкционированные действия, если имеется их точное представление в виде характерных идентифицирующих свойств) атак (сигнатур, экспертных правил). Данные методы являются точным и обоснованным средством выявления известных типов атак, но не пригодны для идентификации новых атак либо модификаций известных атак. Обнаружение аномалий на основе методов интеллектуального анализа данных (нейронные сети, деревья решений, индуктивные выводы, методы рассуждения по аналогии, нечеткие логические выводы, генетические алгоритмы, методы искусственных иммунных систем) – важное средство

обнаружения незнакомых атак, но принимаемые ими решения базируются не использовании эвристичных процедур, что не гарантирует их точности и однозначности.

Перспективным направлением при проектировании систем обнаружения атак представляется в настоящее время реализация подходов, совмещающих в себе преимущества сигнатурных и эвристических методов. Кроме того, анализируется целесообразность использования сигнатур, основанных не только на конкретном эксплоите (программном коде, автоматизирующем проведение атаки), но и на уязвимости сетевых протоколов и атакуемых систем.

Возможность эффективной практической реализации подходов, основанных на использовании комбинации нескольких алгоритмов обнаружения атак, обусловлена достигнутым в настоящее время уровнем развития компьютерной техники, телекоммуникационных средств, информационно-коммуникационных технологий.

## ВЕБ-СЕРВИС ДЛЯ ЗАДАЧИ КЛАССИФИКАЦИИ СТЕПЕНИ КРИТИЧНОСТИ УЯЗВИМОСТИ ПО ЕЕ ТЕКСТОВОМУ ОПИСАНИЮ

А.К. Доронин

Процесс определения характеристик CVE-уязвимостей сопряжен с ручной экспертной оценкой, что может приводить к неточным или неполным данным [1], и, следовательно, к непредсказуемым последствиям. На момент появления уязвимости имеется лишь ее текстовое описание, из которого можно получить всю релевантную информацию о ее характеристиках [2]. Поэтому актуальной является разработка системы автоматического определения степени критичности уязвимости по ее текстовому описанию. В качестве ядра, производящего автоматическую оценку критичности уязвимости, предлагается использовать построенную нами модель машинного обучения с точностью предсказания 85,52 % [3]. Однако процесс практической реализации данной модели сопряжен с рядом трудностей. В частности, необходимо разработать: архитектуру системы; процесс загрузки всех необходимых для работы модели машинного обучения компонентов; процесс работы функции предсказания степени критичности по входному текстовому описанию, а также необходимо обеспечить отказоустойчивость и масштабируемость решения. В данной работе предлагается реализация такой системы в виде веб-сервиса. Разработан проект архитектуры для обращения к веб-серверу, алгоритм функции вычисления вероятностных значений модели, процесс загрузки начальных компонентов. Веб-сервис в соответствии со спроектированной архитектурой реализован на языке программирования Python 3 с использованием фреймворков Keras, Tensorflow и Flask. Проведено нагрузочное тестирование веб-сервиса на одной машине, на основе которого сделан вывод о наличии ограничения эффективной максимальной пропускной способности в 130 запросов/секунду в идеальных условиях. Веб-сервис упакован в Docker-контейнер. Среди преимуществ реализованной системы являются: масштабируемость, отказоустойчивость, легкость развертывания и взаимодействия с другими системами. Исходный код выложен в открытый доступ и доступен для дальнейших экспериментов по ссылке: https://www.github.com/teacherlex/cve_vulns_classifier/tree/master/api.

**Литература**

1. Massacci F., Nguyen V. H. Which is the right source for vulnerability studies? An empirical analysis on Mozilla Firefox // Proceedings of the 6th International Workshop on Security Measurements and Metrics,MetriSec’10. – 2010; 1: 4:1 – 4:8.

2. Gonzalez D., Hastings H., Mirakhorli M. Automated Characterization of Software Vulnerabilities // 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME). – 2019. – P. 135–139. – DOI:10.1109/ICSME.2019.00023.

3. Доронин А.К., Липницкий В.А. Построение модели машинного обучения для задачи классификации степени критичности CVE-уязвимостей // Вестник МГУ им. А. А. Кулешова. – 2020. – № 1 (55). – С. 51–63.

## ОСНОВНЫЕ ПРИНЦИПЫ БЕЗОПАСНОСТИ В ПРОЕКТЕ АСУ ТП БЕЛОРУССКОЙ АЭС

С.В. Дробот

Учебный план подготовки специалистов в области систем контроля и управления для Белорусской АЭС включает дисциплину «Автоматизированные системы управления технологическими проектами атомных электростанций» (АСУ ТП АЭС) в рамках которой, в том числе, изучаются основные принципы и критерии безопасности, лежащие в основе проектирования этих систем АЭС.

Проектирование АСУ ТП ведется в соответствии с определенными в техническом задании на АСУ ТП нормативными документами. Подсистемы и элементы АСУ ТП АЭС, как и все другие системы и элементы АЭС, классифицируются по назначению и по влиянию на безопасность. По влиянию систем и элементов АЭС на безопасность установлены четыре класса безопасности. Причем четвертый класс безопасности является самым низким, к нему относятся системы и элементы, не влияющие на безопасность. Требования к качеству систем и элементов АСУ ТП АЭС, отнесенных к классам безопасности 1, 2, 3 и его обеспечению устанавливаются в нормативных правовых актах, определяющих требования к их устройству и эксплуатации. При этом более высокому классу безопасности соответствуют более высокие требования к качеству и его обеспечению.

Принципы безопасности при проектировании АСУ ТП Белорусской АЭС приняты в соответствии с требованиями нормативных правовых актов Российской Федерации, Республики Беларусь и учетом рекомендаций Международного агентства по атомной энергии (МАГАТЭ). К основным принципам относятся следующие: единичного отказа, отказа по общей причине, разнообразия, независимости, резервирования, отключения оборудования и др.

В докладе рассмотрена классификация подсистем и элементов АСУ ТП АЭС по назначению и представлены системы и элементы, относящиеся к важным для безопасности, а также перечень принципов безопасности с использованием которых осуществлено проектирование указанных систем. Рассмотрены нормативные правовые акты в области использования атомной энергии Республики Беларусь, Российской Федерации, а также документы МАГАТЭ, которые содержат требования и рекомендации к системам и элементам АСУ ТП АЭС.

## ТРЕБОВАНИЯ К ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА УПРАВЛЯЮЩИХ СИСТЕМ АЭС

С.В. Дробот

Важнейшим свойством АЭС является ее безопасность, т. е. свойство ограничивать радиационное воздействие на персонал, население и окружающую среду установленными пределами при нормальной эксплуатации, нарушении условий нормальной эксплуатации и в условиях аварий. Безопасность в условиях нормальной эксплуатации достигается решением задачи минимизации радиоактивных выбросов за счет обеспечения правильного функционирования систем и оборудования и предупреждения их отказов и инцидентов. При возникновении отказов безопасность обеспечивается предотвращением их перерастания в проектные аварии. В случае возникновения проектной аварии безопасность обеспечивается путем правильного функционирования систем безопасности.

Важную роль в обеспечении безопасности АЭС играют управляющие системы, осуществляющие управление технологическим оборудованием по заданным целям, критериям и ограничениям в различных условиях эксплуатации. Поскольку современные управляющие системы реализуются на основе программно-технических средств, использующих цифровые технологии и микропроцессорную технику, то несанкционированный доступ к ним создает две основные значительные угрозы для обеспечения безопасности всей АЭС:

– внесение дефектов в программы микропроцессорных устройства с целью вывода из строя управляющих систем и АЭС в целом;

– непреднамеренные ошибки оперативного и эксплуатационного персонала, при изменении установок срабатывания защит и калибровок.

В докладе представлен результат анализа развития регулирующих требований к защищенности от несанкционированного доступа, которые произошли за 10 лет в руководствах по безопасности Международного агентства по атомной энергии (МАГАТЭ), устанавливающих требования к управляющим системам АЭС, с учетом современного уровня развития технологий и научных знаний с целью обеспечения наивысших реально возможных стандартов безопасности для защиты персонала, населения и окружающей среды от вредного воздействия ионизирующих излучений [1, 2]. Результаты анализа могут быть использованы при совершенствовании национальной нормативной правовой базы по вопросам обеспечения ядерной и радиационной безопасности в части управляющих систем АЭС и ее гармонизации с рекомендациями МАГАТЭ.

**Литература**

1. Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций. Серия норм МАГАТЭ по безопасности. № NS-G-1.3 // МАГАТЭ, Вена, 2008. [Электронный ресурс]. – Режим доступа: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1116r_web.pdf. – Дата доступа: 07.05.2020.

2. Проектирование систем контроля и управления для атомных электростанций. Нормы безопасности МАГАТЭ. Специальное руководство по безопасности. № SSG-39 // МАГАТЭ, Вена, 2018. [Электронный ресурс]. – Режим доступа: http://www-pub.iaea.org/MTCD/Publications/PDF/P1694_R_web.pdf. – Дата доступа: 07.05.2020.

## ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

А.О. Дударенков, О.Б. Зельманский

Широкое распространение сетей подвижной радиосвязи обуславливает необходимость обеспечения защиты передаваемой по ним информации. В настоящее время шифрование речевой информации осуществляется на основе программных средств, не позволяющих подтвердить отсутствие незадекларированных возможностей и оценить их эффективность. Таким образом, задача защиты речевой информации, передаваемой по сетям радиосвязи, является весьма актуальной.

Предложен программный модуль для передачи зашифрованного речевого сигнала между мобильными устройствами. Данный модуль осуществляет передачу сигнала с минимальными искажениями, что позволяет избежать лавинного эффекта в криптографических преобразованиях. Предлагаемый модуль реализован на базе Sinch API на языке Java. Для тестирования модуля была сформирована база из 150 wav файлов, содержащих речевые сигналы длительностью от 3 до 10 с. В результате сравнительного анализа таких алгоритмов шифрования как AES, RSA, Triple DES, XOR, в качестве наиболее подходящего алгоритма шифрования был выбран алгоритм AES, средняя скорость шифрования и дешифрования которого составила 325 кб/с, а процент блоков, дешифрованных с ошибкой составил 4,738 %.

Разработанный программный модуль применяется совместно с удаленной гарнитурой и ограничением доступа речевого сигнала к встроенному микрофону мобильного устройства путем использования зашумляющего чехла, звуконепроницаемой камеры или его демонтажа.

## ОЦЕНКА УЯЗВИМОСТИ МОБИЛЬНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ SAILFISH OS

А.П. Жук, Е.С. Тран, Е.П. Жук

В настоящее время существует проблема импортозамещения в сфере информационных технологий, которая объясняется, в частности, потребностью в сертифицированных информационных технологиях, способных обрабатывать конфиденциальную информацию в соответствии с требованиями законодательства Российской Федерации.

Поскольку единственной отечественной мобильной операционной системой, которая имеет сертификат ФСТЭК по требованиям информационной безопасности, является Sailfish OS, разработанная ООО «Открытая мобильная платформа», то оценка ее безопасности и поиск уязвимых мест является актуальной задачей. С точки зрения возникновения уязвимостей, по мнению авторов, особый интерес представляет использование режима разработчика в Sailfish OS. Режим разработчика позволяет в разблокированном состоянии смартфона злоумышленнику получить root-доступ к нему, поэтому данное обстоятельство рассматривается авторами как уязвимость Sailfish OS. Данная схема атаки позволяет злоумышленнику загрузить на устройство вредоносное программное обеспечение, с помощью которого возможно удаленно контролировать все функции смартфона, а также скрытно использовать всю существующую периферию, что останется незамеченным для пользователя.

В качестве рекомендаций по локализации описанной уязвимости Sailfish OS, по мнению авторов, можно рекомендовать поддержание смартфона в состоянии физической безопасности, а также установку стойкого пароля на экран блокировки, что сделает невозможным реализацию атаки путем получения несанкционированного root-доступа к смартфону [1, 2].

**Литература**

1. Колисниченко Д.Н. Безопасный Android: защищаем свои деньги и данные от кражи. – СПб.: БХВ-Петербург, 2015. – 161 с.

2. Security – SailfishOS Documentation [Electronic resource]. – Access mode: https://sailfishos.org/wiki/Security. – Date of access: 03.04.2020.

## МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ ИЗБИРАТЕЛЬНОЙ ЗАПИСИ АУДИОИНФОРМАЦИИ

С.А. Зайкова, В.А. Ефремов

В работе предложено новое программное решение – специальное мобильное приложение, с помощью которого можно избирательно сохранять аудиозаписи пользователя, записанные с микрофона. Изучены средства и инструменты записи, источники и способы хранения, спроектировано и разработано собственное программное обеспечение.

Для создания мобильного приложения с избирательной записью аудиоинформации в работе используются следующие инструменты и методы. Model-View-ViewModel, адаптированная для современных платформ разработки пользовательского интерфейса, так как в предлагаемом программном решении специальным образом организована связь данных и MVVM шаблон делится на 3 части: модель, представление, модель представления. Первая часть отвечает за логику работы с данными и их описание, необходимых для работы приложения. Вторая часть отвечает за пользовательский интерфейс. Третья часть – это объект, в котором описывается логика поведения View в зависимости от результатов работы Model. JetPack navigation – навигация, обеспечивает согласованное и предсказуемое взаимодействие с пользователем, придерживаясь установленного набора принципов [1, 2]. Live data, учитывает жизненный цикл других компонентов приложения, таких как действия, фрагменты и/или службы. Эта гарантирует, что LiveData обновляет только те компоненты приложения, которые находятся в состоянии активного жизненного цикла. В разработке мобильного приложения также использован Manifest.perrmision, он объявляет любые разрешения, которые должны иметь другие приложения, если они хотят получить доступ к контенту из этого мобильного приложения.

В настоящее время в мобильном приложении реализованы функции записи с микрофона, пауза записи, остановка записи, сохранение в формате MP3, целевое воспроизведение аудиозаписей. В активной разработке находится добавление функции целевого поиска по словарю пользователя, реагирование/автозапись аудиофайла с учетом ключевых слов-оскорблений в зависимости от специфики жизненной ситуации: сфера обслуживания, грузоперевозки, медицинские, образовательные учреждения и др. объекты с потенциально возможными конфликтными ситуациями, возникающими в схеме: поставщик услуг – потребитель.

**Литература**

1. Карпюк И.А., Куляшова Н.М. Сравнительный анализ мобильных приложений и инструментальных средств их разработки // Научно-методический электронный журнал «Концепт». – 2017. – Т. 31. – С. 826–830. – URL: http://e-koncept.ru/2017/970180.htm.
2. Мобильное приложение с использованием AR-технологий для визитных карт / С.А. Зайкова [и др.] // Актуальные теории, концепции, прикладной характер современных научных исследований: сборник научных статей по итогам Международной научно-практической конференции. Санкт-Петербург, 30–31 мая 2019 г. – Спб.: Изд-во СПбГЭУ, 2019. – С. 32–34.

## ПОВЫШЕНИЯ РАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

А.В. Захаренко

На сегодняшний день важными задачами в системах видеонаблюдения является обнаружение объектов и детальное представление сцены. Основными препятствиями для более точной детализации при видеонаблюдении являются ограниченные возможности видеокамеры, неблагоприятные погодные условия, шумы, возникающими из-за плохой освещенности. Все это приводит к тому, что идентифицировать объекты может быть практически невозможно. Повышение разрешения изображений видеопоследовательности в системах видеонаблюдения позволит не только улучшить качество восприятия человеком изображения, но и качество последующей его обработки.

Часто используемым методом повышения разрешения является метод сверхразрешения. При сверхразрешении используется информация из других изображений с помощью микросканирования (процесс получения сдвинутых изображений низкого разрешения для последующего восстановления изображения высокого разрешения субпиксельной обработкой). Так как значение пикселя соответствует усредненному значению ярости некоторой окрестности точки на реальном изображении, то при смещении изображения объекта в разных кадрах на одинаковое значение части пикселя, усреднение производится по разным окрестностям. В итоге результирующее изображение высокого разрешения содержит в себе больше полезной информации. Если движение объекта и функция усреднения известны, то можно использовать информацию со всех кадров для построения одного изображения высокого разрешения.

Таким образом, метод сверхразрешения может использоваться для повышения детализации информации об объекте на видеопоследовательности.

## ВЗЛОМ КЛЮЧЕВОГО КОДА СТРУКТУРЫ ЦУ НА ОСНОВЕ РЕШЕНИЯ ЗАДАЧИ SAT

Л.А. Золоторевич, А.В. Павлова

В связи с проблемами пиратства, перепроизводства и контрафакции в последние годы стала актуальной необходимость защиты проектов СБИС, СнК от несанкционированного доступа в цикл проектирования и производства интегральных схем на основе создания общего подхода к их контролю. По оценкам Technology Information Handling Services (IHS), финансовый риск из-за контрафактных и несанкционированных микросхем оценивается в более чем 169 миллиардов долларов в год [1]. Кроме больших финансовых потерь существует реальная проблема обеспечения национальной безопасности.

В работе [2] проанализированы различные модели процесса злонамеренного искажения проекта, описывающие условия, при которых подобное искажение может внедриться в цифровую систему. В числе возможных источников искажений рассматриваются поставщики базовых функциональных блоков интеллектуальной собственности (IP’s), которые приобретаются разработчиками СнК, собственно разработчики СнК, а также кремниевые фабрики – изготовители СнК. Одним из методов борьбы с вышеупомянутыми угрозами является логическая блокировка. Основная идея блокировки состоит в том, чтобы изменить

конструкцию ИС, добавив в нее дополнительные логические элементы и новые входы, называемые ключевыми. Ключевые входы подключаются к защищенной от несанкционированного доступа памяти, а закодированная схема будет работать правильно только в том случае, если поданы правильные значения на ее ключевые входы. Значения ключевых входов передаются конечным пользователям. Одновременно с исследованиями по повышению эффективности кодирования разрабатываются и исследуются методы взлома кода [3].

В докладе рассматривается возможность раскрытия кода злоумышленником на основе описания зашифрованной схемы в виде КНФ булевой функции разрешения и решения выполнимости данной функции.

**Литература**

1. Subramanyan P., Ray S., Malik S. Evaluating the security of logic encryption algorithms // Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium. – IEEE, 2015. – P. 137–143.

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

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

## ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В РОБОТОТЕХНИКЕ

И.Ю. Изгачёв, М.А. Климович, А.И. Гридасов, А.А. Григорьев

Роботы используются уже более 50 лет в разных сферах деятельности человека: экономике, производстве, логистике, военном деле. Как и в случае других встроенных систем, производители робототехники уделяют первостепенное внимание безопасности, стоимости разработки, скорости выхода на рынок и предоставлению функций клиентам. Кибербезопасность имеет более низкий приоритет потому, что безопасность не является основным фактором для клиентов [1].

Роботы представляют собой встроенные системы и могут быть подвержены тем же типам кибератак, что и другие встроенные системы, а именно аппаратным атакам при изготовлении подобных систем, а также во время их использования.

Так, в штате Калифорния разрешили тестирование автомобилей, для которых водитель-человек не будет нужен даже в качестве запасного варианта. Этим транспортным средствам не обязательно иметь рулевое колесо, педаль тормоза или газа [2]. Подобные машины, смогут получать обновления программного обеспечения удаленно через Интернет. Гипотетическая атака будет состоять из двух частей: получение доступа к беспроводной системе обновления ПО автомобиля, дальнейшей загрузке в сеть измененной версии прошивки автомобиля, возможно, такой, которая позволит дистанционно управлять транспортным средством. Теперь злоумышленник контролирует легион автоматизированных автомобилей.

Военные дроны - это беспилотные летательные аппараты (БПЛА), дистанционно управляемые пилотом, их можно использовать для наблюдения и нападения на вражеские цели. Эти дроны могут быть модифицированы противником при изготовлении или транспортировке их частей. Модификации могут включать в себя удаленный выключатель, который позволит в определенный момент времени отключить дроны.

Согласно исследованию World Robotics 2019, к концу 2017 года насчитывалось около 2,44 млн. промышленных роботов [3]. Атака на предприятие может начаться с зараженного письма, которое устанавливает вредоносное ПО в корпоративной сети, позволяющее нарушителю напрямую управлять промышленными роботами, что может привести к их повреждению или уничтожению.

**Литература**

1. Mirjalili S.H., Lenstra A.K. Security observance throughout the life-cycle of embedded systems // Proceedings of the 2008 International Conference on Embedded Systems and Applications, ESA 2008. – 2008. – P. 186–192.
2. Baron E. Fully autonomous cars get lift from gov. jerry brown [Electronic resource]. – Access mode: http://www.mercurynews.com/2016/09/29/fullyautonomous-self-driving-cars-get-lift-from-governor. – Date of access: 10.05.2020.
3. Hagerty J. Meet the new generation of robots for manufacturing // Wall Street Journal. – 2015. – P. 3–4.

## ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА

А.Н. Кайтанова, И.А. Мурашко

В современном обществе способность надежно идентифицировать людей в режиме реального времени является фундаментальным требованием во многих приложениях, включая криминалистику, международные пересечения границ, финансовые транзакции и компьютерная безопасность. Традиционно для идентификации личности широко используется исключительное владение жетоном, например, паспортом или удостоверением личности. Для того чтобы уменьшить издержки на охранном персонале и повысить уровень физической безопасности применяют системы контроля и управления доступом (в здания и помещения). Как правило, современные офисные помещения снабжены камерами видеонаблюдения, поэтому в случае неправомерных действий посетителей их можно будет легко идентифицировать [1].

Данной задачей является учет рабочего времени сотрудников на основании анализа изображений с камер. Необходимо произвести поиск объекта на изображении с дальнейшим распознаванием и доступом.

Для реализации данной системы обычно используется камера, которая передает на входные данные, в виде изображения покадрово, на нейронную сеть. Алгоритм распознавания состоит из трех шагов: нахождение лица на изображении; поиск уникальных точек лица; распознавание лица с помощью сравнения уже существующей базой данных. Контроль и управление доступом будет представлен электромагнитным замком на двери [2].

Установка системы контроля доступа в здания и помещения позволит оценить эффективность, так как она позволяет исключить факты прохода посторонних лиц в здания, сократить количество сотрудников охраны, что в свое время уменьшит затраты на зарплату, а также вести учет рабочего времени сотрудников предприятия.

**Литература**

1. Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия Телеком, 2010. – 272 с.
2. Шолле Ф. Глубокое обучение на Python. – СПб.: Питер, 2018. – 400 с.

## ИСПОЛЬЗОВАНИЕ DSP БЛОКОВ FPGA ФИРМЫ XILINX ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

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

Одним из основных требований к современным системам цифровой обработки информации является высокая производительность. Достигнуть высокой скорости вычислений можно с помощью методов параллельной обработки, удобных для реализации в ПЛИС. FPGA фирмы Xilinx позволяют существенно увеличить производительность реализации алгоритмов обработки информации за счет использования параллельно работающих аппаратных узлов, размещенных на кристалле ПЛИС. Современные FPGA, кроме собственно логических ресурсов

и блоков ввода-вывода, содержат большое количество аппаратных блоков, реализующих часто используемые в цифровой схемотехнике операции. Аналогичные узлы, выполненные на просмотровых таблицах (LUT), требуют больше ресурсов кристалла и имеют пониженное быстродействие. В то же время аппаратная реализация этих блоков несущественно увеличивает площадь кристалла и стоимость ПЛИС, однако при этом заметно улучшает характеристики проекта в целом [1]. Одним из видов таких узлов являются блоки DSP (цифровой обработки сигналов). В докладе рассматривается использование DSP блоков в FPGA семейства Virtex-7 фирмы Xilinx для реализации различных конвейерных криптографических алгоритмов. Для иллюстрации используется алгоритм шифрования данных стандарта DES, который хорошо пригоден для конвейерной обработки.

FPGA семейства Virtex-7 фирмы Xilinx содержат блоки DSP48E1 [2]. В общем случае блоки DSP48E1 предназначены для реализации алгоритмов цифровой обработки сигналов и содержат избыточные для криптографических алгоритмов узлы такие, как умножитель, предварительный сумматор и некоторые другие. В криптографических алгоритмах блоки DSP48E1 могут использоваться в упрощенной конфигурации для реализации арифметических и логических операций, а также операции сравнения. Например, с помощью блоков DSP48E1 могут выполняться операции XOR для раундов алгоритма DES. В версии алгоритма DES, удобной для конвейерной реализации, эта операция 4-входовая, поэтому вычислительный модуль для раундов строится на трех блоках DSP48E1. Задержка выполнения операции XOR в блоках DSP48E1 составляет 4 такта, общая задержка модуля составляет 5 тактов синхронизации. Такой подход позволяет получить более экономичную реализацию конвейера алгоритма шифрования данных в целом за счет уменьшения количества используемых LUT кристалла FPGA.

**Литература**

1. Тарасов И. ПЛИС Xilinx и цифровая обработка сигналов. Особенности, преимущества, перспективы // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2011. – № 3.

2. 7 Series DSP48E1 Slice User Guide: [Электронный ресурс]. – Режим доступа: https://www.xilinx.com/support/documentation/user_guides/ug479_7Series_DSP48E1.pdf. – Дата доступа: 10.05.2020.

## ДВУХУРОВНЕВОЕ ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ДЛИНАМИ 192 И 1024 БИТ

Н.Г. Киевец

Широкое распространение получили электронные пластиковые карты (ЭПК), имеющие встроенный генератор случайных чисел (ГСЧ), который применяется для выработки криптографических ключей.

Оценка качества работы ГСЧ ЭПК может быть выполнена на основе двухуровневого тестирования вырабатываемых ГСЧ случайных последовательностей (СП), что позволяет также выполнить проверку статистических свойств отдельных сгенерированных СП, предназначенных для создания ключей.

Ранее автором было выполнено двухуровневое тестирование СП с длинами 128 и 256 бит, полученных от ГСЧ четырех ЭПК с микроконтроллером К5004 ВЕ2 [1, 2]. Полученные результаты показали высокое качество работы ГСЧ ЭПК.

В докладе обсуждаются результаты двухуровневого тестирования СП с длинами практически используемых ключей 192 и 1024 бит. СП получены от ГСЧ двух ЭПК с микроконтроллером К5004 ВЕ2, при тестировании применялся частотный тест. Полученные результаты представлены в виде таблиц и гистограмм. Выводы, сделанные по результатам тестирования СП с длинами 192 и 1024 бит, соответствуют выводам, сделанным ранее, и подтверждают возможность использования ГСЧ ЭПК для криптографических приложений.

**Литература**

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

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

## БЕЗОПАСНОСТЬ В RUBY ON RAILS

И.А. Клапаток, И.В. Чибисов, А.А. Виноградов, М.А. Климович

Ruby on Rails (RoR) – это популярная среда для веб-разработки, которая считается довольно легкой в освоении. Но, как и в любых средах разработки, в этой среде также нужно защищаться от разного рода атак.

Ниже представлены распространенные атаки в RoR.

1. XSS/Межсайтовый скриптинг: XSS-атака, наиболее распространенное нарушение безопасности в проектах Ruby on Rails, она может полностью разрушить веб-приложение. Она выбирает из множества точек входа для внедрения вредоносного кода в проект. XSS-атака может быть запущена со страниц результатов поиска, сообщений, комментариев, обзоров и т. д. Здесь вредоносный код остается интегрированным в продукт приложения и доступен для пользователя.

2. CSRF: сокращение от cross-site request forgery (подделка межсайтовых запросов). Использование метода match в файле rout.rb описывает систему обработки пути на сайте. Он помогает сопоставить конкретное действие всем возможным методам HTTP-запроса: GET, POST, PATCH, DELETE и т. д. Сканер безопасности Rails всегда предлагает передавать параметры через альтернативные методы HTTP и отслеживать ответы сервера.

Разработчики RoR создали механизм защиты от таких атак, который называется аутентификация токенов.

3. SQL Инъекции: часто используются злоумышленниками для поиска способа передачи непроверенных данных. Инъекция SQL не только открывает доступ к базе данных, но также предоставляет возможность доступа к конфиденциальным данным. Хакеры часто используют SQL-инъекцию для поиска определенной информации, поскольку она позволяет быстро искать нужные записи. Также хакеры используют возможность вводить вредоносный код в SQL записи.

4. Clickjacking (англ. «захват клика»): Сетевая атака, которая автоматически перенаправляет пользователя на другую страницу без ущерба вашему сайту. Clickjacking – это меньшее из зол. Хакеры часто использую такие атаки, чтобы увеличить количество посетителей стороннего ресурса. В среде разработки RoR появился механизм, который может предотвращать такие перенаправления. Это можно сделать, добавив HTTP-заголовок «X-Frame-Options: SAMEORIGIN» на созданные страницы.

В Ruby on Rails разработаны необходимые механизмы и методы защиты, чтобы обеспечить высокий уровень безопасности. Следуя нескольким кратким руководствам по предотвращению потенциальных проблем безопасности, вы можете легко рассчитывать на преимущества, которые инфраструктура Ruby on Rails предлагает для веб-разработки [1].

**Литература**

1. Ruby on Rails: Guides [Электронный ресурс]. – Режим доступа: https://rubyonrails.org. – Дата доступа: 10.05.2020.

## БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНЫХ СЕТЯХ

Д.А. Климов

Особенности практических задач обеспечения безопасности конкретных операционных систем связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Уязвимыми являются буквально все основные структурно-функциональные элементы современных ОС. Защищать компоненты ОС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Угрозы безопасности операционной системы существенно зависят от условий ее эксплуатации, от того, какая информация в ней хранится и обрабатывается, и т.д.

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации:

– по цели атаки;

– по принципу воздействия на операционную систему;

– по типу используемой злоумышленником уязвимости защиты;

– по характеру воздействия на операционную систему.

Вышеперечисленные типы угроз и проникновений могут вызывать множество видов проблем различных уровней – от относительно безобидных до представляющих крайне серьезную степень опасности. Тем не менее, даже кажущиеся несерьезными нарушения могут в итоге приводить к существенному нарушению работы корпоративных сетей. Именно поэтому в современном мире необходимо осуществлять постоянный пересмотр и обновление подходов к защите операционных систем [1].

Политика безопасности должна учитывать два главных фактора:

– максимальную защиту операционных систем от внешних и внутренних, санкционированных и несанкционированных вторжений;

– доступность и отзывчивость для администраторов и пользователей самой корпоративной сети [2].

**Литература**

1. Шаньгин В.Ф. Комплексная защита информации КС. Эффективные методы и средства. – М: ДМК-Пресс, 2010. – 545 с.

2. Проскурин В.Г. Защита в операционных системах. – М.: Горячая линия – Телеком, 2014. – 192 с.

## АСИМПТОТИКА ДЛЯ ВЕРОЯТНОСТИ ОШИБКИ ПРИ НАБЛЮДЕНИИ ЛЕБЕГОВСКОЙ МЕРЫ ВЕКТОРОВ ПЕРЕХОДОВ

И.П. Кобяк

Рассмотрен метод идентификации случайных процессов оценками вероятности наблюдения векторов переходов. Определена верхняя граница для вероятности пропуска ошибки, соответствующая данному алгоритму при регистрации заданных пар событий в асимптотике. Полученное соотношение позволило выполнить сравнение уровней ошибки, порождаемых методом наблюдения векторов переходов с известными алгоритмами формирования контрольных кодов, такими как сигнатурный анализ и счет векторов состояний.

Применительно к задаче наблюдения и анализа многомерных последовательностей сущность алгоритма синтеза векторов переходов заключается в следующем. Система идентификации настраивается на регистрацию пар $r$-разрядных векторов, формируемых источником последовательностей случайных событий, в моменты переключения его выходов из состояния $A(t)$ в состояние $A(t+1)$. При этом считается, что в $\nu$-м разряде ВП формируется логическая единица, если в последовательности из двух векторов состояний (ВС) также

в $\nu$-м разряде имеет место переключение бита из 0 в 1. Все остальные пары символов в том числе и переход из 1 в 0 в системе идентификации рассматриваются как логический ноль, то есть фактически осуществляется измерение числа ВП заданного вида, образуемых $3^{r-\mu}$ парами ВС из $m^2$ со сдвигом $\tau = 1$, где $m = 2^r$, а параметр $\mu = sum\ v$ [1].

В представляемой работе получены следующие результаты: 1) выполнен анализ структурных компонентов $r$-разрядных последовательностей с точки зрения длины серии из единиц, определяющей отсутствие или наличие возможности формирования очередного субдинамического объекта; 2) на основе вероятностного анализа получено равенство для среднего числа последовательных пар объектов в бесконечной выборке событий; 3) показано, что увеличение выборочной вероятности наблюдения лебеговской меры ВП при $\mu = r$ приводит к уменьшению значения верхней границы вероятности пропуска ошибки за счет отсутствия перестановок в ВС на местах расположения регистрируемых ВП; 4) сравнительный анализ метода наблюдения лебеговской меры ВП с алгоритмами линейной свертки и СВС показал, что в асимптотике принцип идентификации случайных процессов вероятностью ВП имеет явное преимущество перед известными алгоритмами синтеза точечных оценок; 5) используя алгоритм перекодирования состояний в выборке, при бесконечном $n$, можно заключить, что полученные результаты будут справедливы и для любых пар соседних векторов заданного вида.

**Литература**

1. Кобяк И.П. Теория внутрисхемного наблюдения СБИС с использованием автокорреляционных функций // Автоматика и вычислительная техника. – 2009. – № 2. – С. 37–46.

## РАСЧЕТ ПРОСТРАНСТВ АТОМА ВОДОРОДА ДЛЯ РЕШЕНИЯ ЗАДАЧ КВАНТОВОЙ КРИПТОГРАФИИ

И.П. Кобяк

Для решения задач синтеза квантово-криптографических систем передачи информации предложена модель формирования релятивистских радиусов атома водорода как лоренцева расширения радиуса Бора. Полученные на основе Лоренцевых преобразований соотношения позволили определить связи центроаффинных пространств атома с учетом представления параметров комплексными величинами. Принцип образования первого $\tau = 1$ релятивистского радиуса боровской орбиты рассмотрен с учетом Лоренц-фактора $\gamma_0$ для составляющих классической формулы. В приведенном соотношении учтено, что масса покоя является векторной, так как природа существования позитрона и его энергетика являются аналогами электрона в пятом измерении. Показано, что скорость движения электрона создает собственную материальную копию шестого измерения в комплексном пространстве, не изменяя массы покоя в установившемся режиме. Данный факт вытекает из следующих рассуждений. Радиус-вектор вращения релятивистской копии электрона может быть рассчитан с использованием поправок Лоренца к формуле Бора. При этом учитывается следующее: 1) гауссовские единицы для заряда электрона можно выразить из общеизвестных физических соотношений таких, например, как стандартная формула для нулевого радиуса; 2) следствием данного факта является отсутствия релятивистских поправок у отношения $\hbar^2 e^{-1}$. Таким образом, в знаменателе соотношения для нулевого радиуса необходимо использовать только поправку для теоретической массы покоя. При этом значение радиуса первой релятивистской орбиты, вытекающее из классического равенства для радиуса Бора, определится коррекцией известной формулы в знаменателе. Знак плюс в полученном соотношении говорит о принадлежности нового радиуса комплексному пространству радиуса $r_0$ со скоростью движения материи, совпадающей по направлению со скоростью материальных объектов того же третьего измерения. Итак, численное значение указанного параметра будет равно 9,6332 ангстрема. Учтем теперь, что значение угловой частоты $\omega_0$ может быть определено на основании «косвенно измеренной» скорости $v_0$, а угловая частота вращения релятивистской копии имеет поправку Лоренца аналогично радиусу, с учетом линейная скорость первой релятивисткой орбиты. Тогда для уже известного значения $v_{0,1} = 67{,}514$ скорость первой релятивистской

орбиты будет равна 1 165,0392 км/с. Соответственно, релятивистская поправка для первой релятивистской орбиты электрона будет иметь мнимое представление численно равное значению *j*5,404. Данный параметр, очевидно, переводит скорость первой релятивистской орбиты в пятое измерение с уровнем: –48 117, 522 км/с. Общие расчеты в данной работе показали, что масса электрона теоретически, испытывая сжатие за счет скорости $v_0$, создает релятивистскую утечку плазмы в третье измерение и далее в мнимое пространство $-Im$ за счет первой релятивистской скорости и создает собственную орбиту $\tau = 1$ с собственной массой шестого измерения $-m_{0,\tau=1}$.

## ОБРАБОТКА ТРЕВОЖНЫХ СООБЩЕНИЙ, ПОСТУПИВШИХ ОТ СРЕДСТВ СБОРА, ОБРАБОТКИ И ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ

А.Н. Коваленко

Средства сбора, обработки и представления информации (ССОИ) – совокупность устройств, предназначенных для обработки информации, поступающей от средств обнаружения и наблюдения с целью последующего ее преобразования в вид, удобный для восприятия оператором, другими лицами караула, выдачи управляющих сигналов различного назначения, а также контроля работоспособности средств обнаружения, дистанционно управляемых устройств и каналов передачи информации.

В процессе обработки часовым-оператором тревожных сообщений, поступивших от ССОИ, мы часто сталкиваемся с проблемой формальной (некорректной) обработки данных сообщений. Для решения проблемы, в процессе разработки интерфейса автоматизированного рабочего места часового-оператора, необходимо прописать ряд правил по созданию диалоговых окон, выводимых на экран.

К таким правилам относится:

– возможность выбора одного из заранее подготовленных вариантов оценки поступившего события;

– исключение открытия нескольких диалоговых окон, при повторных срабатываниях одного технического средства охраны в течение установленного времени;

– новые сигналы, принадлежащие одному происшествию, должны добавляться в открытое диалоговое окно;

– при возникновении нескольких ложных тревог в течение небольшого промежутка времени от одного технического средства охраны, должно автоматически создаваться сообщение о неисправности и обеспечиваться возможность контроля устранения неисправности;

– сообщения диалогового окна при срабатываниях должны иметь ранжирование по степени угрозы и т.д.

**Литература**

1. Гарсиа М.Л. Проектирование и оценка систем физической защиты. – М.: АСТ, 2003 – 386 с.

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

## АРХИТЕКТУРА СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

И.П. Ковятинец

Система обнаружения вторжений (Intrusion Detection System, IDS) – это программное или аппаратное средство, предназначенное для предупреждения, выявления и протоколирования некоторых типов сетевых атак. В отличие от файерволов, в обязанности IDS не входит блокировка подозрительного траффика. IDS пытается выявить подозрительную активность и поднять тревогу.

IDS сетевого уровня анализирует все поля пакетов, в том числе и поле данных, которое переносит информацию приложений. IDS хоста анализирует события, происходящие в операционной системе и приложениях.

Источниками данных для сетевой IDS являются маршрутизаторы, коммутаторы и хосты локальной сети.

Датчик копирует пакеты и передает их анализатору. Датчик может представлять собой отдельный компьютер или же это может быть программный компонент маршрутизатора.

Анализатор получает данные от датчиков и проверяет их на наличие угроз и подозрительной активности в сети. Анализатор работает на основе правил, составленных администратором системы безопасности предприятия в соответствии с политикой безопасности. При выполнении одного из правил анализатор передает сообщение «тревога» менеджеру IDS – программной компоненте, которая хранит конфигурацию IDS. Менеджер оповещает оператора о тревоге в виде уведомления.

Оператор IDS на основе данных уведомления принимает решение о реакции сети на подозрительную активность – это может быть отключение сетевого интерфейса, изменение правил файервола для блокировки пакетов или же игнорирование уведомления, если оператор считает, что вероятность вторжения очень мала.

Описанная выше архитектура является функциональной, в реальной IDS эти функции не обязательно реализуются в отдельных блоках или модулях системы. В минимальном варианте все функции IDS могут быть сосредоточены в программном обеспечении компьютера, сетевой адаптер которого выполняет роль датчика.

**Литература**

1. Олифер В.Г., Олифер Н А. Безопасность компьютерных сетей. – М.: Горячая линия – Телеком, 2016. – 644 с.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2013. – 960 с.

## МЕТОДЫ ПРОТИВОДЕЙСТВИЯ АТАКАМ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА DNS

Н.Р. Коляго, Д.Н. Одинец

Атаки с использованием инфраструктуры DNS в основном относятся к DoS атакам. К ним можно отнести «отраженные» атаки и «отраженные» атаки с усилением. Эффективных способов защититься от таких атак нет. Фильтрация пакетов позволяет лишь частично ослабить воздействие.

Также с помощью DNS можно произвести разведывательную атаку. Обычно она является частью какой-то другой атаки. Защититься от нее можно только путем недопущения хранения чувствительной информации в системе DNS.

Протокол DNS разрабатывался с идеей общедоступности, никакой аутентификации пользователя или шифрования данных не предусмотрено. Кроме того, он реализован с помощью протокола UDP.

Обновление записей в реальном времени или по запросу является основной функцией DDNS (Dynamic DNS). Злоумышленник, подменив адрес в пакете DNS, мог добавить на сервер новую запись либо обновить существующую.

Отравление кэша (атака Каминского) [1] эксплуатирует отсутствие существенной проверки источника ответов и отсутствие установки соединения в протоколе UDP. Она позволяет подменить ресурсную запись в кэше рекурсивного сервера

DNS трафик может быть модифицирован Интернет-провайдером. Для защиты от таких атак были разработаны расширения DNSSEC и экспериментальный протокол DoH (DNS over HTTPS), которые обеспечивают надежность. Также DNS-серверы уязвимы перед DoS атаками случайного поддомена и NXDOMAIN атаками. Они заключаются в трате ресурсов на заведомо бесполезный поиск адреса. От таких атак, как и от других DoS невозможно полностью защититься, можно лишь смягчить воздействие путем оптимизации программного кода сервера и фильтрации входящих пакетов [2].

**Литература**

1. The Hitchhiker's Guide to DNS Cache Poisoning [Electronic resource]. – Access mode: https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. – Date of access: 15.03.2020.

2. DNS Amplification Attack Detection and Mitigation via sFlow with Security-Centric SDN / A. Atan [et al.] // IMCOM '17. – 2017. – P. 1–7.

## ОЦЕНКА ЭФФЕКТИВНОСТИ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ИНФОРМАЦИОННЫХ СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

В.Н. Корделюк

Информационные сети военного назначения (ИСВН) являются технической основой для интеграции информационных ресурсов (ИР), в том числе относящихся к информации ограниченного распространения, в единое информационное пространство Вооруженных Сил. Для защиты ИР ограниченного распространения в ИСВН и их сегментах создаются системы защиты информации (СЗИ).

Состав используемых мер (средств) защиты ИР ограниченного распространения, как правило, формируется на основании требований нормативных правовых актов различного уровня. При этом в качестве оценки эффективности функционирования СЗИ контролирующие лица используют степень выполнения предписанных требований нормативных правовых актов. Недостатком этого подхода является отсутствие учета стоимости реализации используемых мер защиты, которая, согласно принципу экономической целесообразности, не должна превышать стоимость защищаемого информационного ресурса.

ИСВН, в которых циркулируют ИР ограниченного распространения, не имеют точек доступа к глобальной сети Интернет. В силу этого в качестве потенциальных субъектов угроз безопасности информации следует рассматривать внутренних пользователей (инсайдеров), имеющих правомочный доступ к ИСВН. Согласно проведенным исследованиям, угрозы безопасности информации со стороны инсайдеров следует классифицировать как несанкционированный доступ, несанкционированное воздействие и компьютерная атака.

Предлагается подход оценки эффективности функционирования СЗИ и ее подсистем, основанная на методах теории военно-экономического анализа. В качестве оценки эффективности мер защиты введен количественный критерий, учитывающий стоимость защищаемой информации, стоимость трудовых и материальных ресурсов, затраченных на создание подсистем, а также время их функционирования в течение контролируемого периода. Для поддержки принятия решений по оценке эффективности принимаемых мер защиты разработаны интервальные диапазоны значений параметров, по которым производится расчет соответствующих показателей. Ко всем возможным сочетаниям диапазонов дается вербальная интерпретация оценки эффективности, а также приводятся рекомендации по повышению ее эффективности.

Внедрение в практику данного подхода позволит унифицировать процедуру оценки эффективности принимаемых мер защиты и принимать решения, оптимизирующие функционирование СЗИ.

## СОБЛЮДЕНИЕ ЭТИЧЕСКИХ НОРМ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.А. Криштопова, А.М. Прудник

Согласно статистическим данным, в 2019 г. 34 % всех утечек данных происходили при участии сотрудников самих организаций, причем в 71 % случаев причиной было желание получения финансовой выгоды [1].

Этические нормы определяют социально приемлемое поведение, в отличие от законов, которые предписывают или запрещают определенное поведение. Основным отличием этических норм от законов является то, что несоблюдение законов влечет за собой наступление ответственности (дисциплинарной, материальной, гражданско-правовой, административной и уголовной).

Многие профессиональные группы и сообщества имеют четкие правила, регулирующие этическое поведение на рабочем месте. Области информационных технологий и информационной безопасности обязательных кодексов этики не имеют. Тем не менее, профессиональные ассоциации

и сертифицирующие агентства работают над созданием кодексов этики, предполагая, что в них можно предписать исполнение этических норм, но, в тоже время, допуская, что не всегда существует возможность отстранить нарушителей этих кодексов от выполнения определенных видов работ или даже от занятия определенных должностей.

В качестве основных кодексов этики, которые можно использовать в областях информационных технологий и информационной безопасности, следует упомянуть Десять заповедей компьютерной этики [2], Кодекс этики и профессионального поведения Ассоциации вычислительной техники [3], Кодекс профессиональной этики ISACA и др. [4].

Основным способом в выравнивании этических представлений среди персонала организации является обучение. Сотрудники должны быть обучены ожидаемому от них этическому поведению, особенно в области информационной безопасности. Надлежащая этическая подготовка жизненно важна для создания информированного, хорошо подготовленного сотрудника.

**Литература**

1. 2019 Data Breach Investigations Report. Verizon.

2. The Ten Commandments of Computer Ethics [Electronic resource]. – Access mode: http://www.computerethicsinstitute.org/images/TheTenCommandmentsOfComputerEthics.pdf. – Date of access: 10.05.2020.

3. Code of Ethics [Electronic resource]. – Access mode: https://www.acm.org/code-of-ethics. – Date of access: 10.05.2020.

4. Code of Professional Ethics [Electronic resource]. – Access mode: https://www.isaca.org/credentialing/code-of-professional-ethics. – Date of access: 10.05.2020.

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИСПОЛЬЗОВАНИЯ АТОМНОЙ ЭНЕРГИИ

А.М. Кузьмицкий

Анализ особенностей функционирования средств физической защиты (СФЗ) ядерного объекта (ЯО) предопределяет необходимость защиты информации, чувствительной по отношению к несанкционированным воздействиям на нее, в результате чего может быть снижена эффективность функционирования СФЗ в целом или ее отдельных элементов.

Прежде всего, должны защищаться сведения, в результате разглашения, утраты, утечки, уничтожения, искажения или подмены которых нарушается функционирование СФЗ.

Объем и степень секретности обрабатываемой в СФЗ информации, режим обработки данных и соответственно уровень требований по защите информации будут различны в зависимости от степени интеграции различных подсистем СФЗ, от характера взаимодействия в конкретной системе, а также с системами учета и контроля ядерных материалов, технологической безопасности и др.

Характерными свойствами функционирования СФЗ ЯО как автоматизированной системы, с точки зрения информационной безопасности являются:

– наличие информации, составляющей государственную и служебную тайну, а также информации конфиденциального характера о различных аспектах функционирования СФЗ;

– территориальное размещение компонентов СФЗ в различных охраняемых зонах ЯО, доступ в которые имеет ограниченный и строго дифференцированный персонал;

– размещение компонентов СФЗ в транспортных средствах, перевозящих ЯМ;

– строгое разделение функциональных обязанностей, распределение полномочий и прав на выполнение регламентных действий между персоналом СФЗ.

**Литература**

1. Об использовании атомной энергии: Закон Респ. Беларусь 30.06.2008 г. № 426-З. – Минск, 2010.

2. ТКП 360-2011 (02300). Положения об общих требованиях к системам физической защиты ядерных объектов. – Минск, 2015.

## РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ «УМНОГО» ДОМА

В.Ф. Кулиш

Системы «умного» дома устанавливаются во все большем количестве квартир и домов. Это создает более комфортные условия для жизни и позволяет накапливать информацию о пользовательских привычках. Пользователи могут создавать и изменять сценарии управления домом использую накопленные данные, что ведет к экономии потребляемых ресурсов. Системы такого вида, как правило, включают в себя большое количество датчиков, а также контролирующие устройства для включения или выключения приборов в доме на основании данных, поступающих от датчиков. Данные о работе приборов в доме накапливаются концентратором, который управляет всеми устройствами, а затем отправляет накопленную информацию на сервер. Сервер, помимо хранения накопленной информации, позволяет удаленно управлять устройствами в квартире или доме. Таким образом архитектура системы «умного» дома состоит из трех слоев: сенсорный слой (собирает информацию о состоянии жилого помещения), слой контроля (управляет устройствами на основе данных от сенсорного слоя), слой хранения (хранит исторические данные о работе приборов). Основными рисками информационной безопасности таких систем являются утечка информации о текущих и о предыдущих состояниях устройств в доме, удаленный контроль над приборами в доме, а также заражение устройств вредоносным программным обеспечением. Данные риски могут быть реализованы с помощью следующих атак.

1. Сбор и анализ метаданных сетевого трафика устройств.
2. Получение доступа к серверу сбора данных.
3. Получение удаленного доступа к одному из устройств системы или всей системе «умного» дома.
4. Создание виртуальной копии устройства для получения статистики работы реального устройства в системе.

## СПОСОБЫ АТАК НА БЕСПИЛОТНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА

Д.В. Куприянова, Д.Ю. Перцев

Постоянное развитие беспилотных транспортных средств привело к постоянному увеличения числа используемых сенсоров и датчиков, совершенствованию программного обеспечения. Однако это приводит к сложностям в организации системы безопасности. Анализ способов атак [1] позволил выделить следующие подходы:

– удаленный доступ на большом расстоянии. Осуществляется с помощью беспроводных интерфейсов связи, установленных на беспилотном автомобиле. При этом можно выделить дополнительные разновидности атаки: на коммуникационные протоколы (например, голосовой ассистент), на систему удаленного управления транспортным средством (по мнению авторов в перспективе данный способ станет менее актуален), на компоненты транспортного средства (телематику, информационно-развлекательную систему и т.д.), на инфраструктуру (например, сервисы обновления программного обеспечения);

– удаленный доступ на коротком расстоянии. При этом можно выделить дополнительные разновидности атаки: с применением коммуникационных протоколов WiFi и Bluetooth, на систему контроля давления в шинах (TPMS), на сенсоры транспортного средства [2, 3] (например, создание помех);

– с непосредственным доступом к транспортному средству: воздействие на электронный блок управление с помощью OBD-II сканнера, воздействие через планшет, установленный в машине.

**Литература**

1. Dr. Charlie Miller. Securing Self-Driving Cars (one company at a time) [Electronic resource]. – Access mode: http://illmatics.com/securing_self_driving_cars.pdf. – Date of access: 03.05.2020.
2. Petit J. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR [Electronic resource]. – Access mode: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf. – Date of access: 03.05.2020.
3. Dr. Charlie Miller. Remote Exploitation of an Unaltered Passenger Vehicle [Electronic resource]. – Access mode: http://illmatics.com/Remote%20Car%20Hacking.pdf. – Date of access: 03.05.2020.

## ТОКОПЕРЕНОС ПО ЛОВУШЕЧНЫМ СОСТОЯНИЯМ В ОКСИДЕ МОЛИБДЕНА

А.А. Курапцова

Оксид молибдена $MoO_3$ находит применение в перезаряжаемых батареях, конденсаторах, газовых сенсорах адсорбционно-резистивного типа, в качестве прозрачного электрического контакта в дисплеях и солнечных батареях. Благодаря слабому поглощению электромагнитного излучения и способностью разделять сгенерированные солнечным излучением носители заряда оксид молибдена значительно увеличивает эффективность солнечных элементов и устройств фотокатализа.

Оксид молибдена обладает относительно высокой проводимостью благодаря неглубокому залеганию ловушечных состояний и их высокой концентрации около $10^{19}$ $см^{-3}$, которые ответственны за транспорт носителей заряда. Моделирование токопереноса по ловушкам проводилось с использованием модели фонон-облегченного туннелирования. Были получены зависимости плотности туннельного тока от напряженности внешнего поля для различных глубин залегания ловушечного уровня и от концентрации ловушек для различных значений напряженности поля.

Изменение глубины залегания ловушечных состояний от 0,3 эВ до 0,7 эВ вызвало значительное уменьшение плотности тока с $10^3$ $мА/см^2$ до $10^{-3}$ $мА/см^2$ для значения напряженности поля $10^6$ В/м. Увеличение концентрации ловушек ведет к уменьшению расстояния между ними и, следовательно, нелинейному возрастанию тока. Также изменение напряженности поля в диапазоне от $2 \cdot 10^5$ В/м до $5 \cdot 10^6$ В/м ведет к нелинейному росту тока, не меняя характер его зависимости от концентрации ловушек.

Таким образом возможность изменения режима токопереноса и возможность достижения высоких значений плотности туннельного тока в оксиде молибдене делает его перспективным материалом для применения в устройствах фотокатализа, солнечных элементах и газовых сенсорах за счет высокой концентрации ловушечных состояний и относительно небольшой глубине их залегания.

## ПРИБОРЫ И МЕТОДЫ ДЛЯ ТЕСТИРОВАНИЯ ЛИНИЙ СВЯЗИ

О.А. Кураш

Все современные информационные системы и технологии связаны с необходимостью обмена информацией и использованием линий связи (ЛС) различных типов. Любая ЛС на этапе подготовки к эксплуатации должна быть протестирована специальным оборудованием для выявления тех или иных дефектов, а также на соответствие заданным характеристикам. Этот этап построения имеет фундаментальное значение, т. к. от результатов тестирования зависит как качество и долговечность установленной системы, так и быстрота и мобильность передачи информации между оконечным оборудованием и подключенными пользователями.

Существуют два основных метода тестирования линий связи − тестирование на постоянном и переменном токе. Тестирование на переменном токе выполняется двумя способами − путем измерения падающей волны или измерения отраженной волны (метод

рефлектометрии). Измерения на постоянном токе и измерения падающей волны используются для определения первичных и вторичных параметров линии. Оба метода могут быть реализованы как путем непосредственного измерения волны, так и с применением метода сравнения, частным случаем которого является мостовой метод.

Современная концепция тестирования сетей связи опирается на модель взаимодействия открытых систем OSI, в соответствии с которой все измерительные приборы для тестирования сетей связи подразделяются на две категории:

1) анализаторы физического уровня (первый уровень OSI);

2) анализаторы более высоких уровней (со второго по седьмой).

К анализаторам физического уровня относятся мультиметры, кабельные тестеры, рефлектометры, осциллографы, измерители уровня сигнала и анализаторы спектра. Вторая группа анализаторов второго-седьмого уровней модели OSI измеряет параметры циклов и пакетов, проверяет целостность данных, сеансы связи, преобразование данных и приложения. Это могут быть карманные тестеры, анализаторы протоколов в виде универсальных приборов со специальными модулями для решения различных задач или пакеты программ для использования в комплексах тестирования и для управления сетевых узлов.

**Литература**

1. Абилов А.В. Сети связи и системы коммутации: учебное пособие для вузов. − М.: Радио и связь, 2004. – 288 с.

2. Тестирование трасс структурированных кабельных систем [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/testirovanie−trass−strukturirovannyh−kabelnyh−sistem. – Дата доступа: 10.05.2020.

## ОБОБЩЕНИЯ КОДОВ ХЕММИНГА

А.В. Кушнеров, В.А. Липницкий

Коды Хемминга – это классика теории помехоустойчивого кодирования [1]. Данное семейство кодов хорошо изучено как с теоретической, так и практической точек зрения. Классический двоичный код Хемминга $C^1_{\chi,n}$ имеет длину $n=2^m-1,$ задается проверочной матрицей, которая состоит из всех степеней примитивного элемента $\alpha$ конечного поля $GF\left(2^m\right),$ и имеет минимальное расстояние три, то есть способен исправлять ошибки весом 1.

Разработанная в [2], теория норм синдромов стимулировала систематические исследования непримитивных БЧХ-кодов, имеющих произвольную нечетную длину $n$, и их конструктивно предельно простой случай – непримитивных кодов Хемминга. У последних в проверочной матрице элемент $\alpha$ заменен непримитивным элементом $\beta$ порядка $n$ в поле $GF\left(2^m\right)$. Как показали исследования, примерно у трети таких кодов Хемминга минимальное расстояние $d$ оказалось большим 3.

Последнее обстоятельство послужило побудительным мотивом к рассмотрению более широкого класса обобщенных (непримитивных) кодов Хемминга. Столбцы проверочной матрицы обобщенного кода Хемминга $C^k_{\chi,n}$ нечетной длины $n$ представляют собой степени элемента $\beta$, предварительно возведенного в некоторую степень $k$. Спектр таких степеней ограничен следующим образом: $1\le k\le n-1.$

Установлено, что число различных кодов Хемминга заданной длины $n$ не превосходит количества различных циклотомических классов по модулю $n$, на которые разбивается множество $T_n=\left(1,2,...,n\right)$. Конкретные свойства и корректирующие возможности новых кодов требуют теоретических исследований и кропотливых компьютерных вычислений.

**Литература**

1. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мн.: Издательский центр БГУ, 2007. – 216 с.

## ТРИПЛЕТНАЯ СВЕРХПРОВОДИМОСТЬ В СТРУКТУРАХ СВЕРХПРОВОДНИК-ФЕРРОМАГНЕТИК ПРИ ПЕРИОДИЧЕСКОМ ИЗМЕНЕНИИ НАМАГНИЧЕННОСТЕЙ

В.Н. Кушнир

В настоящее время проводятся интенсивные исследования по созданию работающего прототипа сверхпроводникового компьютера с элементной базой, включающей гетероструктуры типа сверхпроводник(S)/ферромагнетик(F) [1]. Принцип работы элементов на S/F гетероструктурах состоит в управлении их критической температурой и критическим током путем изменения состояния ферромагнитной подсистемы. В данной работе исследовалась структура с вращающимся магнитным моментом управляющего *F*-слоя в формализме нестационарных уравнений диффузионного предела микроскопической теории сверхпроводимости относительно функций Грина, заданных в пространстве Намбу – Келдыша. Определялись условия реализации схемы периодической накачки триплетной компоненты сверхпроводящего конденсата. Найдено унитарное преобразование, которое сводит задачу о планарном периодическом вращении магнитного момента F-слоя к стационарной задаче с вектором эффективного обменного поля, величина и направление которого зависят от частоты вращения. Помимо того, кинематический фактор унитарного преобразования отражается слабой намагниченностью всей структуры в направлении, ортогональном плоскости слоев. Это приводит к перераспределению (1, 1) и (1, 0) триплетных компонент и возникновению дополнительной триплетной компоненты (1, –1) [2]. Перераспределение триплетных компонент является эффектом первого порядка по параметру, равному отношению критической температуры структуры к обменной энергии, выраженной в кельвинах.

**Литература**

1. Holmes D.S., Ripple A.L., Manheimer M.A. IEEE Trans. Appl. Supercond. – 2013. – Vol. 23, №. 3. – P. 1701610(3).

2. Konschelle F., Buzdin A. Phys. Rev. Lett. – 2009. – Vol. 102. – P. 017001(4).

## АНТИОТРАЖАЮЩИЕ ПОКРЫТИЯ ВИДИМОГО И ИНФРАКРАСНОГО ДИАПАЗОНОВ НА ОСНОВЕ АНОДНЫХ ОКСИДОВ ВЕНТИЛЬНЫХ МЕТАЛЛОВ

А.С. Лазарук, В.В. Дудич, Д.А. Сасинович, О.В. Купреева

Светопоглощающие покрытия для излучения видимого и инфракрасного диапазонов являются составляющими компонентами в стелс-технологии, и одним из средств, используемых для снижения заметности объектов. Кроме того, светопоглощающие покрытия обеспечивают увеличение эффективности работы оптоэлектронных устройств, преобразующих оптический сигнал в электрический. К таким устройствам относятся солнечные батареи, фотодетекторы и др. Кроме способности к светопоглощению, к таким материалам предъявляют еще ряд требований: они должны обладать высокой механической прочностью, устойчивостью к износу и перепадам температур.

Проведено исследование влияния режимов формирования анодных оксидов вентильных металлов ряда Al, Ti, Nb на их светопоглощающие свойства в видимом и инфракрасном диапазонах. Доказано, что за счет предварительной механической обработки поверхности и использования специальных режимов формовки, полученные оксидные пленки обеспечивают от 95 % поглощения оптического сигнала в видимом диапазоне и от 90 % в инфракрасном.

Установлено, что светопоглащающие покрытия с наилучшими характеристиками получают в органических электролитах. Полученные результаты использованы для формирования антиотражающих покрытий корпусов микросхем, используемых в устройствах для фотосъемки поверхности Земли. Данные покрытия позволяют снизить фоновое излучение светового потока от корпуса фотодетектора, вследствие чего уменьшается «шум» на получаемом изображении.

## КОНДЕНСАТОРЫ ПОВЫШЕННОЙ ЕМКОСТИ НА ОСНОВЕ ПОРИСТОГО АЛЮМИНИЯ

С.К. Лазарук, Л.П. Томашевич, Д.А. Манцевич, К.Т. Кольченко, А.А. Кисель, О.В. Купреева

В RFID (Radio Frequency Identification; радиочастотная идентификация) интегральных микросхемах необходимо использование конденсатора высокой емкости. Традиционные планарные технологии не позволяют решить эту задачу. Наноструктурированный пористый алюминий, формируемый методом электрохимического анодирования, может быть использован как материал для обкладок конденсатора высокой емкости.

Исходные пленки алюминия толщиной до 3 мкм осаждали на установке электронно-лучевого напыления. Наноструктурирование алюминиевой поверхности проводили в электролитах на основе водного раствора NaCl при анодном напряжении до 50 В. Исследования на электронном микроскопе показали, что в результате электрохимической обработки образуется пористая структура с минимальными размерами до 100 нм. Далее на пористой алюминиевой поверхности формировали слой анодного оксида алюминия при помощи электрохимического анодирования в 1 % водном растворе лимонной кислоты. Верхняя обкладка конденсаторной структуры формировалась магнетронным осаждением никеля через теневую маску. Измерения емкости показали, что использование в качестве нижней обкладки конденсатора пористого алюминия позволяет повысить удельную емкость конденсаторов более чем на порядок по сравнению с аналогами, у которых в качестве нижней обкладки используется планарная алюминиевая пленка.

Таким образом, наноструктурирование алюминиевой поверхности в процессе изготовления конденсаторных структур позволяет решить задачу увеличения удельной емкости, что важно для формирования RFID микросхем, используемых при идентификации товаров, а также в бесконтактных платежных системах.

## ОПТИЧЕСКИЙ ИНТЕРПОЗЕР НА ОСНОВЕ МИКРОКАНАЛЬНОГО КРЕМНИЕВОГО КРИСТАЛЛА ДЛЯ ОПТИЧЕСКИХ МЕЖСОЕДИНЕНИЙ МЕЖДУ КРЕМНИЕВЫМИ МИКРОСХЕМАМИ

Ле Динь Ви, А.Ю. Клюцкий, А.В. Долбик, А.А. Лешок, С.К. Лазарук

Оптические межсоединения по сравнению с электрическими позволяют значительно повысить быстродействие функционирования устройств обработки и передачи информации. Помимо высокой производительности в этом случае особо следует отметить надежную защиту передаваемой информации за счет локализации информационного потока внутри системы источник света – волновод – фотоприемник. Для кремниевых микросхем главные сложности связаны с преобразованием электрического сигнала в оптический. Лавинные светодиоды на основе наноструктурированного кремния, встроенного в матрицу анодного оксида алюминия, позволяют решить данную проблему.

Авторами разработаны конструкция и технология изготовления лавинных светодиодов, использующих наноструктурированный кремний, встроенный в матрицу оксида алюминия в качестве активного материала, обеспечивающего излучение света видимого диапазона с эффективностью более 0,1 %. Между источником света и фотодетектором расположен микроканальный кремниевый кристалл, выполняющий функцию оптического интерпозера. Таким образом, световой сигнал, генерируемый лавинным светодиодом первого чипа, проходит через микроканальные отверстия оптического интерпозера и регистрируется фотодетектором, расположенным на втором чипе. Коэффициент передачи по току такой оптоэлектронной

системы составлял 0,1–0,3 %. Максимальные значения данного параметра были получены для импульсного режима функционирования лавинных светодиодов.

Разработанная система оптических межсоединений демонстрирует новые возможности для развития кремниевой фотоники, способной значительно увеличить скорость обработки информации устройствами интегральной электроники.

## СВЕТОИЗЛУЧАЮЩИЕ ДИОДЫ НА ОСНОВЕ НАНОКРИСТАЛЛИЧЕСКОГО КРЕМНИЯ ДЛЯ ПЕРСПЕКТИВНЫХ КВАНТОВЫХ УСТРОЙСТВ

А.А. Лешок, А.В. Долбик, Ле Динь Ви, С.К. Лазарук

Создание эффективных светоизлучающих устройств на основе кремния является одной из приоритетных задач текущего времени, решение которой позволит преодолеть многие существующие ограничения интегральной электроники. Помимо этого создание кремниевых светоизлучающих диодов с заданными эксплуатационными характеристиками открывает новые перспективы и для других областей электроники и оптики. В частности, разработка светоизлучающих диодов, функционирующих при определенных пространственно-временных условиях в режиме однофотонного излучения, обеспечит значительный прогресс в развитии систем квантовой криптографии и квантовых вычислений.

Авторами разработаны конструкция и технология изготовления оптоэлектронного элемента на основе лавинных светодиодов, использующих нанокристаллический кремний, встроенный в матрицу оксида алюминия в качестве активного материала. Конструктивно разработанный элемент представляет собой оптопару, состоящую из двух контактов Шоттки, а также из слоя анодного оксида алюминия, разделяющего алюминиевые электроды. Если один из диодов имеет обратное смещение, превышающее напряжение лавинного пробоя, он излучает свет видимого диапазона. При этом второй диод при обратном смещении менее напряжения лавинного пробоя обладает светочувствительными свойствами, т. е. функционирует как фотодетектор и способен принимать световой сигнал первого диода. В нашем случае при подаче обратного смещения на светодиод величиной 6 В и выше их излучение регистрировалось интегрированными фотодетекторами. Уменьшая линейные размеры светоизлучающих структур до единиц микрометров и варьируя диапазон их рабочих напряжений регистрировались предельно низкие оптические сигналы порядка мкВт/см$^2$, особенно на специфических элементах геометрии электродов - угловых сегментах разной формы. Столь малые интенсивности светоизлучения позволяет рассматривать разработанную конструкцию как перспективную для ее использования в системах генерации индивидуальных фотонов.

Разработанный оптоэлектронный элемента способен функционировать в гигаргерцевом диапазоне частот при минимальных размерах рабочей области светодиодов. Данная разработка открывает новые возможности для развития как кремниевой фотоники, так и квантовых систем.

## КОНСТРУКТИВНЫЙ МЕТОД ФОРМИРОВАНИЯ Г-ОРБИТ ВЕКТОРОВ-ОШИБОК В ЛИНЕЙНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДАХ

В.А. Липницкий, Е.В. Реентович

Применение автоморфизмов помехоустойчивых кодов предполагает, как правило, разбиение пространства векторов-ошибок на орбиты относительно групп этих автоморфизмов. Декодеры на основе автоморфизмов кодов осуществляют поиск ошибок сначала по орбитам, а в дальнейшем, по строго алгоритмизованным шагам внутри выбранной орбиты. Подобный подход четко реализован для семейства БЧХ-кодов на рубеже XX–XXI веков теорией норм синдромов (ТНС) [1].

В главе 2 монографии [1] подробно исследованы свойства и методики формирования Г-орбит векторов-ошибок весом 2 и 3 в двоичных пространствах произвольной размерности $n$ относительно группы Г порядка $n$ циклических сдвигов координат векторов.

С ростом $n$ и веса селектируемых ошибок задача построения полного списка Г-орбит векторов-ошибок зачастую становится весьма трудоемкой – то не удается построить полный список образующих Г-орбит, то он становится слишком большим и весьма затруднительно

установить совпадающие Г-орбиты. Для кодов длиной $n$, выражаемой простым числом (тогда вес взаимно-прост с длиной кода и все Г-орбиты содержат по $n$ векторов; подобные коды часто привлекают теоретиков и представителей практики [2]) авторами разработан конструктивный метод формирования полного спектра Г-орбит векторов-ошибок любого веса. Метод отличается простой рекурсивной процедурой, однозначно завершается, не допускает повторений и «лишних орбит».

**Литература**

1. Липницкий В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. / В.А. Липницкий, В.К. Конопелько. – Мн.: Издательский центр БГУ, 2007. – 240 с.

2. Липницкий В.А., Реентович Е.В. Квадратично-вычетные коды как коды Хемминга и обобщенные коды Боуза-Чоудхури-Хоквингема. // Тезисы докладов XVI Белорусско-российская научно-техническая конференция «Технические средства защиты информации», Минск, 5 июня 2018 г. – 2018. – С. 80–81.

## АСПЕКТЫ ИЗУЧЕНИЯ МЕТОДОВ СЕТЕВОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В РАМКАХ СПЕЦИАЛЬНОСТИ «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ»

А.В. Ломако

Проблемы защиты информации остро стоят в автоматизированных информационных системах (АИС), работающих на базе компьютерных сетей. Особую остроту эти проблемы приобретают в случае использования при работе АИС глобальной сети Интернет. Именно этим обусловлена актуальность изучения методов сетевой безопасности при подготовке специалистов в рамках специальности 1-53 01 02 «Автоматизированные системы обработки информации», особенно для ее специализации «Интернет-технологии». Причина состоит в том, что сетевая безопасность, как правило, обеспечивает информационную безопасность АИС.

В ходе обучения, студенты должны четко усвоить, что обеспечение сетевой безопасности является комплексной задачей, решение которой требует системного подхода, предполагающего анализ и структурирование возможных нарушений информационной безопасности с последующей разработкой и внедрением необходимых средств обеспечения защиты от таких нарушений. Для достижения этой цели следует в процессе обучения раскрыть основные аспекты построения систем защиты информации в сетях. В докладе приводится перечень и дается краткая характеристика указанных аспектов. Приведем некоторые из них.

Имеются множество международных стандартов по информационной безопасности, а также регламентирующие документы и стандарты процесса создания систем защиты информации. Одной из наиболее удачных технологий создания современных систем безопасности считается разработанная компанией Cisco Systems стратегия безопасности, получившая название SAFE**,** которая включает пять этапов. Важное значение имеет политика информационной безопасности, представляющая собой изложение целей, задач и решений, которые должны быть достигнуты при внедрении системы защиты информации. В политике информационной безопасности должны быть отражены шесть ключевых аспектов. Защита сети включает в себя три уровня: физическая защита; контроль действий пользователей; программная защита.

## ПРОЕКТИРОВАНИЕ ЭЛЕМЕНТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ С ПОНИЖЕННЫМ ЭНЕРГОПОТРЕБЛЕНИЕМ

С.О. Ломако, И.А. Мурашко

Снижение мощности, потребляемой цифровыми схемами, является актуальной научно-технической проблемой, которая привлекает внимание все большего и большего числа ученых и инженеров [1]. В ходе работы по изучению и анализу энергопотребления различными логическими элементами было выявлено, что реализация какой-либо логической функции

на элементах «исключающее ИЛИ» дает больший эффект по потреблению энергии, нежели используя остальные элементы. На основании этого был написан программный продукт на языке JavaScript, который способен рассчитать минимальную переключательную активность, полученную путем наращивания уровней с двухвходовыми элементами «исключающего ИЛИ». Ее реализацию при пяти входах можно записать в виде скобочной функции вида $((x_1 \oplus x_2) \oplus x_3) \oplus (x_4 \oplus x_5)$ [2]. При увеличении количества входов на сумматор соответственно добавляются слагаемые в выражение.

**Литература**

1. Anuj Divya K. A Literature Review on Design Strategies and Methodologies of Low Power VLSI Circuits // IOSR Journal of VLSI and Signal Processing. – 2014.

2. Мурашко И.А. Анализ энергопотребления многовходового сумматора по модулю два // Информатика. – 2006. – № 1 (9). – С. 97–103

## ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНОГО МЕТОДА ДЛЯ АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

А.М. Мажейко, Е.С. Белоусова

Авторизация пользователей компьютерных систем в классическом варианте представляет собой однократный этап аутентификации. Это значит, что после получения пользователем прав доступа не производится каких-либо промежуточных проверок и сессия считается легитимной до момента ее завершения. В этом случае кража либо утеря ключа доступа может предоставить злоумышленнику возможность пользования ресурсами без ограничений. При предварительной разведке такая ситуация способствует получению более широких прав доступа, вплоть до уровня администратора либо владельца системы. Таким образом ввод дополнительных элементов управления доступом является актуальным. В настоящее время попытки ввода систем защиты информации с использованием поведенческого анализа предприняты на базе антивирусных продуктов и межсетевых экранов следующего поколения (Next-Generation Firewall). Применение подхода подобного типа для аутентификации пользователей представляется перспективным направлением. Анализ поведения пользователя предоставляет возможность более быстрой реакции на инциденты незаконного проникновения, сканирования структуры сети передачи данных и действий, не связанных с выполнением непосредственных рабочих задач. Математическим инструментом данного подхода может служить вероятностный метод [1]. Определение вероятностей подключения от имени определенного пользователя к различным ресурсам и элементам сети передачи данных создает дополнительный контроль в управлении доступом. К примеру, подключение бухгалтера к сервису начисления заработной платы происходит по определенному расписанию ежемесячно. В этом случае создаются временные метки, содержащие различные величины вероятности подключения бухгалтера к данному сервису. Сопоставление активности данного пользователя и ранее определенной вероятности подключения предоставляет возможность принятия решения об аномальном поведении, и соответственно, принятии мер о блокировке доступа.

Таким образом, проведение оценки сетевой активности пользователя персонального компьютера позволит применять автоматические меры ограничения либо полной блокировки доступа при аномальной активности до момента анализа ситуации администратором информационной безопасности.

**Литература**

1. Вероятностные методы для выявления аномальной активности в компьютерных сетях / А.А. Шевченко [и др.] // Нейрокомпьютеры и их применение: XVII Всероссийская научная конференция, Москва, 19 марта 2019 г. – 2019. – С. 285–287.

## ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРИНЦИПОВ ПРИМЕНЕНИЯ РЕЗОНАНСНО-РЕФЛЕКТОМЕТРИЧЕСКОЙ ЛОКАЦИИ ДЛЯ ПОИСКА СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

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

Анализ данных по информационной безопасности показывает, что, в мире растет доля утечек информации по в государственном секторе [1]. Более 30 % от общего объема утечек составляет информация, относящееся к государственной тайне. Утечка такой информации, по определению, может нанести ущерб, как экономике, так и суверенитету страны. Как правило, на объектах, где циркулирует секретная информация, (далее – объекты информатизации) отсутствуют незащищенные сетевые устройства и устройства беспроводного доступа. Такие меры практически исключает атаки злоумышленников по сети. Поэтому для съема информации, как правило, используют специальные технические средства. Организационные меры, принимаемые на объектах информатизации уменьшают возможности злоумышленника по монтажу и изъятию специального технического средства, поэтому большое распространите получили устройства, использующие для передачи данных радиоканал.

Как известно в конструкции любого СТС с радиоканалом есть антенный тракт и поэтому перспективным методом для обнаружения является использования принципов резонансно-рефлектометрической локации. Передатчик излучает зондирующие импульсы разной частоты, параллельно с передатчиком перестраивается приемник. Решающее устройство определяет есть ли закладное устройство путем измерения относительного уровня принятого отраженного сигнала. Резонансно-рефлектометрический локатор способен находить подслушивающие устройства в выключенном состоянии, имеет небольшие габариты и, как следствие, высокую мобильность. Важным преимуществом такого прибора, по сравнению с нелинейным локатором и системами радиомониторинга, является высокая степень помехозащищенности. [2]

**Литература**

1. Исследование утечек информации ограниченного доступа в госсекторе. М.: Мир, 2018.

2. Ворошень А.В., Ворошень В.И. Функциональные особенности резонансно-рефлектометрического локатора для обнаружения радиозакладных устройств // Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 4–5 июня 2015 г. – С. 13.

## ВВЕДЕНИЕ В ТЕОРИЮ ЦИФРОВОЙ МОДЕЛИ ЯДЕР ИНТЕГРАЛЬНОГО ПРЕОБРАЗОВАНИЯ МЕЛЛИНА

А.М. Макаров, Е.А. Писаренко

Подход к обнаружению сложных фазоманипулированных сигналов с относительной фазовой манипуляцией, предложенный авторами в работе [1], получил математическое доказательство своей работоспособности в условиях априорной неопределенности корреляционной функции гауссовской помехи. Это позволило разработать для технических средств защиты информации алгоритм обнаружения сигналов систем связи WI-FI, использующих фазоманипулированные сигналы. При этом встала задача цифровой реализации базисных ядер интегрального преобразования Меллина [2]. В настоящее время эта задача не имеет удовлетворительного решения, поэтому требуются дополнительные теоретические исследования способов ее решения для цифровой обработки сигналов.

Целью работы является развитие теории нового класса функций, получающихся при использовании преобразования Меллина как основного блока в общей структуре систем обработки сигналов на фоне помех.

В работе доказаны две теоремы, результаты которых приводят к новому классу периодических функций, так называемых параметрически-периодических тригонометрически-логарифмических функций. Анализ методов их цифровой реализации выявил три подхода, которые подробно рассматриваются в работе. Для их реализации разработаны цифровые

алгоритмы и требования к шагу дискретизации и точности представления, а также приведен сравнительный анализ с быстрым преобразованием Фурье.

**Литература**

1. Макаров А.М., Писаренко Е.А. Исследование комплексных спектров сложных сигналов в базисе преобразования Меллина // Технические средства защиты информации : тез. докл. 17 Белорусско-российской научн.-техн. конф., Минск, 11 июня 2019 г. – С. 46–47.

2. Макаров А.М., Постовалов С.С. Математическая модель тригонометрически-логарифмических базисных функций преобразования Меллина и их цифровая реализация // Известия ЮФУ. Технические науки. – 2018. – № 3 (197). – С. 22–33.

## ОЦЕНКА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В.А. Маласай

Средства вычислительной техники (СВТ), обрабатывающие защищаемую информацию, можно рассматривать как совокупность элементарных электрических и магнитных излучателей. Канал утечки информации за счет побочных электромагнитных излучений (ПЭМИ) является далеко не новым, однако оценка защищенности информации на объекте вычислительной техники (ОВТ) по каналу ПЭМИ является обязательной частью при аттестации соответствующего объекта информатизации. Целью работы является исследование утечек информации за счет ПЭМИ цифровых и аналоговых интерфейсов монитора с помощью RTL-SDR приемника. СВТ, обрабатывающие защищаемую информацию, рассматриваются как совокупность элементарных электрических и магнитных излучателей. При обработке, хранении и передаче информации СВТ возникает изменение электрических токов, проходящих по токопроводящим элементам и образование разности потенциалов между различными точками цепи, которые в свою очередь порождают электрические и магнитные поля. К безопасным информативным излучениям ПК можно отнести из лучения цепей, формирующих шину данных системной шины и внутреннюю шину данных микропроцессора, а также излучения других цепей, служащих для передач информации, представленной в виде многоразрядного параллельного кода. На персональной электронно-вычислительной машине (ПЭВМ), ведущей обработку защищаемой информации, т.е. являющейся основным техническим средством приема, обработки и передачи информации (ОТСС), не разрешается использование беспроводных устройств.

**Литература**

1. Алексеенко В.Р., Петраков А.В., Лагутин В.С. Техническая защита информации / Алексеенко В.И., Петраков А.В., Лагутин В.С. // Вестник связи – 1994. – № 12. – С. 27–34.

2. Лысов А.В., Остапенко А.Н. Промышленные шпионаж в России: методы и средства. – СПб.: Лаборатория ППШ, 1994. – 71 с.

## АНАЛИЗ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ ОБЩЕГО ДОСТУПА С ПАРОЛЬНОЙ ЗАЩИТОЙ

В.В. Маликов, А.В. Макатерчик

Использование хеш-функций находит широкое применение в различных областях информационной безопасности. Однако, техническая осведомленность злоумышленников и их инструментарий постоянно растут и изменяются, поэтому в интересах защиты информации является жизненно необходимым знать реальное состояние дел с уровнем возможностей используемых технологий защиты информации. В ходе исследования авторами выполнен анализ возможностей программных средств анализа и расшифровки паролей, функционирующих на основе методов анализа значений хэш-функций.

На первом этапе исследования были выбраны для исследования следующие программные средства: скрипт определения хэш-функции hash-identifier, списки паролей RockYou, программа расшифровывания Hashcat. Проверены возможности проведения атаки прямым перебором и расшифровка по словарю. Исследование выполнялось по отдельности для каждого контрольного слова и с использованием различных хэш-функций.

Выявленные ограничения возможностей программных средств: атака прямым перебором для сложных паролей практически невозможен; обязательным условием расшифровки пароля по значению хэш-функции, является нахождение данного пароля в словаре либо как целое слово, либо как часть другого слова; поддерживается только латиница.

Результаты исследования позволяют утверждать, что реальные возможности существующих программных средств по расшифровке паролей на основе анализа значений хэш-функций достаточно ограничены. При этом стоит учитывать, что идентификация хэш-функции выполняется быстро и достоверно, что значительно повышает эффективность расшифровки паролей, но способ на скорость и качество расшифровки не влияет.

## ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЦИОИНЖЕНЕРНЫХ АТАК НА ПОЛЬЗОВАТЕЛЕЙ СЕТЕВЫХ РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, А.В. Макатерчик

В настоящее время в мире и Республике Беларусь значительно возрастает число инцидентов, связанных с несанкционированных доступом к сетевым ресурсам кредитно-финансовых организаций (КФО). В ходе исследования авторами описана базовая структура проведения социоинженерных (социотехнических) атак, которая включает детализацию каждого из 5-ти ее этапов.

Предложен подход к оценке вероятности успеха многоходовой социоинженерной (социотехнической) атаки, а также описана модель базового профиля уязвимости цели (объекта атаки). Для оценки применимости существующих методик/алгоритмов социоинженерных (социотехнических) атак, авторами статьи было проведено практическое тестовое исследование (fair use / fair dealing). В качестве объектов атаки были выбраны два пользователя сервисов двух разных КФО (согласие пользователей сервисов КФО на исследование получено и проведен дополнительный инструктаж, Ф.И.О. пользователей – заменены порядковыми номерами, фишинг эмулировал адресные данные сервисов КФО, срок возможного проведения цикла атаки – до 10-ти дней). Оценка полноты информации по базовому профилю уязвимости цели атаки осуществлялась на основе метода экспертных оценок.

Предложены рекомендации для противодействия ряду способов, используемых для проведения социоинженерных (социотехнических) атак.

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ МИНИСТЕРСТВА ПРИРОДНЫХ РЕСУРСОВ И ОХРАНЫ ОКРУЖАЮЩЕЙ СРЕДЫ РЕСПУБЛИКИ БЕЛАРУСЬ

Д.А. Мельниченко

Информационная безопасность организации: частной, коммерческой или государственной, есть гарантия ее жизнедеятельности и конкурентоспособности на современном рынке. В особой степени это касается республиканских органов государственного управления и иных государственных организаций, в работе которых может использоваться информация, представляющая не только торговый, но и стратегический интерес.

Для организации взаимодействия в системе Министерства природных ресурсов и охраны окружающей среды Республики Беларусь (Минприроды) используется широкий ряд специализированных компьютерных информационных систем, систем управления базами данных, баз данных: интегрированная автоматизированная система контрольной (надзорной) деятельности в Республике Беларусь, система межведомственного документооборота

государственных органов Республики Беларусь, система электронного документооборота, комплекс программ «Экология», система электронного визирования документов с облисполкомом «Визадок» и др.

Министерство природных ресурсов и охраны окружающей среды Республики Беларусь при обеспечении информационной безопасности как среди структурных подразделений, так и между комитетами природных ресурсов и охраны окружающей среды и подчиненными организациями использует комплексный подход, который включает в себя организационные, организационно-технические и технические мероприятия, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

При этом особое внимание уделяется обучению специалистов Минприроды в области информационной безопасности, повышению их профессиональной компетенции в данной сфере. С этой целью Республиканским центром государственной экологической экспертизы и повышения квалификации Минприроды разработана и внедрена образовательная программа обучающего курса «Система информационной безопасности и средства ее защиты», при изучении которой специалисты имеют возможность приобрести практические навыки и умения для грамотной организации политики безопасности, способной реализовать ее функционирование не только в повседневных условиях, но и в критических ситуациях.

## ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ТАБЛИЦЫ ДЕКОДИРОВАНИЯ

А.И. Митюхин, В.А. Томин

Рассматривается решение задачи зашиты информации на основе кодирования цифровой информации с использованием кодов с расширением спектра. Известно, при расширении спектра сигнала с равномерным распределением энергии, уменьшается его спектральная плотность мощности и тем самым обеспечивается энергетическая скрытность передачи закодированной информации [1]. Наряду с открытым широкополосным кодированием предлагается осуществлять дополнительное кодирование, основанное на алгебраических свойствах и особенностях низкоскоростных кодов. Для этого можно применить алгебраическую операцию разложения группы на смежные классы по подгруппе. В теории кодирования эта операция определяет построение таблицы декодирования кода с расширением спектра. Информации ставится в соответствие номер смежного класса. Далее закодированные данные передаются по двоично-симметричному каналу (ДСК) с шумом. В качестве ключей используются случайно выбираемые шумовые векторы, отражаемые операцией разложения группы на смежные классы подгруппы. Порядок группы определяет значность кода. Для повышения надежности информационной системы предлагается шумовые векторы дополнительно кодировать с помощью апериодической псевдослучайной последовательности, например, М-последовательности. Длительность последовательности соизмерима с временем сеанса связи. Кроме того, структура полиномов над полем Галуа, генерирующая псевдослучайную последовательность, может меняться через заранее выбранный промежуток времени. Уполномоченный пользователь системы использует декодер, работающий по синдромному алгоритму. При этом используется теорема о связи формы синдрома и номера соответствующего смежного класса [2]. В случае обнаружения активной работы системы, несанкционированный доступ к информации усложняется из-за необходимости проведения значительных вычислительных операций на основе поэлементного сравнения входного процесса ДСК с векторами смежных классов. Стойкость рассматриваемого алгоритма зависит от параметров открытого кода (значности, размерности и минимального расстояния), а также количества вариантов разложения исходного открытого кода на смежные классы по параметру, характеризующему избыточность кода. Представлены оценки сложности несанкционированного декодирования с использование энтропийного подхода.

**Литература**

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

2. Митюхин А. И. Прикладная теория информации. – Минск: БГУИР, 2018.

## МЕЖСАЙТОВЫЕ АТАКИ С ВНЕДРЕНИЕМ СЦЕНАРИЯ

А.С. Михайлов, А.П. Турлай, С.Б. Саломатин

Рассматриваются следующие алгоритмы возможных атак в рамках схемы работы межсайтовой атаки с внедрением сценария.

Хранимые XSS (постоянные) – один из самых опасных типов уязвимостей, так как позволяет злоумышленнику получить доступ к серверу и уже с него управлять вредоносным кодом (удалять, модифицировать).

Отраженные XSS (непостоянные): в этом случае вредоносная строчка выступает в роли запроса жертвы к зараженному веб-сайту.

DOM-модели: в этом варианте возможно использование как хранимых XSS, так и отраженных.

*Правила безопасности*. Защита применяется последовательно, без исключений и упрощений, желательно с самого начала разработки веб-приложения.

Рассматриваются следующие варианты: проверка входных данных, экранирование данных на выходе.

*Заключение.* Разработанные алгоритмы, реализованные в виде программ, позволяют повысить эффективность защиты веб-приложения от атак. Они значительно упрощают процесс тестирования веб-ресурса разработчиком, благодаря функционалу формирования отчета с рекомендациями по устранению найденных уязвимостей.

**Литература**

1. Элхади А.М. Полное пособие по межсайтовому скриптингу.

2. Элхади А.М. Уязвимости веб-приложений: пора анализировать исходный код.

3. Джатана Н., Агравал А., Собти.К. Пост эксплуатация XSS: продвинутые методы и способы защиты.

## ОБ ОПЫТЕ ПРОВЕДЕНИЯ СЕМИНАРОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ПОДГОТОВКИ ВОЕННЫХ СПЕЦИАЛИСТОВ

Л.В. Михайловская, Е.В. Валаханович

Одним из требований к профессиональной подготовке военных специалистов в век цифровых технологий является уверенное владение методами защиты информации. Разумеется, для обеспечения качественной подготовки курсантов в данной области самим преподавателям необходимо не только обладать соответствующими знаниями и навыками в области защиты информации, но и постоянно совершенствовать указанные компетенции.

Исходя из этого, одним из важных этапов подготовки специалистов в области защиты информации на кафедре высшей математики УО «Военная академия Республики Беларусь» является систематическое проведение научных семинаров по защите информации. Вышеназванные семинары проводятся ежемесячно для профессорско-преподавательского состава, адъюнктов, магистрантов и аспирантов кафедры. Данные семинары являются важной частью подготовки ППС кафедры к работе с учетом особенностей занятий по защите информации с курсантами факультетов связи и АСУ и военной разведки УО «Военная академия Республики Беларусь».

Целями данных семинаров являются: расширение представлений о существующих компьютерных уязвимостях, методах защиты информации и ознакомление ППС

с особенностями проводимых занятий (так как большинство занятий по защите информации проводится в виде лабораторных работ). Авторы считают, что современные специалисты в области защиты информации обязательно должны иметь знания об особенностях многомерного векторного представления информации GloVe, о классификации компьютерных уязвимостей с ее помощью, понимать особенности работы и корректирующие возможности, недостатки и преимущества обобщенных БЧХ-кодов, владеть навыками работы с криптоситемами RSA, Рабина, Эль Гамаля и др., что, в свою очередь, обеспечивает качественную подготовку курсантов в изучении стандарта шифрования AES.

Таким образом, проведение ежемесячных семинаров на кафедре высшей математики УО «Военная академия Республики Беларусь» способствует действенному улучшению работы ППС по подготовке будущих военных специалистов в области защиты информации.

## МОДЕЛИРОВАНИЕ ВЫХОДНЫХ ХАРАКТЕРИСТИК ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ С ИСПОЛЬЗОВАНИЕМ ГРАФЕНА И ГЕКСОГОНАЛЬНОГО НИТРИДА БОРА

В.В. Муравьев, В.Н. Мищенко

Рассмотрены вопросы моделирования выходных характеристик полупроводниковых приборов с использованием материалов графена и гексогонального нитрида бора (BN). Высокое значение подвижности носителей заряда, высокая теплопроводность и ряд других его положительных свойств делают графен перспективным материалом для использования в полупроводниковых приборах и структурах. Вместе с тем, для реализации уникальных свойств и характеристик графена, учитывая двухмерный характер этого материала, весьма важен выбор сопутствующих полупроводниковых и диэлектрических материалов, обеспечивающих формирование полупроводникового прибора, пригодного для практического применения. В этом плане большое внимание привлекает внимание использование пленочного BN, имеющего гексогональную кристаллическую структуру, близкую к структуре графена. Ряд положительных свойств гексогонального BN позволяет прогнозировать получение высоких выходных характеристик полупроводниковых приборов, использующих графен в сочетании с этим материалом. С использования метода статистического моделирования – метода Монте Карло разработана программа для моделирования выходных характеристик полупроводниковых приборов, в которых формируется многослойная структура, содержащая слои графена и гексогонального BN. Путем моделирования получены и исследованы основные выходные характеристики полевых транзисторов, построенных на основе многослойной полупроводниковой структуры, содержащей слой графена, размещенного на подложке из гексогонального BN. Использование полевых транзисторов и других приборов, использующих графен и гексогональный BN, найдут широкое применение в системах приема, усиления и обработки сигналов в диапазонах СВЧ и КВЧ.

## АНАЛИЗ УЯЗВИМОСТЕЙ ОПЕРАЦИОННЫХ СИСТЕМ НА БАЗЕ ЯДРА LINUX

Э.К. Мурадов, С.Ю. Павлович

Согласно данным Лаборатории Информационных технологий Национального Института стандартов и технологий США, к маю 2020 года было обнаружено 4017 уязвимостей в ядре Linux [1]. Эксплуатация более половины из обнаруженных уязвимостей приводит к отказу в обслуживании (нарушению доступности операционной системы на базе ядра Linux), более 15 % – к несанкционированному доступу к данным, более 10 % – к повышению привилегий пользователей системы. Причинами большого количества обнаруженных уязвимостей ядра Linux являются открытость его исходного кода и широкое применение. При этом следует заметить, что эти причины обуславливают возможность превентивного обнаружения уязвимостей и оперативного их устранения.

Уязвимости наиболее высокой степени информационного риска обусловлены следующими причинами.

1. Значение TCP_SKB_CB(skb)→tcp_gso_segs может быть переполнено целым числом в ядре Linux при обработке выборочных подтверждений TCP (SACK). Злоумышленник может использовать это удаленно для того, чтобы реализовать угрозу типа «отказ в обслуживании» [2].

2. Функция mq_notify в ядре Linux не устанавливает значение указателя сокета на NULL при входе в режим повторов. Во время закрытия сокета Netlink пользовательским пространством, злоумышленники могут организовать угрозу типа «отказ в обслуживании» [3]. Netlink – интерфейс ядра Linux для установки связи между пользовательскими процессами и процессами самого ядра.

3. В ядре Linux hns_roce_alloc_ucontext не инициализирует соответствующую структуру данных, что может позволить злоумышленникам реализовать несанкционированный доступ к информации из памяти стека ядра [4].

4. Реализация coredump в ядре Linux не использует блокировки или другие механизмы для предотвращения изменений макета vma или флагов vma во время работы, что позволяет локальным пользователям реализовать несанкционированный доступ к информации [5].

5. Функция vmacache_flush_all в mm/vmacache.c неправильно обрабатывает переполнения порядкового номера. Злоумышленник может инициировать use-after-free с помощью определенных операций создания потоков, сопоставления, отмены отображения, аннулирования [6].

6. Состояние гонки в kernel/events/core.c в ядре Linux позволяет локальным пользователям получать привилегии через специально созданное приложение, которое делает одновременные системные вызовы perf_event_open для перемещения группы программного обеспечения в аппаратный контекст [7].

Для снижения вероятности реализации угроз, связанных с эксплуатацией рассмотренных и ряда других уязвимостей, необходимо выполнять настройки безопасности используемой операционной системы на базе ядра Linux, уделяя при этом особое внимание настройке подключаемых модулей аутентификации (PAM-модулей), либо применять такую систему в защищенном исполнении (например, операционную систему специального назначения Astra Linux SE).

**Литература**

1. National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results _type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Alinux&cpe_product=cpe%3A%2F%3A%3Alinux_kernel. – Дата доступа: 10.05.2020.

2. CVE–2019–11477 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–11477. – Дата доступа: 10.05.2020.

3. CVE–2017–11176 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2017–11176. – Дата доступа: 10.05.2020.

4. CVE–2019–16921 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–16921. – Дата доступа: 10.05.2020.

5. CVE–2019–11599 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–11599. – Дата доступа: 10.05.2020.

6. CVE–2018–17182 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2018–17182. – Дата доступа: 10.05.2020.

7. CVE–2017–6001 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2017–6001. – Дата доступа: 10.05.2020.

## ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В КОРПОРАТИВНЫХ СЕТЯХ

Е.А. Мурашко, С.Н. Петров

Современные способы обнаружения и предотвращения сетевых атак с использованием программно-аппаратных средств защиты информации (СЗИ) широко распространены в сфере

информационных технологий. При этом процессы и методы испытаний зачастую засекречены. Данный факт объясняется тем, что в ситуации, когда описание процесса испытаний продукта находится в общем доступе, потенциальный злоумышленник может видеть места, через которые легче всего если не полностью перехватить информацию, то нанести ей вред. Обнаружение сетевых атак с использованием программно-аппаратных СЗИ способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Другими словами, заблаговременное обнаружение уязвимостей позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды. Для успешного применения программно-аппаратного СЗИ необходимо произвести его тестирование на соответствующем оборудовании и средствах соединения через каналы связи, соответствующих определенным требованиям и с использованием специализированного программного обеспечения. Результаты тестирования помогают увидеть, какими функциональными возможностями может обладать устройство, либо программный продукт, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именное решение правильнее и выгоднее всего использовать в организации сетевой инфраструктуры компании либо предприятия. Также определенные средства защиты информации возможно протестировать только лишь на определенном типе тестового стенда, содержащим в себе специфичесике элементы сетевой инфраструктуры.

**Литература**

1. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. – 2016. – Вып. 45. – С. 207–244.
2. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. – СПб: Питер, 2017. – 256 с.

## ПРОБЛЕМЫ БЕЗОПАСНОСТИ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ МОНИТОРИНГА

Е.В. Новиков, Д.А. Мельниченко

Мониторинг состояния природных систем, в том числе и очагов поражения, возникающих в чрезвычайных ситуациях с выбросом токсичных веществ, наиболее эффективно может осуществляться с применением распределенных автоматизированных систем сбора данных. Особенно актуальным это оказывается в ситуациях, когда необходимо длительное (сутки и более) накопление данных, площади мониторинга составляют десятки квадратных километров, а динамика контролируемых параметров значительна.

В современных условиях рассматриваемые системы мониторинга имеют классическую мультиагентную структуру, причем в реальных условиях могут быть использованы разные типы первичных датчиков и различные интерфейсы передачи данных, которая практически всегда является беспроводной [1].

Обеспечение безопасности рассматриваемых сетей при этом представляет сложную задачу из-за наличия большого числа агентов, обеспечивающих сбор и передачу блоков данных, их удаленности и физической незащищенности, а также возможности внешнего вмешательства в собственно процесс передачи данных.

Несмотря на наличие в большинстве протоколов беспроводной передачи средств криптографической защиты данных и политик безопасности, это не гарантирует неуязвимость отдельных узлов и мультиагентных систем в целом [2].

В работе исследуются подходы к решению рассматриваемой задачи обеспечения должного уровня безопасности сети мониторинга с учетом как аспектов информационной защиты, так и физической защищенности агентов при условии сохранения эффективности сбора данных и энергоэффективности.

**Литература**

1. Мобильная система химического мониторинга атмосферы / С.Б. Прямухин [и др.] // Ракетно-космическая техника // Информационные системы и технологии. Научные труды. Т. 2. – 2012. – С. 387–396.

2. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – № 5 (87). – С. 149–154.

## ИМИТАЦИОННАЯ МОДЕЛЬ ПСЕВДОСЛУЧАЙНОГО ДОСТУПА КОНКУРИРУЮЩИХ УСТРОЙСТВ К РЕСУРСАМ БЕСПРОВОДНОЙ СЕТИ

Д.Н. Одинец, В.В. Носков

Для подготовки специалистов в области защиты информации разработана имитационная модель, которая предназначена для поиска минимума потери информации при передаче данных от большого количества устройств-клиентов к одному серверу, а также исследования устойчивости сети к различным видам хакерских атак. Модель относится к моделям беспроводных сетей с [1] с временным разделением каналов

Модель имеет ряд изменяемых входных параметров для оптимизации интервала времени, после которого все устройства-клиенты модели будут успешно выходить на связь с сервером.

К входным параметрам относятся:

а) $N$ – количество устройств;

б) $A$ – закон распределения выходов устройств на связь;

в) $T$ – интервал выхода на связь для каждого устройства;

г) Tstat – постоянное время ожидания перед повторной отправкой;

д) Trand – случайное время ожидания перед повторной отправкой;

е) $\tau$ – длительность передачи пакета;

ж) $k$ – количество повторных выходов на связь при повторной отправке.

Для первой итерации генерируются согласно выбранному случайному закону временные интервалы выходов на связь устройств-клиентов. Модель размещает интервалы выходов на временной области. По окончанию перовой итерации начинается поиск коллизий, то есть наложений временных каналов. Если коллизии присутствуют и количество повторных выходов на связь не равно 0, то данная итерация повторяется с учетом старых коллизий и новых временных интервалов повторных отправок. Данные действия осуществляются до тех пор, пока не обнулиться счетчик повторных отправок устройств-клиентов. По окончании каждой итерации модель проверяет количество коллизий и анализирует успешность выходов на связь всех устройств.

В результате исследований получены графические зависимости времени оптимизации модели от входных параметров.

**Литература**

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

## АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ ОТ ВНЕШНЕГО ВОЗДЕЙСТВИЯ

Д.Ю. Перцев, Д.В. Куприянова

Развитие алгоритмов машинного обучения и глубоких нейронных сетей привели к тому, что все больше компаний (например, Яндекс и Waymo) проводят исследования в области беспилотных автомобилей на дорогах общего пользования. Анализ текущего уровня систем

безопасности позволил выделить одну существенную проблему, приводящую к сбоям в системе управления, – связь электронных блоков управления с внешней средой через радиоинтерфейсы (например, для обновления программного обеспечения).

Как показывают некоторые исследования [1], применение CAN-шины для организации взаимодействия между всеми модулями системы является стандартом, однако технические ограничения протокола приводят к существенным трудностям в реализации системы безопасности, что делает данную сферу применения практически не защищенной. В то же время систематизация информации [2, 3]) показывает, что любое вмешательство в данные, получаемые от установленных сенсоров (например, внесение искажений в изображение) приводит к некорректной работе алгоритмов. При этом на восприятие человеком данные искажения не сказываются.

Анализ показал, что на момент написания тезисов, данное направление несмотря на определенный прогресс, является незащищенным и данную проблему требуется решать в комплексе: как на уровне протоколов взаимодействия, так и на уровне алгоритмов.

**Литература**

1. Automobile CAN Bus Network Security and Vulnerabilities [Electronic resource]. – Access mode: https://www.researchgate.net/publication/321124827_Security_Issues_in_Controller_Area_Networks_in_Automobiles. – Date of access: 20.04.2020.

2. Are Self-Driving Cars Secure? Evasion Attacks Against Deep Neural Networks for Steering Angle Prediction / Chernikova A. [et al.] // Proceedings of IEEE Security and Privacy Workshops (SPW). – 2019. – P.132-137.

3. Проблемы беспилотных автомобилей: нельзя научить компьютер водить машину так же, как это делают люди [Электронный ресурс]. – Режим доступа: https://www.iguides.ru/main/other/problemy_bespilotnykh_avtomobiley_nelzya_nauchit_kompyuter_vodit_mashinu_tak_zhe_kak_eto_delayut_lyu. – Дата доступа: 20.04.2020.

## ЗАЩИТА ОТ НЕПРЕДНАМЕРЕННОГО ПРЕКРАЩЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ИНТЕРНЕТЕ

А.А. Петрашевский

На странице РУП «Белтелеком» по адресу https://vk.com/topic-81246291_30909002?offset=7680 есть вопрос, адресованный предприятию 19.02.19 в 16:20 пользователем сети Интернет Александром Петрушем: «Почему очень плохо работает инет? Вчера все гуд было». Александра отправили в службу техподдержки по номеру 123. И на форумах таких жалоб много: роутеры зависают, интернет пропадает. Перезагрузка роутера (вкл/выкл) на некоторое время решает проблему, но причиняет большие неудобства пользователям: затраченное время, несвоевременность отправки и получения срочных писем по E-mail и т. д. Известны другие пути решения проблемы (прокладка витой пары, покупка дорогостоящего роутера), но они также имеют свои недостатки. В докладе для начала исследований по качественной защите от непреднамеренного прекращения доступа к интернету предлагается мониторинг эксплуатации оборудования для доступа в интернет (ОДДИ), установленного в квартире, частном доме, на даче, в небольшом офисе на 3–5 компьютеров. Пример результатов аналогичного высококачественного мониторинга и разработанного для этого методического обеспечения комплексов платежной системы Нацбанка Республики Беларусь [1] «…Проводимые мероприятия позволили в 5 раз снизить число отказов системы за второе полугодие 2001 года по сравнению первым полугодием того же года...». Работы по мониторингу ОДДИ начаты. Для сбора информации, получаемой в ходе мониторинга, разработаны формы в среде Microsoft Office Excel, которые позволят использовать для обработки информации простейшую компьютерную СУБД [1].

**Литература**

1. Ильин А.А. Технологическая политика Нацбанка Республики Беларусь в области оказания банковских услуг с применением современных информационных технологий // Веснік сувязі. – 2002. – № 4. – С. 33–42.
2. База данных для повышения уровня защиты информации в компьютерах// Материалы 14-й межд. НТК «Комплексная защита информации», Могилев 19–22 мая 2009 г. – 2009. – С. 76.

## ИСПОЛЬЗОВАНИЕ 3D СКАНИРОВАНИЯ КАК СПОСОБА СОХРАНЕНИЯ ИНФОРМАЦИИ С МЕСТА ПРОИСШЕСТВИЯ

Е.В. Плескач, В.С. Гладкая

Информационные технологии современного типа все шире включаются в деятельность по раскрытию и расследованию преступлений и происшествий, в частности дорожно-транспортных. Объективная фиксация и сохранение информации с места происшествия – первоочередная задача, разрешив которую станет возможным в последующем дать наиболее объективную оценку совершенному деянию. Уже на современном этапе развития 3D-сканеров можно сказать, что система лазерного 3D-сканирования места происшествия, которая позволяет с высочайшей точностью получать информацию с места происшествия в виде трехмерной модели, конкретнее и детальнее по сравнению с панорамным фотографированием. Полученная модель наиболее полно может воспроизводить обстановку и расположение объектов на месте происшествия. В результате сканирования, в отличие от проведения исключительно традиционной панорамной съемки, имеются координаты каждой отсканированной точки, позволяющие проводить все виды измерений без каких-либо искажений. С помощью многочисленного программного обеспечения можно измерить расстояния, углы, площади, объемы. Также применение 3D технологии позволяет хранить некоторые данные, которые раньше возможно было хранить лишь в виде слепков, в электронной базе. Например, возможно хранение отпечатка стопы человека. Стоит также отметить, что лазерное сканирование производится бесконтактным способом, что позволяет сделать фиксацию следов не только более легко и неразрушимо, но и помогает применять один и тот же след различными методами. Также, если рассматривать фиксацию следа обуви стоит отметить, что ранее для этого применялись гипсовые слепки, которые имели ряд недостатков, а именно: продолжительность изготовление слепка, невозможность его совершения из-за погодных условий или материала, в котором оставлен след, слепки занимали значительно много места, не всегда детализировались признаки при получении слепка, сложная транспортировка. Все эти недостатки исключены при получении 3D скана или снимка. Также стоит отметить, что во всех 3D сканерах применяется лазерная или ламповая подсветка, которая позволяет получить изображения высочайшего качества даже при слабой освещенности объекта [1, 2].

**Литература**

1. Майлис Н.П. Судебная трасология: учебник для студентов юридических вузов. – М.: Экзамен, Право и закон, 2013.
2. Горбулинская И.Н., Барбачакова Ю.Ю., Шавленко Е.В. О возможностях применения методов 3D-моделирования в ходе производства криминалистических экспертиз // Вестник экономической безопасности. – 2018. – № 1. – С. 42–45.

## МЕХАНИЗМ ТОКОПЕРЕНОСА В МЕТАСТАБИЛЬНОЙ ОБЛАСТИ КАНАЛА ПРОБОЯ НАНОРАЗМЕРНЫХ ОКСИДОВ МЕТАЛЛОВ

Д.А. Подрябинкин

Наноструктуры на основе оксидов металлов, перспективны для применения в качестве подзатворных диэлектриков в металл-окисел-полупроводник (МОП) транзисторах и энергонезависимой резистивной памяти с произвольной выборкой. У таких оксидов высокая диэлектрическая проницаемость в сочетании с большой энергией запрещенной зоны и термодинамически стабильная граница с кремнием.

Формовка таких оксидов в электрическом поле (обратимый пробой) приводит к образованию метастабильной области проводящего канала (нитевидных шнуров тока по границам зерен диэлектрика). В канале возникает высокая плотность ловушек с бистабильными состояниями, обусловливающая токоперенос в нем и возможность длительного хранения заряда (до $10^6$–$10^7$ с).

Такой канал может работать в 2х состояниях: состояние с высоким сопротивлением (HRS), когда ток протекает слабо и, при приложении электрического поля к каналу, состояние с низким сопротивлением (LRS), приводящее к существенному росту тока в нем.

Механизм токопереноса в метастабильной области канала пробоя состоит в захвате электронов на ловушечные центры по механизму Пула-Френкеля с участием многофононных взаимодействий (характеризующихся сильной электрон-фононной связью) и их освобождения в результате изменения энергии их ионизации, при переходе электронов из одного бистабильного состояния в другое.

Для бистабильных ловушечных состояний взаимодействие с горячими электронами приводит не только к переходу в возбужденное состояние, но и способствует снижению энергии их ионизации вплоть до их делокализации. Также, в данном случае, бистабильные ловушечные состояния могут переходить в верхнее энергетическое состояние, не напрямую взаимодействуя с горячими электронами, а за счет воздействия шума и периодической силы. Такие переходы существенно зависят от соотношения глубин потенциальных ям и определяются уровнем шума. Возникновению шума в данном случае способствуют флуктуации заряда при воздействии горячих электронов, связанные с их рассеянием на дефектах, что еще больше увеличивает ток в канале.

Таким образом, ловушечные центры в оксидах металлов способны изменять свою конфигурацию в зависимости от зарядового состояния, величины внешнего поля, наличии периодического воздействия и шума. Это позволяет создать на основе оксида металла элемент резистивной памяти, отличающимися конкурентными параметрами функционирования, такими как время переключения, низкое внешнее смещение (а значит и энергопотребление) и стабильность.

## ПОЧЕМУ КАЖДОМУ ВЕБ-САЙТУ НУЖЕН HTTPS?

Т.Д. Позняков

Прежде всего, что означает использование веб-сайтом HTTPS, а не просто старого HTTP? Это означает, что сайт защищен SSL (Secure Sockets Layer) или более поздним TLS (Transport Layer Security). Если вы не осведомлены в этой теме, это заявление может ничего для вас не значить, так что давайте разберемся. При посещении сайта и использовании URL-адреса https запрашивается защищенная версия сайта. Короче говоря, это означает, что ваш браузер надеется увидеть сертификат SSL/TLS на сервере веб-сайта. Этот сертификат должен быть предоставлен проверяемым центром сертификации (ЦС) и в основном позволяет вашему браузеру взаимодействовать с ним через зашифрованное соединение. В зависимости от сертификата, на нем также может быть написано: «Смотрите, этот сайт – это тот, кто он говорит, что он был проверен». После того как этот сертификат будет найден, между вашим браузером и веб-сайтом может быть установлено безопасное зашифрованное соединение. Теперь, если кто-то попытается вмешаться и перехватить вашу связь, данные будут

зашифрованы. Возможно, ваш интернет-провайдер сможет определить, на какой веб-сайт вы заходили, или сколько данных передается туда и обратно, но дальнейшего отслеживания не будет. Если сервер веб-сайта принимает HTTPS-запросы, но для этого веб-сайта нет действительного сертификата или истек срок действия сертификата сайта, у него недействительный ЦС или любая другая проблема, браузер уведомит вас и попытается предотвратить продолжение работы. Это связано с тем, что сайт говорит, что есть защищенное подключение доступно, но не предоставляет его, поэтому браузер пытается сделать так, чтобы вы знали об этом.

Многие веб-серверы либо имеют сертификат, либо маршрутизируют весь входящий трафик по протоколу HTTPS, заставляя использовать безопасную версию, либо, если у них нет сертификата, маршрутизируют весь трафик по протоколу HTTP, тем самым предотвращая попытки пользователей получить доступ к несуществующему безопасному соединению.

**Литература**

1. Stephen A. Thomas. HTTP Essentials: Protocols for Secure, Scaleable Web Sites.

2. Krishnamurthy B., Rexford J. Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement.

## ДИФФЕРЕНЦИРОВАННЫЙ ПОДХОД В ОБУЧЕНИИ СПЕЦИАЛИСТОВ В ТЕХНИЧЕСКИХ ВУЗАХ

З.Н. Примичева

В условиях социально-экономических изменений в обществе и активного внедрения новых информационных технологий потребность в специалистах технических вузов постоянно растет. Специалист в области защиты информации должен иметь фундаментальную математическую подготовку, поскольку на уровне использования вычислительных средств приходится проводить предварительный анализ решаемой задачи, опираясь на математические закономерности. Успешная реализация целей и задач образовательного процесса зависит не только от содержания образования, методов и форм обучения, применяемых педагогом, но и от умелой организации им образовательного процесса, создания комплекса дидактических условий с учетом особенностей обучающихся (их интересов, способностей, обученности, обучаемости, работоспособности).

В настоящее время в системе высшего образования приоритетной является лекционно-семинарская система обучения, которая отличается слабой направленностью на формирование у студентов умений решения конкретных практических задач. Повышение качества учебного процесса возможно лишь при наличии самостоятельной работы студентов, сопровождаемой контролем со стороны преподавателя. Применение новых нетрадиционных форм занятий, таких, как: тематические конференции, метод проектов, сетевые олимпиады, позволяет повысить самостоятельную творческую работу студентов. Учитывая, что итоговые показатели успеваемости студентов в сессии не всегда отражают реальную картину состояния процесса обучения, необходимо увеличивать роль текущего контроля знаний. При осуществлении математической подготовки студентов наблюдается неоднородность их состава, которая проявляется в различном уровне овладения предметными знаниями и умениями. Поэтому для проведения самостоятельных и контрольных работ рекомендуется разрабатывать комплекс дифференцированных заданий с учетом индивидуальных различий студентов.

Таким образом, внедрение дифференцированного обучения в рамках информатизации образования приводит к выработке у студентов внутренней мотивации, умения работать самостоятельно и, следовательно, к подготовке специалистов, обладающих системным и аналитическим мышлением, умением принимать оперативные и нестандартные решения.

## СИНТЕЗ АНСАМБЛЯ НАНОЧАСТИЦ Co НА ПОДЛОЖКАХ $SiO_2$/Si

Е.Н. Прокопюк, С.Л. Прищепа

Методом магнетронного распыления осаждались тонкие (толщина не более 10 нм) пленки Co на подложки $SiO_2$/Si. Далее пленки обрабатывались в плазме водорода и аммиака при давлении 12 мбар и температуре подложки 300 °C в течение 15 мин. В результате, из-за больших разностей поверхностной энергии Co и оксида кремния, проходило «сворачивание» тонкой пленки в наночастицы размером порядка 15 нм. Варьируя давление, температуру и время обработки, а также толщину исходной пленки, можно было варьировать в небольших пределах средний диаметр и плотность упаковки наночастиц. Методом дифракции электронов была определена кристаллическая структура полученных наночастиц. Установлено, что кобальт представлял смесь кубической гранецентрированной (кгц) и гексагональной плотноупакованной (гпу) решеток. С помощью сканирующей электронной микроскопии было установлено, что наночастицы обладали высокой плотностью упаковки на подложке, более $10^{10}$ см$^{-2}$. При этом было установлено, что с уменьшением среднего размера наночастиц растет плотность упаковки. Анализ гистограмм распределения средних размеров наночастиц показал, что средний размер составляет (20±5) нм. Методами рентгеновской фотоэлектронной спектроскопии был исследован фазовый состав полученных наночастиц. Он показал, что материал наночастиц – металлический кобальт, без наличия фазы кобальт – кислород. Это связано с тем, что весь процесс синтеза был проведен in situ, т. е. в одном вакуумном цикле, без разгерметизации камеры. Полученные образцы являются основой для последующего роста массива углеродных нанотрубок методом химического парофазного осаждения (ХПО), поскольку кобальт является хорошим катализатором. Особенностью данного метода является то, что при синтезе в реактор не требуется подача частиц катализатора, и каждая выращенная УНТ будет содержать только одну частиц ферроманетика.

## СИНТЕЗ ОРИЕНТИРОВАННЫХ МАССИВОВ УГЛЕРОДНЫХ НАНОТРУБОК С ОДНОЙ ФЕРРОМАГНИТНОЙ НАНОЧАСТИЦЕЙ НА ВЕРШИНЕ КАЖДОЙ УГЛЕРОДНОЙ НАНОТРУБКИ

Е.Н. Прокопюк, С.Л. Прищепа

На предварительно сформированных площадях однородно распределенных по площади подложки наночастиц Co проводился рост ориентированных массивов углеродных нанотрубок (УНТ). Рост УНТ проводился методом химического парофазного осаждения в смеси газов $C_2H_2$ и $H_2$ (20:80) при давлении $p$ = 15 мбар в течение 6 минут. Температура синтеза составляла 973 К. Малое время синтеза было выбрано для того, чтобы минимизировать дефектность УНТ. Качество УНТ проверялось методом Рамановской спектроскопии, которая показала, что спектр показывает расщепление D линии на 2 моды, 1306 см$^{-1}$ и 1334 см$^{-1}$. Наблюдалась интенсивная $G$ линия (1591 см$^{-1}$) с малой полушириной (13 см$^{-1}$), что указывает на то, что УНТ являются проводящими и высокого качества. Можно также было наблюдать пренебрежимо малое наличие аморфного углерода с модой на 1525 см$^{-1}$. Методом сканирующей электронной спектроскопии было установлено, что массив трубок был вертикально ориентирован, высота трубок составляла порядка 2 мкм, их средний диаметр составлял порядка 20 нм, т. е. был задан диаметром наночастиц кобальта. Методом просвечивающей электронной микроскопии было установлено, что наночастицы кобальта локализованы в верхней части углеродных нанотрубок. Их морфология представляла собой вытянутые вдоль оси УНТ наноцилиндры с аспектным отношением, близким к 5. Изменение морфологии наночастиц после роста УНТ по сравнению с исходными связано со сложными процессами роста нанотрубок при высоких температурах. Однако, тот факт, что наночастицы оставались внутри УНТ и сверху были закрыты слоями углеродной нанотрубки, предотвращает окисление кобальта и оставляет его ферромагнитным, что важно для применений в магнитоэлектронике.

## ВЛИЯНИЕ TYPESCRIPT НА БЕЗОПАСНОСТЬ JAVASCRIPT

А.П. Протасов, Ю.И. Алексеев, В.Я. Анисимов

TypeScript – язык программирования, созданный компанией Microsoft, являющийся библиотекой JavaScript. Он предназначен для помощи в разработке больших приложений путем добавления статической типизации, объектно-ориентированного программирования на основе классов и модульности в JavaScript. TypeScript использует транспортер, компилятор исходного кода, который берет исходный код TypeScript и преобразует его в код JavaScript.

Любой правильный код JavaScript является правильным кодом TypeScript, поэтому при замене разрешения файла с .js на .ts, файл станет действительным для Typescript. Цель TypeScript – сделать разработку больших приложений на JavaScript более управляемой, особенно в командах. TypeScript позволяет создавать четко определенные API для других разработчиков.

Однако, TypeScript не является надежным языком. TypeScript не гарантирует никакой проверки типов во время выполнения программы, что может привести к многочисленным ошибкам «Runtime Error», которые появляются из-за единственного типа данных «Any», с которыми компилятор допускает любую операцию.

Из-за присутствия ложной проверки типов, TypeScript можно найти альтернативу, основывающуюся в первую очередь на надежности, что утверждается в строго типизированных языках Dart, Kotlin, Rust. TypeScript предлагает ощутимые преимущества как вашим разработчикам, так и заинтересованным сторонам проекта. Написав немного больше кода, ваша команда сможет быстрее достичь большей производительности: меньше ошибок, более быстрые запуски, больше уверенности в качестве кода [1].

**Литература**

1. Защита бизнеса NCCGroup [Электронный ресурс]. – Режим доступа: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/october/does-typescript-offer-security-improvements-over-javascript. – Дата доступа: 02.05.2020.

## МЕТОДЫ ОБЕСПЕЧЕНИЯ И ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Хакерские атаки на компьютерные сети АЭС могут вызвать отключение электричества или поступление вирусного кода, который (как в некоторых известных случаях) не просто делает невозможной выполнение отдельных операций, начиная с простой перезагрузки компьютера, но может блокировать АСУ управления всего цикла производства электроэнергии.

Система безопасности АЭС имеет сложную структуру, состоящую их пяти контуров кибербезопасности. Первый и второй контуры состоят из датчиков, объединенных в локальной сети обработки информации. Третий и четвертый уровни обеспечивают работу операторов оперативного и неоперативного управления, необходимую для управления технологическим оборудованием АЭС и технологов на автоматизированных рабочих местах (АРМ), которые снабжены средствами визуализации технологических процессов, но лишены возможности управления. Пятый контур – контур внешнего доступа для сопряжения с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления по автономным изолированным от Интернета каналам связи.

В работе для каждого контура рассмотрены возможности нарушения режима безопасности и пути уменьшения вероятности их возникновения или умышленной реализации, необходимые при разработке моделей угроз, модели нарушителя и соответственно модели защиты.

Практически важными и обязательными средствами для уменьшения потенциальной угрозы является: снижение числа уязвимостей еще на этапе проектирования, например, использованием в контурах управления сертифицированных операционных систем на базе Linux, которые исследовать на уязвимости намного проще; получение доступа к USB-портам

компьютеров на АЭС согласно установленным процедурам; учет «недокументированных возможностей» (НДВ) электронных компонентов как знанием исходного кода, так и самостоятельной прошивкой используемых электронных компонентов, а также решением задачи о создании из «недоверенных» компонентов собственной программной платформы, как доверенной системы и верификацией ее модели на симуляторе на предмет расхождения контролируемых параметров.

**Литература**

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

## ПРОГРАММНЫЙ МОДУЛЬ КЛАССИФИКАЦИИ РЕЧИ

А.С. Райкевич

В современных условиях информационного общества с каждым днем все более актуальным становится использование речевых технологий, таких как распознавание, анализ речи, голосовое управление сложными техническими системами, а также автоматизированная постановка произношения. Автоматическое распознавание речи является динамично развивающимся направлением в области искусственного интеллекта. Распознавание речи является задачей классификации образов акустических характеристик речевых сигналов.

Архитектура системы включает два основных модуля – модуль предобработки сигнала, который предназначен для выделения информативных акустических характеристик речевого сигнала и формирования акустического сигнала как набора характеристик и модуль постобработки сигнала.

На этапе предварительной обработки исходный сигнал преобразуется в векторы признаков, на основе которых затем будет произведена классификация. Этот этап включает в себя следующие шаги:

– процесс ввода речевого сигнала;

– применение фильтров для подавления шумов;

– выделение границ речи;

– нарезка речевого сигнала перекрывающимися кадрами;

– выделение признаков сигнала.

Выделение признаков сигнала происходит по методу мел-частотных кепстральных коэффициентов. Вычисление мел-частотных кепстральных коэффициентов включает в себя следующие шаги:

– разделение исходного сигнала на кадры, кадры накладываются друг на друга;

– к каждому кадру применяется преобразование Фурье;

– к каждому кадру применяется блок мел-фильтров – треугольных пересекающихся фильтров, расположенных наиболее плотно в области нижних частот;

– полученные энергии логарифмируются;

– применяется дискретное косинусное преобразование;

На вход программной оболочки попадает звуковой файл форматом WAV. На экране отображаются сигналы, соответствующие этапы обработки, а также параметры преобразования. В результате обработки на выходе образуется массив фонетических единиц.

В результате предложена программная оболочка для обработки речевых сигналов для системы распознавания речи.

## БЕЗОПАСНОСТЬ КООРДИНАЦИИ ЗАДАНИЙ АГЕНТОВ НАБЛЮДЕНИЯ

М.П. Ревотюк, О.В. Кузнецова

Предмет рассмотрения – способ компактного представления в произвольный момент состояния распараллеливаемых и мигрируемых процедур оптимальной координации агентов наблюдения в системах сервисов с целью последующего восстановления состояния и продолжения процесса решения на любом доступном узле вычислительной сети.

В любой момент времени поиска решения на дереве вариантов можно выделить фронт волны переменных состояния рекурсивно вызываемых функций анализа отдельного узла. Возможность выделения пути от его корня дерева к листу в произвольный момент прерывания появится лишь после дополнения переменных состояния ссылкой на их предыдущий экземпляр. Предлагается такое дополнение оформить объектом класса в рамках объектных технологий, автоматизируя функциональное замыкание интервала перехода между смежными уровнями дерева вариантов. Локальный фрагмент переменных состояния включаются в список конструктором такого класса непосредственно после выделения памяти. Исключение из списка производится деструктором перед освобождением памяти.

Переход между уровнями ветвления дополняется операциями в рассматриваемом классе для синхронной обработки прерываний. Альтернативы ветвления представимы инкрементом вектора состояния на предыдущем уровне. Возврат процесса в предшествующее состояние реализуется операцией декремента. Сохранение состояния процесса решения удобно синхронизировать с моментом обработки листа дерева вариантов.

Таким образом, состояние процесса решения оказывается представленным удобным для его миграции и дальнейшего распараллеливания системно-независимым и проблемно-ориентированным способом. Иллюстрация применения предлагаемой технологии проводится на примере динамической задачи о назначении [1] и задачи многих коммивояжеров.

**Литература**

1. Zlot R., Stentz A. Market-based multirobot coordination for complex tasks // International Journal of Robotics Research. – 2006. – No. 25 (1). – P. 1–25.

## БЕЗОПАСНОСТЬ РЕАЛИЗАЦИИ СИСТЕМ КООРДИНАЦИИ АГЕНТОВ

М.П. Ревотюк, М.Д. Тараскевич

Координация систем взаимодействующих агентов требует регулярного решения задач о динамическом назначении свободным агентам новых возникающих заданий [1] и возможной коррекции текущего плана назначения. Необходимость учета реальных отношений между агентами и заданиями приводит к экспоненциальной сложности алгоритма формирования их оптимального паросочетания, что ограничивает возможности обеспечения безопасности систем управления.

Предлагается операции реализации стандартных функциональных требований безопасности синхронизировать с работой процедур оптимизации управления на интервалах ожидания событий. Такие интервалы естественно определяются понятиями наиболее раннего и позднего срока начала исполнения заданий процедурами жадного упреждающего поиска окончательного назначения. Так как процедура назначения дополняет граф оптимального паросочетания при поступлении новых заявок, то время реакции на заявку определяется сложностью обработки последней группы заявок.

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

**Литература**

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

## СРАВНЕНИЕ СИСТЕМ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ СЕТИ WI-FI

А.С. Савичев

В представленных ниже таблицах приведены данные, на основе которых на практике можно упростить процесс оценки функционала существующих свободно распространяемых систем мониторинга сетевого оборудования сети Wi-Fi.

| Название системы | Диаграммы | Отчеты SLA | Логическая группировка | События | Прогнозирование событий |
|---|---|---|---|---|---|
| Cacti | Да | Да | Да | Да | Да |
| Nagios | Да | Плагин | Да | Да | Нет |
| Zabbix | Да | Да | Да | Да | Да |
| Observium | Да | Да | Да | Да | Да |

| Название системы | Автоматическое обнаружение | Агент | SNMP | Syslog | Внешние скрипты |
|---|---|---|---|---|---|
| Cacti | Через плагин | Нет | Да | Плагин | Да |
| Nagios | Через плагин | Да | Плагин | Плагин | Да |
| Zabbix | Да | Да | Да | Да | Да |
| Observium | Да | Нет | Да | Да | Да |

| Название системы | Плагины | Сложность создания плагинов | Триггеры / Тревоги | Инвентаризация | Карты |
|---|---|---|---|---|---|
| Cacti | Да | Средний | Да | Нет | Плагин (Weathermap) |
| Nagios | Да | Легкий | Да | Плагин | Динамические и настраиваемые |
| Zabbix | Да | Средний | Да | Плагин | Да |
| Observium | Да | Легкий | Да | Да | Да (Google Maps) |

### Литература

1. Основы мониторинга и сбора метрик [Электронный ресурс]. – Режим доступа: https://www.8host.com/blog/osnovy-monitoringa-i-sbora-metrik. – Дата доступа: 10.05.2020.

2. Шмелев В.В. Метод мониторинга технологических процессов на основе структурно-логического подхода // Интеллектуальные технологии на транспорте. – 2017. – № 2. – С. 5–14.

3. Линикова О.Е. Мониторинг серверного оборудования и приложений. – Екатеринбург, 2014.

## ЗАЩИТА ИНФОРМАЦИИ В ШИРОКОВЕЩАТЕЛЬНОМ КАНАЛЕ НА ОСНОВЕ СМЕЖНЫХ КЛАССОВ РЕШЕТЧАТЫХ КОДОВ

С.Б. Саломатин, М.А. Алисеенко, В.В. Панькова

Защита информации в широковещательном канале от перехвата предполагает организацию схемы передачи данных с заданной скоростью и решения задачи восстановления информации из перехваченных сообщений нелегитимным пользователем [1, 2]. При этом предполагается, что перехватчик обладает неограниченными вычислительными способностями.

*Схема защиты*. Схема использует свойства смежных классов модулярных решетчатых кодов. В процессе кодирования сообщение отображается на смежный класс кода, а в канал передается случайная точка в пределах смежного класса.

*Варианты случайного кодирования.* Рассматриваются многомерные модулярные решетки обобщенных кодов конечных полей. Модели декодеров соответствуют схемам декодирования по критерию максимального правдоподобия и решению задачи CVP – поиска ближайшего вектора.

Статистический анализ процессов декодирования сигналов без использования случайности и случайного кодирования с использованием смежных классов показывает, что рандомизация алгоритмов передачи снижает эффективность приемника-анализатора в канале перехвата.

**Литература**

1. Semantically Secure Lattice Codes for the Gaussian Wiretap Channel/ C. Ling [et al.] // IEEE Transactions On Information Theory. – 2014. – Vol. 60, no 10.

2. Zamir R., Nazer B., Kochman Y. Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation abd Multi-user Information Theory. – Cambridge University Press, 2014.

## ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ В ОБУЧАЮЩИХ СИСТЕМАХ

А.В. Саскевич

При разработке информационных обучающих систем вопрос безопасности может оказаться вне зоны внимания разработчиков и исследователей. Тем не менее, обучающие системы, находящие свое применение в таких сферах как авиация, медицина, инженерия, требуют адекватного подхода к вопросу технической организации безопасности, так как это может повлиять как на подготовку учащихся, так и на их качество работы в будущем [1].

Разделение процесса организации безопасности позволяет разделить подходы, применяя их точечно в рамках задач, для которых они предназначены [2]. Информационная обучающая система подразумевает организацию безопасности как внешне – от несанкционированного доступа, DDoS-атак, так и изнутри – от попыток учащихся получить доступ, например, к ответам на тесты, или к редактированию итоговых оценок. Для внешней защиты подойдут классические методы и системы, такие как, например, фаервол. Для защиты изнутри могут применяться методы изоляции процессов в ОС, формирование уровней доступа пользователей и организация системы привилегий. В некоторых случаях информационные обучающие системы подразумевают возможность выполнения пользовательского кода. В данном случае потребуется изоляция исполняемого процесса, например, в виртуальную машину или контейнер.

Таким образом, при разработке обучающих систем необходимо обеспечить адекватный уровень изоляции пользователей, учебного и тестового материала, в ряде случаев обеспечить физическую и сетевую изоляцию машины, уровни доступов для учащихся разных направлений и категорий, а также, при разработке конкурирующей информационной системы, применить методики защиты информации и повышения отказоустойчивости системы.

**Литература**

1. Данилов А.Н., Шабуров А.С. О проблеме информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – №. 1. – С. 89–95.

2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации. – Directmedia, 2015.

## КОМПЬЮТЕРНЫЙ ТРЕНАЖЕР ЯДЕРНОЙ ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ

С.М. Сацук, С.С. Стома

Обеспечение безопасной и эффективной эксплуатации Белорусской АЭС – одна из приоритетных задач при подготовке высококвалифицированных специалистов в рамках

специальности «Электронные и информационные управляющие системы физических установок». Подготовка таких специалистов осуществляется в рамках Государственной программы «Образование и молодежная политика» на 2016–2020 годы.

Национальным исследовательским ядерным университетом «МИФИ» (г. Москва), для учебного процесса в БГУИР, был поставлен компьютерный многофункциональный анализатор режимов ядерной энергетической установки (ЯЭУ) с реактором ВВЭР-1000. Кроме модели ЯЭУ с реактором типа ВВЭР в состав программного обеспечения включена модель реактора ВВЭР, которая предназначена для изучения характеристик исключительно активной зоны реактора. В состав оборудования для этой модели входят реактор, активная зона и система управления и защиты реактора (СУЗ). Эти составляющие модели позволили разработать для студентов комплекс работ, связанный с решением ряда задач, таких как, анализ физических процессов, происходящих в активной зоне в различных режимах, их взаимосвязь с процессами в других системах энергоблока; прогнозирование эксплуатационных характеристик оборудования активной зоны и параметров топливного цикла; расчет физических процессов, происходящих в реакторе и ЯЭУ, в активной зоне реактора во время плановых экспериментов по сбросу «АЗ», измерению коэффициентов реактивности и интегральной и дифференциальной характеристик органов регулирования СУЗ, определение характеристик самозащищенности и параметров СУЗ.

В ходе работы на тренажере студенты моделируют различные отказы в оборудовании, аварийные ситуации на АЭС. Кроме этого, им ставятся задачи по изучению физических процессов, происходящих в реакторной установке, режимах работы и алгоритмах управления энергоблоком.

Комплекс работ на компьютерном анализаторе позволяет значительно повысить качество подготовки специалистов для ядерной энергетики, сформировать целостное понимание процессов, происходящих в активной зоне реакторной установки. Аналитический тренажер с комплексом практических занятий может успешно использоваться и при подготовке персонала для Белорусской АЭС.

## ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ДЛЯ ЯДЕРНОЙ ЭНЕРГЕТИКИ

С.М. Сацук, С.С. Стома

В соответствии с программой МАГАТЭ по разработке и внедрению Стандартов (Норм) по безопасности, одной из тематических областей является система управления, построенная на основе программно-технических средств (ПТС). Такие ПТС должны содержать средства защиты от несанкционированного доступа и изменения информации и/или специальных программных воздействий на нее.

На Белорусской АЭС одним из основных ПТС является оборудование ТПТС-НТ, предназначенное для создания программно-технических комплексов, выполняющих автоматический контроль и управление технологическим оборудованием.

При подготовке специалистов для Белорусской АЭС в рамках специальности «Электронные и информационно-управляющие системы физических установок» осуществляется практическое обучение на базе типового комплекта оборудования ТПТС-НТ, производимого «Всероссийским научно-исследовательским институтом автоматики имени Н.Л. Духова». На базе этого оборудования был подготовлен комплекс работ для студентов.

В процессе работы на оборудовании ТПТС-НТ студенты создают тестовые алгоритмы приема и первичной обработки дискретного сигнала, алгоритмы обработки аналогового унифицированного сигнала тока и/или напряжения средствами стандартных функциональных блоков в редакторе GET-R1, алгоритмы с использованием двух входных дискретных и одного аналогового сигналов для управления электродвигателем и запорной арматурой, реализуют алгоритмы контроля и управления регулирующим клапаном и обеспечивают защиту от несанкционированного доступа на программном уровне. В качестве источника аналогового сигнала тока используется мультиметр-калибратор АКИП-2201. В качестве источника дискретных сигналов применяется имитатор дискретных сигналов. В ходе реализации алгоритма ставится задача обеспечить необходимую логику блокировок, защит

и автоматических команд, передачу сигналов состояния и неисправностей по шине ввода-вывода в алгоритмы, выполняемые в других модулях ТПТС. Созданные алгоритмы проверяются на ошибки аппаратными средствами GET-R1. Система тестируется с помощью диагностической станции, имитаторов двигателя, задвижки и клапана.

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

## МОДЕЛИ ПОЛИНОМИАЛЬНО-НОРМЕННОГО ДЕКОДЕРА БЧХ-КОДА

Е.В. Середа

Разработанная на рубеже XX–XXI веков теория норм синдромов (ТНС) обеспечила новые, перестановочные норменные методы коррекции ошибок семейством кодов Боуза-Чоудхури-Хоквингема, альтернативные классическим синдромным методам. В частности, методам, базирующимся на решении алгебраических уравнений в полях Галуа из $2^m$ элементов – полях определения конкретных применяемых БЧХ-кодов.

Так или иначе, любой метод исправления ошибок помехоустойчивым кодом решает проблему «селектора» – перебора в каждом случае наличия ошибки всего многообразия $M$ исправляемых в принципе кодом векторов-ошибок. Главная особенность норменных методов в том, что селеекции подвергается не весь спектр M векторов-ошибок, а их Г-орбиты, то есть в n раз меньшее множество. Здесь n – длина кода, Г – группа порядка n циклических сдвигов координат векторов.

На самом деле перебор проводится среди норм Г-орбит – специальных синдромных идентификаторов этих орбит. Группа автоморфизмов БЧХ-кода позволяет объединять Г-орбиты в более крупные – $G$-орбиты, которых идентифицируют полиномиальные инварианты. Это неприводимые над Z/2Z полиномы с корнями – нормами Г-орбит, составляющих ту или иную $G$-орбиту. Переход к $G$-орбитам и их инвариантам позволяет еще в m раз сократить переборные процедуры [1].

В настоящее время проводится разработка моделей полиномиально-норменных декодеров, их программных и программно-аппаратных реализаций.

**Литература**

1. Липницкий В.А., Середа Е.В. Полиномиальные инварианты $G$-орбит ошибок в непримитивных БЧХ-кодах с конструктивным расстоянием 5 // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 2. Матэматыка. Фізіка. Інфарматыка, вылічальная тэхніка і кіраванне. – 2019 – Т. 9, №1. – С. 118–127.

## ХЕШИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ ЭЛЕКТРОННОМ ГОЛОСОВАНИИ

А.В. Сидоренко, А.В. Валенда

В последнее время системы электронного голосования находят все более широкое распространение. Под электронным голосованием обычно подразумевается процесс голосования с помощью компьютеризированного оборудования.

При этом существенное значение приобретают вопросы обеспечения безопасности, что связано с предоставлением таких услуг, как конфиденциальность и целостность данных, аутентификация объектов и источника данных. Технология блокчейна [1] может обеспечить не только надежный канал передачи информации, но и способ преодоления потенциальных угроз, уязвимостей и атак. Блокчейн представляет собой новую технологию, возникшую в поле биткоинов и демонстрирующую, что с помощью объединения одноранговых сетей с криптографическими алгоритмами можно предоставить необходимые возможности для того,

чтобы сделать операции внутри системы более гибкими, автономными и безопасными [2]. Блокчейн является, по сути, общедоступной хронологической базой данных транзакций. Данные сгруппированы в наборы, называемые блоками. Каждый блок содержит информацию об определенном количестве транзакций, ссылку на предыдущий блок в цепочке блоков и ответ на задачу, известную как «доказательство работы». Она основана на криптографических вычислениях, в частности вычислении значений хеш-функции, которые дают непредсказуемые числовые последовательности. Блокчейн инкапсулирует все транзакции внутри блока в цифровом отпечатке, которым и является хеш. Хеш-функции в блокчейнах гарантируют «необратимость» всей цепочки транзакций.

В данной работе предложена система электронного голосования, в которой для формирования хеш-функции применяются хаотические отображения. Среди исследованных хаотических отображений выбраны: логистическое отображение, тент-отображенние и отображение Чирикова. Проведен вычислительный эксперимент, в котором в качестве критерия производительности выбрано время, необходимое для генерации одного блока блокчейна. Показано, что использование логистического отображения при хешировании позволяет получить оптимальное значение и повысить производительность на 5–7 %.

**Литература**

1. Nakamoto S. Bitcoin: a Peer-to-Peer Electronic Cash System. – 2008.

2. Chi L., Zhu X. Hashing techniques: a survey and taxonomy // ACM Computing Surveys. – 2017. – Vol. 50, no. 1. – P. 1–36. – https://doi.org/10.1145/3047307.

## ТУННЕЛИРОВАНИЕ СПИН-ПОЛЯРИЗОВАННЫХ ЭЛЕКТРОНОВ НА ПОВЕРХНОСТНЫЕ СОСТОЯНИЯ ДИОКСИДА ТИТАНА

Т.Н. Сидорова

В данной работе расссмотрим процессы, происходящие в гетероструктуре $TiO_2$/Co/Si (Si – подложка, $TiO_2$ – пленка нанометровой толщины, Co – прослойка(подложка) для усиления поляризации света) под действием падающего на нее пучка поляризованного света [1]. Неравновесные дырки, проходя Co, диффундируют в Si, а электроны уходят в $TiO_2$ и далее на его поверхность. Движимые градиентом концентрации неравновесные электроны проходят нанометровый $TiO_2$ практически без рассеяния. На своем пути к границе раздела между структурой и окружающей ее газовой (или жидкой) средой они встречают потенциальный барьер из поверхностных состояний, образованных адсорбированными на поверхности $TiO_2$ примесями. Здесь каждый локальный энергетический максимум соответствует определенному поверхностному состоянию, а потенциальные ямы между максимумами отражают возможность перехода электронов из одного поверхностного состояния в другое. Очевидно, что прохождение электронами такого потенциального барьера может происходить исключительно путем их туннелирования. Для нахождения коэффициентов прохождения нами разработана модель на основе метода фазовых функций [2]. Будем вычислять не саму волновую функцию, а только ее изменение вследствие действия потенциала. В соответствии с предложенной моделью рассчитаны зависимости величины степени поляризации от приложенного напряжения для генерируемых солнечным светом электронов, при условии, что поверхностные состояния на $TiO_2$, образованы адсорбированными на его поверхности органическими загрязнениями. Рассмотренная величина степени поляризации электронов, генерируемых солнечным светом в $TiO_2$, на его поверхностные состояния с учетом формы связанных с ними потенциальных барьеров, показало, что с увеличением приложенного напряжения величина степени поляризации солнечного света линейно увеличивается, если потенциальный рельеф представляет собой один барьер. В случае, когда потенциальный рельеф на поверхности $TiO_2$ состоит из двух барьеров, разделенных потенциальной ямой, возникает нелинейность, которая определяется резонансным прохождением электронов через дискретные уровни в квантовой яме и интерференцией электронных волн, отраженных от второго барьера. Установленные закономерности спин-поляризованного туннелирования электронов, генерируемых солнечным светом в $TiO_2$, через его поверхностные состояния позволяют

выбирать оптимальные условия его облучения, обеспечивающие максимальный выход электронов на поверхность $TiO_2$, а, следовательно, наивысшую эффективность протекания фотокаталитических процессов с их участием.

**Литература**

1. Алексеев П.С., Чистяков В.М., Яссиевич И.Н. Влияние эленктрического поля на спин-зависимое резонансное туннелирование // ФТП. – 2006. – Т. 40, вып. 12. – С. 1436–1442.
2. Бабиков В.В. Метод фазовых функций в квантовой механике. – М.: Наука, 1976. – 224 с.

## ИНСТРУМЕНТЫ АНАЛИЗА РИСКОВ В JAVASCRIPT

И.Д. Стаселько, М.А. Аниховский, Ю.И. Алексеев, А.С. Летохо

В наши дни практически невозможно писать на JavaScript без использования одной из тысяч доступных библиотек JavaScript с открытым исходным кодом. Библиотеки делают кодирование в JavaScript эффективнее, упрощая процессы, которые требуют нескольких строк кода для их достижения. Однако эти преимущества не обходятся без рисков.

Библиотеки JavaScript уязвимыми. Согласно исследованию, Северо-Восточного университета, «более 37 % веб-сайтов используют хотя бы одну версию библиотеки с известной уязвимостью» [1]. Уязвимости безопасности в JavaScript включают межсайтовый скриптинг (возможность внедрить вредоносный код) «Экосистема JavaScript не имеет надежной структуры для документирования уязвимостей в библиотеках и документирования их последствий», – сказал SD Times Арнал Дайаратна, директор по исследованиям IDC.

Нет единого списка уязвимостей, доступных для разработчиков. Уязвимости JQuery отображаются на веб-сайте CVE (каталогом распространенных уязвимостей). Тем не менее, Angular не отображается в CVE; вместо этого он использует GitHub CHANGELOG для сообщения об уязвимостях безопасности, каждая библиотека обрабатывает информацию о безопасности по-разному, поэтому разработчики не могут полагаться на одно местоположение обновлений списка угроз. Согласно сообщению, в блоге npm: «Современный проект JavaScript обычно зависит от 700–1200 пакетов». Именно здесь инструменты анализа состава программного обеспечения становятся необходимыми. Инструменты анализа проверяют код и выбирают уязвимые компоненты, например, инструмент «SonarQube». Это ускоряет процесс обнаружения уязвимостей на сайте, а также снижает риск человеческих ошибок. Исследование Северо-Восточного университета показало, что медианный веб-сайт использовал библиотечную версию, которая была «на 1177 дней старше, чем новейшая версия».

Переход на более новую версию, учитывающую потенциальную угрозу, требует времени, поскольку необходимо выполнить тестирование, чтобы убедиться, что последняя версия совместима с существующим приложением или сайтом. Постоянное обновление до более новых версий библиотек не может гарантировать полную защиту существующим сайтам от уязвимостей, что отменит любую экономию средств, полученную от неправильного обновления сайта.

**Литература**

1. K. Watanabe, T. Fukamachi, N. Ubayashi and Y. Kamei, PosterIEEE International Conference on Software Testing [Electronic resource]. – Access mode: https://aws.amazon.com/solutions/casestudies. – Date of access: 29.11.2019.

## НЕКОТОРЫЕ ТЕХНИКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

М.В. Стержанов, А.И. Гридасов, В.Я. Анисимов, В.Н. Теслюк

Социальная инженерия представляет из себя совокупность методов получения необходимого доступа к информации, основанных на особенностях психологии людей.

Приемы социальной инженерии классифицируются как нетехнические, однако они могут эффективно сочетаться с широко известными приемами использования вредоносных вложений, скрытого внедрения программ и т. д.

Претекстинг – это набор действий, отработанных по определенному, заранее составленному сценарию (содержащему психологические ловушки), в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Зачастую данный вид атаки применяется по телефону, при этом злоумышленник действует максимально быстро, не оставляя времени на размышления. В начале общения злоумышленник пытается получить доверие при помощи использования заранее заготовленных данных (имя человека; номер автомобиля; адрес).

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей (например, пин-кодов, авторизационных данных). Мошенники создают поддельные сайты, мимикрирующие под хорошознакомые ресурсы. Основным видом фишинговых атак является рассылка поддельных писем, с просьбой срочно выполнить какие-либо действия, связанных с аккаунтом пользователя (разблокировка, обновление информации, получение выигрыша и т.д.). Пользователь направляется на страницу ввода ввода учетных данных.

Для предотвращения атак, основанных на техниках социальной инженерии, рекомендуется регулярно проводить инструктаж сотрудников о способах реализации данных угроз, а также учитывать данные угрозы при составлении политики информационной безопасности. Рекомендуется использовать почтовые антивирусы, которые производят постоянное автоматическое сканирование писем на предмет вредоносного программного обеспечения.

## ТРЕХМЕРНОЕ ТВЕРДОТЕЛЬНОЕ МОДЕЛИРОВАНИЕ СТАБИЛИЗАТОРА НАПРЯЖЕНИЯ, ИЗГОТОВЛЕННОГО НА БАЗЕ SMD КОМПОНЕНТОВ

В.А. Столер, Е.П. Федорович

Предлагается рассмотреть построение в САПР Autodesk Inventor трехмерной твердотельной модели стабилизатора напряжения, изготовленного на базе SMD компонентов, для использования в системах защиты от ЭМИ. Перспектива увидеть разрабатываемое радиоэлектронное устройство в трехмерном изображении еще до его изготовления позволяет оценить, как все изделие в целом, так и отдельные его элементы [1].

В работе отмечаются следующие принципиальные достоинства SMD технологии. Во-первых, это уменьшение размеров готового электронного устройства благодаря малым размерам SMD компонентов, что позволяет увеличить плотность монтажа и как следствие уменьшить общие габариты изделия. Во-вторых, сокращение числа технологических операций за счет отсутствия отверстий для крепления элементов, которые при такой технологии запаиваются на поверхностные контактные площадки. В-третьих, вес SMD компонентов заметно легче, чем их вес в дискретном исполнении, и как результат – уменьшение массы радиоаппаратуры. Кроме того, SMD компоненты можно монтировать с обеих сторон платы, что позволяет учесть их электромагнитную совместимость. В то же время при изготовлении радиоэлектронного устройства и при проведении его ремонтных работах, когда нужно монтировать или демонтировать SMD компоненты, требуется специальное оборудование в виде автоматизированных комплексов. Но при всех своих минусах, которые имеют место быть, результирующий эффект от применения SMD компонентов говорит о перспективности и востребованности данной технологии. Компьютерная проработка изделия в виде трехмерной твердотельной модели наглядно это демонстрирует, позволяя заблаговременно выявлять возможные недостатки его конструкции.

**Литература**

1. Столер В.А., Столер Д.В. Использование трехмерных технологий для моделирования и создания защитных экранов ЭМИ // Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 4–5 июня 2015 г. – 2015. – С. 79.

## БЕЗОПАСНОСТИ И ТЕХНИКИ ОТКАЗОУСТОЙЧИВОСТИ

Х.Х.К. Судани, М.Б. Абросимов

Надежность системы – ключевое требование к отказоустойчивой системе, тогда как безопасность обеспечивается посредством модернизации межсетевой защиты и обнаружения вторжений. В терминологии безопасности термин «уязвимость» вследствие ошибок программного обеспечения или неправильных настроек сопоставим с термином «ошибки (неисправности) в отказоустойчивости».

Таким образом, разработка совокупности подходов и методов для повышения эффективности системы информационной безопасности за счет применения отказоустойчивых вычислительных систем является актуальной научно-технической проблемой, имеющей важное социально-экономическое значение [1]. При несвоевременном обнаружении и исправлении ошибок может произойти сбой, показывающий неспособность оказания соответствующей системной услуги. Отказоустойчивость – это способность системы восстанавливаться после произошедшего сбоя или возникшей ошибки без демонстрации самого сбоя. Сбой в системе не обязательно приводит к ошибке; он может оставаться в месте его возникновения, что не приводит к ошибке. Для вызова ошибки сбой должен быть активизирован определенным состоянием системы и условиями ввода. Методы, связанные с отказоустойчивыми системами, включают в себя предотвращение сбоя, его маскирование, обнаружение ошибочной или скомпрометированной системной операции, сдерживание распространения ошибок и восстановление нормальной работы системы [2]. Отказоустойчивость, направленная на предотвращение неисправностей, осуществляется посредством обнаружения ошибок и восстановления системы. При этом отказоустойчивая система может продолжать работать в нормальном режиме. Система информационной безопасности и отказоустойчивости позволит при распознавании известных неисправностей задействовать меры по их парированию с гарантированием достоверности выходной информации системы [3].

**Литература**

1. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа // Вестник ПНИПУ. – 2015. – № 16. – С. 23–27.

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

3. Лобанов А.В., Сиренко В.Г. Проблема отказоустойчивости в сетецентрических информационно-управляющих системах // Образовательные ресурсы и технологии. – 2014. – № 2 (5). – С. 115–121.

## CROSS-SITE SCRIPTING

А.Ю. Сычев, Т.Д. Позняков, Ю.И. Алексеев

JavaScript – это высокоуровневый интерпретируемый динамически типизированный язык программирования, который взаимодействует с «Document Object Model» пользователя для выполнения различных функций, таких как: структурированное представление документа и определение того, как эта структура может быть доступна из программ, которые могут изменять содержимое, стиль и структуру документа. Cross-Site Scripting является одним из самых распространенных уязвимостей веб-приложений, используемая хакерами для получения несанкционированного доступа к информации. XSS осуществляется путем выполнения любого нежелательного, вредоносного или несанкционированного JavaScript сниппета (скрипта) на компьютере жертвы или в веб-приложении. Такая процедура может привести к потере информации, перенаправлению пользователя на нежелательный сайт, получения доступа к пользовательскому буферу обмена или истории браузера. Даже такие гиганты, как Facebook, подвергались атакам: в июле 2015 г. личный аккаунт М. Цукерберга был взломан и оповещен об уязвимости. Важно отметить, что любая информация, передаваемая от пользовательского до серверного, может нести в себе потенциальную угрозу или фактор

заражения. К ним относятся: параметры запроса, URL-путь, методы PUT / POST, файлы cookie, Cross-Site Scripting (XSS) и т. д. Данная уязвимость не может быть предотвращена фаерволом веб-приложения(web app firewall). Однако есть некоторые методы противодействия, например:

1) проверка и обработка вводимых пользователем данных;

2) кодирование выходных данных для конкретного элемента, особенно, если выходные данные содержат HTML теги;

3) укзаание правильных заголовков: Strict transport security, X-frame-options, X-XSS-protection, X-Content-Type-Options, Content-Security-Policy.

Предпринимая вышеуказанные меры, можно существенно сократить риск атаки, но не устранить угрозу в полной мере. Поэтому поиск эффективных мер противодействия является актуальной задачей [1, 2].

**Литература**

1. What is Cross-site Scripting and How Can You fix it? [Electronic resource]. – Access mode: https://acunetix.com/websitesecurity/cross-site-scripting/. – Date of access: 30.04.2020.

2. How does Cross-site Scripting (XSS) impact customers? | Packetlabs [Electronic resource]. – Access mode: https://www.packetlabs.net/cross-site-scripting-xss/. – Date of access: 30.04.2020.

## ЗАЩИЩЕННЫЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА КАНАЛ ОДНОФОТОННОЙ СВЯЗИ С КОДИРОВАНИЕМ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ДЛИТЕЛЬНОСТЬЮ ОПТИЧЕСКОГО ИМПУЛЬСА

А.М. Тимофеев

При передаче информации в современных сетях связи важно обеспечивать ее скрытность и конфиденциальность. Для решения этой задачи целесообразно применять однофотонные каналы связи, характеризующиеся максимально высоким уровнем информационной безопасность за счет использования квантово-механического ресурса при кодировании передаваемых данных [1]. Однако скорость передачи информации в однофотонных каналах связи мала и зачастую не превышает нескольких десятков кбит/с [2, 3], что объясняется достаточно большой вероятностью ошибочной регистрации данных. Поскольку до настоящего времени отсутствует способ кодирования передаваемой информации в однофотонных каналах связи, позволяющий достичь максимальной скорости передачи информации, это являлось целью данной работы. Объект исследования – однофотонный канал связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа. Применительно к однофотонным каналам связи разработан способ кодирования передаваемой информации длительностью оптического импульса. Выполненная оценка показала, что максимальная скорость передачи информации достигается при средних длительностях однофотонной передачи символов «0» и «1» 12 мкс и 38 мкс соответственно и использовании счетчика фотонов со средней длительностью мертвого времени 5 мкс.

**Литература**

1. Photon-counting underwater optical wireless communication for reliable video transmission using joint source-channel coding based on distributed compressive sensing / Z. Hong [et al.]. // Sensors. – 2019. – Vol. 19. № 5. – P. 1042–1054.

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

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

## ДОСТИЖЕНИЕ НАИМЕНЬШИХ ПОТЕРЬ ИНФОРМАЦИИ В ОДНОФОТОННОМ КАНАЛЕ КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ

А.М. Тимофеев, А.С. Колядич, М.В. Корбут

При создании современных систем защиты информации требуется обеспечивать достаточно высокий уровень информационной безопасности передаваемой информации. Это становится возможным благодаря использованию однофотонных каналов связи [1–3], при реализации которых критически важно применение легитимными пользователями высоконадежного оборудования [2, 3]. Для оценки надежности оборудования, реализующего системы связи на базе двоичных асинхронных однофотонных каналов передачи информации, могут быть использованы такие характеристики, как достоверность принятой информации [2], либо вероятность ее ошибочной регистрации [3]. Однако достижение наибольшей достоверности принятой информации и наименьшей вероятности ее ошибочной регистрации для указанных систем связи затруднено из-за необходимости выбора пороговых уровней регистрации (нижнего и верхнего), интенсивностей оптических излучений (для каждого двоичного символа) и среднего времени однофотонной передачи одного бита (символа). Поскольку до настоящего времени методика выбора указанных параметров отсутствует, это являлось целью данной работы. Применительно к асинхронному двоичному однофотонному двоичному каналу связи разработана методика достижения наименьших потерь информации. Методика основана на учете двух составляющих вероятностей ошибочной регистрации двоичных символов, включает измерение статистических распределений смеси числа темновых и сигнальных импульсов, полученных на выходе приемного модуля, и позволяет определить нижний и верхний пороговые уровни регистрации, интенсивности оптических излучений для каждого двоичного символа и среднее время однофотонной передачи одного бита (символа), при которых потери передаваемой информации наименьшие.

**Литература**

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

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

3. Тимофеев А.М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи // Вестник связи. – 2018. – № 1. – С. 56–62.

## ВЛИЯНИЕ КОНСТРУКЦИИ КОРПУСА МИКРОСХЕМ НА ИХ ВОСПРИИМЧИВОСТЬ К ВОЗДЕЙСТВИЮ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ

Н.А. Титович, В.Н. Теслюк

Перед разработчиками специальных радиоэлектронных систем нередко стоит задача обеспечения их надежной работы при уровнях напряженности электромагнитных полей до 20 и более кВ/м. При проектировании бортовой аппаратуры вопросы защиты от помех целесообразно рассматривать на этапе выбора элементной базы, а традиционные экраны во избежание увеличения габаритов и веса используются только для защиты наиболее уязвимых мест устройства. Результаты исследований показали, что для получения достаточно полной информации о восприимчивости интегральных микросхем (ИМС) к воздействию ЭМП можно использовать дешевый кондуктивный способ подачи помехового сигнала непосредственно на объект исследования. Однако при оценке влияния конструкции корпуса ИМС на их реакцию к воздействию ВЧ и СВЧ помех целесообразнее применять метод ТЕМ-камеры, так как, несмотря на большие затраты, он более точный.

Проведены исследования воздействия мощных СВЧ импульсных помех на ИМС серий 1533 (ЛА3 и ТР2) и 1564 (ТЛ2). Исследуемые микросхемы помещались перед раскрывом антенны имитатора электромагнитных помех (ЭМП). Исследовалось воздействие как одиночных, так и серий импульсов. С целью исследования зависимости восприимчивости от конструкции микросхем, в частности от длины и расположения выводов, были выбраны ИМС с одинаковыми типами корпусов (типов 401 и 402). При испытаниях в режиме хранения микросхемы располагались в трех положениях: 1) кристалл расположен в горизонтальной плоскости, параллельной оси рупорной антенны имитатора помех; выводы – параллельно оси антенны; 2) кристалл и выводы – в вертикальной плоскости, перпендикулярно оси антенны; 3) кристалл – в горизонтальной плоскости, выводы перпендикулярно оси антенны. В активном режиме микросхема устанавливалась в испытательную ячейку и включалась в соответствии с техническими условиями. С целью повышения достоверности данных исследовались не менее 5 ИМС каждого типа. Результаты испытаний показали, что устойчивость ИМС зависит как от длины выводов, так и от ориентации их к направлению электромагнитного излучения. Наибольшее число отказов наблюдалось при расположении микросхем перпендикулярно раскрыву антенны имитатора ЭМП (положение 2), когда наводки на их выводах за счет электромагнитных полей максимальные. Самыми уязвимыми в этом случае оказались цепи с более длинными выводами. Так для четырех ТТЛШ элементов 2И-НЕ из 8 входов максимальное число отказов пришлось на входные выводы, расположенные по углам корпуса, т. е. на наиболее длинные. Результаты исследований позволили уточнить параметры моделей корпуса ИМС, используемых при расчете влияния ЭМП на работоспособность ИМС и радиоэлектронных устройств.

## БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ БЕЛАРУСЬ В КОНТЕКСТЕ БОЛЬШИХ ДАННЫХ

К.И. Тишук, А.М. Прудник

В Республики Беларусь ожидается принятие закона «О персональных данных», который будучи внесенным правительством в нижнюю палату парламента, уже был одобрен в первом чтении. Данный закон призван регулировать сбор, хранение и обработку персональных данных, которые определяются как «любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано на основании такой информации». Это включает в себя не только прямые идентификаторы (например, полное имя, личный номер), но также и косвенные идентификаторы, такие как номера телефонов, IP-адреса и т.п.

Результаты анализа больших данных очень часто являются статистическими данными без прямых ссылок на конкретных физических лиц. Следовательно, простейший способ соблюдения Закона — обрабатывать только обезличенные данные. Однако определение обезличенности не является простой задачей. Даже если непосредственно идентифицируемые параметры удаляются из набора данных, возможно, можно будет повторно идентифицировать отдельных лиц, комбинируя набор данных с другой информацией.

Для обработки персональных данных Закон определяет ряд правовых, организационных и технических требований и предлагает различные методы. Прежде всего, в большинстве случаев обработка персональных данных разрешается только в том случае, если субъект данных дал свое согласие (ст. 5). Другим принципом обработки данных является минимизация данных (ст. 4), которая относится к ограничению сбора, хранения и использования персональных данных данными, которые являются необходимыми для достижения цели, для которой данные обрабатываются.

Термины «большие данные» или «анализ данных» напрямую не рассматриваются Законом. Однако из приведенного выше ясно, что большие данные и некоторые положения Закона могут входить в противоречие. Например, анализ данных основывается на анализе больших объемов данных, что часто противоречит принципу минимизации данных. Кроме того, в анализе данных очень часто вводятся новые гипотезы для тестирования после сбора данных. Однако субъекты персональных данных, у которых были получены данные, изначально давали согласие для другой

цели. Таким образом, с юридической точки зрения, если это возможно, должна производиться обработка анонимных данных. Это может потребовать оценки воздействия на безопасность данных, либо оценки того, как определенные действия могут повлиять на конфиденциальность персональных данных.

## ПРЕОБРАЗОВАНИЕ ХОТЕЛЛИНГА

В.А. Томин

Преобразование Хотеллинга один из основных способов уменьшить размерность данных, потеряв наименьшее количество информации. Применяется во многих областях, таких как распознавание образов, компьютерное зрение, сжатие данных и т.п. Преобразование сводится к вычислению собственных векторов и собственных значений ковариационной матрицы исходных данных. Имеет наилучшую эффективность в смысле концентрации энергии изображения. Преобразование обеспечивает процесс декорреляции непрерывных коррелированных сигналов в набор некоррелированных. Задача анализа главных компонент имеет своей целью аппроксимировать (приблизить) данные линейными многообразиями меньшей размерности; найти подпространства меньшей размерности, в ортогональной проекции на которые разброс данных (то есть среднеквадратичное отклонение от среднего значения) максимален; найти подпространства меньшей размерности, в ортогональной проекции на которые среднеквадратичное расстояние между точками максимально. В этом случае оперируют конечными множествами данных. Они эквивалентны и не используют никакой гипотезы о статистическом порождении данных. Кроме того, задачей анализа главных компонент может быть цель построить для данной многомерной случайной величины такое ортогональное преобразование координат, что в результате корреляции между отдельными координатами обратятся в ноль. Эта версия оперирует случайными величинами. Преобразование Хотеллинга используется для компрессии изображений. Для уменьшения пространственной избыточности пикселей при кодировании изображений используется линейное преобразование блоков пикселей. Последующие квантования полученных коэффициентов и кодирование без потерь позволяют получить значительные коэффициенты сжатия. Использование преобразования в качестве линейного преобразования является для некоторых типов данных оптимальным с точки зрения размера полученных данных при одинаковом искажении.

**Литература**

1. Гонсалес Р.С., Вудс Р.С. Цифровая обработка изображений. – Нью-Джерси: Прентис Холл, 2002.

2. Пирсон К. О прямых и плоскостях, наиболее близких к системам точек в пространстве // Философский журнал. – 1901. – № 2. – 559–572.

## ЗАЩИТА ИЗОБРАЖЕНИЯ СЕГМЕНТИРОВАННОГО ОБЪЕКТА

В.А. Томин, А.И. Митюхин

В работе рассматривается алгоритм защиты 2D-сигнала с уровнем яркости $g(m,n)$. Сигнал отображается матрицей размером $N \times N$. Переменная $m$ сигнала $g(m,n)$ обозначает положение пикселя в строке матрицы, переменная $n$ – это положение пикселя в столбце матрицы. Дискретный сигнал формируется устройством дискретизации и квантования на $L$ уровней. Передаточная характеристика квантователя соответствует нечетной ступенчатой функции $\hat{g} = f(-v) = -f(v)$, где $\hat{g}$ – целочисленное значение квантованного сигнала. Алгоритм строится на основе применения к $g(m,n)$ декоррелирующего линейного ортогонального преобразования [1], порогового кодирования (фильтрации) коэффициентов преобразования (трансформант) и кодирования с расширением спектра.

1. В общем виде операция декорреляции 2D-сигнала определяется выражением

$$\hat{g}(u,v)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}g(m,n)h(m,n;u,v)=\sum_{n=0}^{N-1}\left(\sum_{m=0}^{N-1}g(m,n)h(m,u)\right)h(n,v),0\le u\le N-1,0\le v\le N-1,$$

где $\hat{g}(u,v)-$ значения трансформант сигнала $g(m,n)$, $h(m,n;u,v)=h_1(m,u)h_2(n,v)-$ ортонормированные базисные функции (базисные изображения) с целочисленными значениями пространственных частотных параметров $u,v$.

2. Фильтрацию трансформант предлагается осуществлять на базе информационного подхода и описания изображения как случайного процесса. Тогда количество средней информации или собственная информация источника $\{\hat{g}\}$, в нашем случае преобразованного изображения, определяется энтропией $H(\hat{g})$. Количественная оценка $H(\hat{g})$ информационного содержания $g(m,n)$ позволяет устранить информационную избыточность, осуществить фильтрацию трансформант на основе дисперсионного критерия [2]. В результате передача цифрового изображения может осуществляться с минимальными временными затратами. Сокращение времени на передачу трансформант является важным приемом для практической защиты информации.

3. Кодирование после этапа фильтрации помехоустойчивым $[n,k,d]$-кодом.

На основе моделирования в среде Matlab показано, что в определенных приложениях предлагаемый алгоритм может обеспечивать высокую степень защиты данных сегментации.

**Литература**

1. Burger W., Burge M.J. Digital Image Processing. – Berlin : Springer-Verlag Heidelberg, 2005. – 515 p.

2. Митюхин А.И. Цифровая обработка речи и анализ изображений. – Минск: БГУИР, 2016. – 71 с.

## ДИАГНОСТИКА УСТАЛОСТИ ПРОГРАММИСТА

В.Н. Точко, И.А. Мурашко

Источниками угрозы информации, помимо субъектов информационных отношений, реализующих право на пользование информацией, являются средства защиты информации, включенные в состав информационных систем. Из-за допущенных ошибок при проектировании, существующие средства защиты информации могут лишь отчасти снизить риск утечки информации. Таким образом, снижение процента допускаемых при проектировании ошибок является задачей актуальной на данный момент [1]. С целью снижения процента допускаемых ошибок предлагается использовать систему диагностики физического состояния программиста, а именно диагностика уровня усталости. Диагностика уровня усталости проводится с целью получения численной характеристики физического состояния программиста. Диагностика усталости программиста проводится на основании изображения, поступающего с рабочего места. Поступающее изображение преобразуется и анализируется по технологии виброизображения. По результатам анализа, проводимого раз в определенный промежуток времени, система выносит решение об уровне усталости программиста и, в случае превышения допустимого уровня, оповещает программиста о необходимости прервать работу. Технология построения виброизображения базируется на исследованиях вестибулярно-эмоционального рефлекса. Исследования показали, что при изменении психологического и физического состояния, изменяется частота и амплитуда вибраций человеческого тела. Были представлены формулы для расчета большинства известных эмоций, включая энергичность. В связи с этим, представляется возможным вычисление уровня усталости на основании анализа перемещений человека, отслеживаемых по изображению [2].

**Литература**

1. Защита информации. Основные термины и определения. СТБ ГОСТ Р 50922-2000: Введ. 22.05.2000 – Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. – 6 с.

2. Минкин В.А. Виброизображение. – СПб.: РЕНОМЕ, 2007 – 108 с

## ТОНКОПЛЕНОЧНЫЕ ПОЛУПРОВОДНИКИ $Cu_2ZnSnS_4$(CZTS) И $SnS_x$ ДЛЯ ФОТОВОЛЬТАИКИ И LiFi СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

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

Новый класс токопленочных халькогенидных солупроводников $Cu_2ZnSnS_4$(CZTS) и $SnS_x$ интенсивно исследуется в последнее время благодаря низкой стоимости и безопасности их исходных компонентов Cu, Zn, Sn, S, высокому коэффициенту поглощения излучения ~$10^4$ $см^{-1}$, а также достаточно простым технологиям получения тонких пленок и гетероструктур на их основе для создания фотовольтаических приборов [1]. Данные материалы обладают широким спектральным диапазоном фотоэлектрической чувствительности благодаря возможности варьирования ширины запрещенной зоны (~ 1,4–2,2 эВ) путем контроля стехиометрии и микроморфологии полупроводника.

Наряду с применением CZTS и $SnS_x$ в фотовольтаике [2], в последнее время актуальны приложения тонкопленочных полупроводниковых широкодиапазонных фотоприемников в LiFi технологиях беспроводной передачи данных поколения 5G с использованием излучения светодиодных источников [3]. В сравнении с известными к настоящему времени LiFi фотоприемниками на основе перовскитных полупроводников [4], тонкопленочные CZTS и $SnS_x$ выгодно отличаются стабильностью фотоэлектрических характеристик и простотой изготовления.

В данной работе сообщается о результатах разработки и исследования модифицированного процесса послойного химического осаждения (SILAR метод) для получения тонких пленок полупроводников $SnS_x$, CZTS. Для осаждения слоев $SnS_x$ использовали последовательное окунание в растворы $Na_2S$ и $SnCl_2$ + NaCl + триэтаноламин, а для осаждения слоев CZTS последовательное погружение в растворы $CuSO_4$ + $ZnSO_4$, $SnCl_2$ и $Na_2S$ с промежуточным промыванием в дистиллированной воде. Приведены результаты исследования оптических и микроморфологических характеристик полученных тонких пленок, а также анализ требований к фотоприемникам на их основе для применения в LiFi системах передачи данных.

**Литература**

1. Copper Zinc Tin Sulfide-Based Thin-Film Solar Cells / Ed. by Kentaro Ito. – John Wiley & Sons, Ltd, 2015. – SBN 978-1-118-43787-2.

2. Beyond 8% ultrathin kesterite $Cu_2ZnSnS_4$ solar cells by interface reaction route controlling and self-organized nanopattern at the back contact / F. Liu [et al.] // NPG Asia Materials. – 2017. – P. 401.

3. Haas H. LiFi is a paradigm-shifting 5G technology // Rev. in Phys. – 2018. – Vol. 3. – P. 26–31.

4. High performance and stable all-inorganic metal halide perovskite-based photodetectors for optical communication applications / C. Bao [et al.] // Adv. Mater. – 2018. – Vol. 30/38. – P.1803422.

5. Уткина Е.А., Ходин А.А., Чекмарев Е.А. Структурно-морфологические особенности тонких слоев SnS и $Cu_2ZnSnS_4$ для солнечных элементов / Межд. научно-техн. конф. «Опто-, микро- и СВЧ-электроника-2018», Минск, 2018. – С. 30–33.

## ВЕКТОРЫ ИНСАЙДЕРСКИХ АТАК НА ЭЛЕМЕНТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.В. Федорцов

Критически важная информационная инфраструктура отдельно взятых организаций (производств) формирует уникальное пространство для развития инсайдерских атак (ИА) на элементы, эмулирующие информационные объекты (ИО) внутри сегментов соответствующих информационных сетей специального назначения (ИССН) [1, 2]. Такие ИССН, как правило, содержат особую конфигурацию структуры/функционала известных категорий средств: программно-технические средства (hardware); программные средства общего и прикладного назначения (software).

В качестве векторов ИА выступают уязвимости вышеназванных элементов ИССН, которые представляют собой частные цели для получения несанкционированного доступа и последующего несанкционированного воздействия на критические свойства ИО. В ходе ИА происходит эскалация привилегий инсайдера посредством эксплуатации уязвимостей элементов ИССН с применением exploit-инструментов/инструкций, полученных из DarkNet, от внешнего злоумышленника. Это приводит к нарушению установленных политик безопасности и реальному ущербу организации (производству) от воздействия на ИО.

Для решения задачи устранения уязвимостей элементов ИССН приоритетным способом следует использовать риск-ориентированный подход, основанный на методологическом аппарате количественной оценки потенциального ущерба от их эксплуатации инсайдером. Ее выполнению предшествует ранжирование по уровням опасности набора метрик уязвимостей software- и hardware-элементов, собранных из соответствующих баз и матриц безопасности программно-технических средств [2].

**Литература**

1. Федорцов А.В. Пути реализации атак на информационную инфраструктуру критически важных объектов Республики Беларусь // Управл. информац. ресурс.: матер. XIV Междунар. науч.-практ. конф., Минск, 20 декабря 2017 г. – С. 191–193.

2. Федорцов А.В. Матрица безопасности программно-технических средств защиты информации организации // Технич. средств. защит. инф.: тезис. докл. XVII Белорус.-российск. науч.-техн. конф., Минск, 11 июня 2019 г. – С. 71–72.

## БЕЗОПАСНОСТЬ В JAVASCRIPT

И.В. Чибисов, И.А. Клапаток, В.В. Шиманский

JavaScript является самым популярным языком, используемым в веб-разработке. Из-за этого существуют десятки методов, которые используют уязвимости этого языка программирования. Главной целью хакера являются данные пользователей, поэтому они нацелены на файлы cookie, данные сессии, пароли и логины. В основном злоумышленник использует уязвимые поля пользовательского ввода, незащищенные элементы отправки HTTP-запросов, а также пользовательский ввод, который требуется серверной команде. Самые распространенные виды атак это Межсайтовый скриптинг (XSS), Подделка межсайтовых запросов (CSRF) и Серверная JavaScript-инъекция. Все они используют вышеперечисленные уязвимости, чтобы завладеть данными пользователей. Но все уязвимости можно компенсировать и не допустить утечки данных. Изучая методы защиты было установлено, что безопасность использования JavaScript полностью зависит от разработчика, который должен всегда использовать все необходимые методы защиты в своем приложении. Используя поля для пользовательского ввода, разработчику нужно использовать специальный синтаксис escape, также можно использовать экранирование JavaScript и HTML. Чтобы исключить вредоносные HTTP-запросы достаточно в элементы отправки внедрить токены, которые будут генерироваться каждый раз при начале нового сеанса, а сервер будет проверять эти токены

перед отправкой запроса. Также разработчик должен избегать использования и знать такие команды JavaScript, которые являются небезопасными и могут исполнить и скомпилировать код.

Подводя итог можно сказать, что в современных веб-приложениях есть много уязвимостей и вся ответственность за безопасность приложения ложиться на плечи разработчика, который должен разбираться в своем деле и знать основы безопасного использования JavaScript.

**Литература**

1. Форристал Д., Брумс К. Защита от хакеров Web-приложений. – М.: Компания АйТи; ДМК Пресс. – 496 с.

2. Фленов М.Е. Web-сервер глазами хакера. – СПб.: БХВ-Петербург, 2009. – 320 с.

## МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

К.В. Чопик, В.М. Алефиренко

На сегодняшний день информация представляет огромную ценность, и поэтому сам факт получения информации злоумышленником приносит ему определенный доход, тем самым причиняя ущерб организации, чья информационная система (ИС) была скомпрометирована. В связи с этим, вопрос оценки защищенности всей ИС в целом является самым главным. Проведя такую оценку, можно выбрать наиболее эффективную систему защиты для каждого частного случая построения ИС. К основным методам, позволяющим оценить защищенность ИС как на этапе проектирования, так и на этапе эксплуатации, относятся: метод оценки на основе графов защищенности и метод оценки на основе нечеткой логики.

Метод оценки на основе графов защищенности обеспечивает повышение эффективности управления защитой информации в ИС за счет комплексного показателя защищенности и применения графа защищенности, который учитывает действительную структуру ИС [1]. Преимуществом данного метода является то, что с его помощью можно получить количественные оценки уровня защищенности ИС для различных типов угроз. Недостатком метода является то, что для его реализации необходима высокая квалификации персонала и относительно большие временные затраты для оценки уровня защищенности в больших информационных системах.

Метод оценки защищенности при помощи нечеткой логики основан на использовании формализованных качественных понятиях [2]. Однако, при этом остается проблема предварительного определения и выбора следующих параметров: выбор представления лингвистических переменных, определение граничных значений выходных данных, выбор метода дефаззификации. Решение данной задачи требует достаточно высокой квалификации персонала. Вся остальная обработка входных данных проводится системой в виде «черного ящика», то есть на вход системы с нечеткой логикой подаются параметры, выбранные для оценивания, а на выходе формируется определенное управляющее воздействие. Применение данного метода позволяет уйти от субъективности персонала за счет автоматизированной обработки статистики по исследуемым инцидентам.

Таким образом, сочетание рассмотренных методов для оценки защищенности информационных систем позволяет учитывать всевозможные прецеденты информационной безопасности, что в свою очередь позволит с большей эффективностью оценивать их защищенность и более динамично управлять конкретной информационной системой.

**Литература**

1. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности / А.В. Козленко [и др.] // Труды СПИИРАН. – 2012. – № 2 (21). – С. 41–55.

2. Жукова М.Н., Коромыслов Н.А. Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 63–69.

## ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ЦИФРОВОЙ РАДИОСВЯЗИ

С.А. Шабанов

Одним из способов достижения скрытого управления войсками является ограничение использования открытых каналов связи. С этой целью во внутренних войсках МВД Республики Беларусь используются цифровые радиостанции стандарта DMR (Digital Mobile Radio). В данных радиостанциях применяется цифровое кодирование речи. При этом для обеспечения требуемой степени защиты информации необходимо применение шифрования. В радиостанциях стандарта DMR используются встроенные шифраторы речи и предусмотрено два типа шифрования информации (базовая – шифрование с ключом размерностью 16 бит и усиленная – шифрование с ключом 40 бит). Хотя шифрование и защищает от несанкционированного прослушивания, имеются и другие виды вмешательства в работу системы связи. Избежать подобных ситуаций помогает система аутентификация, которая предназначена для определения подлинности радиоабонента по индикационному номеру радиостанции и исключения несанкционированного использования ресурсов системы связи.

В радиостанциях стандарта DMR используется передача специального кода для проверки принадлежности к системе по принципу «свой-чужой». На экране диспетчерского пункта отображается вся информация о работающих в радиоэфире абонентах. С учетом наличия функции дистанционного отключения абонентов диспетчером, данная система показывает свою эффективность. Таким образом, можно сказать, что сочетание цифрового формата передачи информации, системы шифрования и системы аутентификации обеспечивает высокий уровень защиты информации при использовании цифровых радиостанций стандарта DMR в процессе управления войсками. При этом, в процессе формирования базы радиоабонентов, необходимо четко соблюдать все требования, предписанные поставщиками специализированного диспетчерского программного обеспечения.

## ОСОБЕННОСТИ ПРИМЕНЕНИЯ АУДИОСТЕГАНОГРАФИИ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

А.М. Шахмуть, С.Н. Петров

С развитием сетей передачи данных, мультимедийная информация подвергается различным типам атак, по причине пользования незащищенными общественными системами связи. Ежедневно многие тысячи мультимедийных файлов загружаются и скачиваются пользователями. Такие мультимедийные данные, как аудио-данные, занимают большое количество места для хранения и считаются наиболее важным типом мультимедийных файлов, содержащих конфиденциальную информацию. Одним из эффективных решений для обеспечения безопасной передачи звука является стеганография, которая предполагает скрытие важных данных в других данных (контейнерах) без того, чтобы посторонние пользователи смогли определить факт существования исходного сообщения. В результате исследований были предложены различные алгоритмы для встраивания и извлечения сообщения в аудиофайл.

Известна модель, реализованная на основе техники LSB (замена наименее значащего бита). Достоинства метода заключаются в его простоте и сравнительно большом объеме встраиваемых данных. Однако результаты тестирования позволяют увидеть серьезные недостатки. Скрытое сообщение легко разрушить, для чего необходимо записать в один или два младших бита каждого байта аудиофайла нули или единицы, тогда, если аудио не содержала скрытого сообщения, то видимых искажений не появится, в противном случае скрытое сообщение будет испорчено. То есть, те же достоинства, которые используются для сокрытия информации, могут быть использованы и для незаметной борьбы со стеганографией.

Предложенный подход для сокрытия звука объединяет LSB-метод стеганографии и шифрование, чтобы сделать систему более надежной. Чтобы в случае перехвата сообщения-контейнера и возникновения подозрения о существовании скрытой передачи, извлечение секретного сообщения с использованием стандартных способов было затруднено.

**Литература**

1. Замена наименее значащего бита или LSB [Электронный ресурс]. – Режим доступа: http://www.nestego.ru/2012/07/lsb.html. – Дата доступа: 10.05.2020.

2. В. Шрайбман. Стеганография аудиофайла методом LSB [Электронный ресурс]. – Режим доступа: https://ru.bmstu.wiki/Стеганография_аудиофайла_методом_LSB. – Дата доступа: 10.05.2020.

## LSB-СТЕГАНОГРАФИЯ В ИЗОБРАЖЕНИИ ФОРМАТА PNG

А.Г. Шрубиков

PNG формат является наиболее подходящим для LSB-стеганографии. Это объясняется его широким распространением и использованием алгоритма сжатия без потерь [1]. Автором предлагается несколько решений по улучшению последовательного встраивания данных в младшие биты изображения.

Одним из решений является вычисление одного (или двух) наиболее часто встречаемых цветов и дальнейшее невнесение битов полезной информации в выделенные пиксели. Данный метод позволяет избежать изменения младшего бита в однотонном фоне изображения (в случае если он ярко выражен), либо при наличии альфа-канала в прозрачном фоне (#00000000), что будет определенно заметно даже при поверхностном стегоанализе. В случае отсутствии ярко выраженного фона данный метод позволяет внедрять биты полезной информации менее последовательно и меньше изменять частотные характеристики изображения. Недостатком данного метода является уменьшение вместительности медиаконтейнера.

Второе решение затрагивает проблематику внедрения русскоязычного текста. В таблице Юникода любой символ кириллицы соответствует 11-разрядному числу. Учитывая высокую вероятность отсутствия необходимости многих символов Юникода, находящихся по порядку до кириллицы, при внедрении русскоязычного текста в изображение, предлагается составление собственной таблицы кодировки. При составлении данной таблицы необходимо выбрать необходимые символы и расположить их как можно ближе к началу таблицы. Исходя из этого, при проектировании программного обеспечения для сокрытия текстовых данных, можно будет выделять меньше бит под каждый символ и, как следствие, достичь большей емкости медиаконтейнера.

**Литература**

1. Конанович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. – 288 с.

## СКРЫТОЕ ВНЕДРЕНИЕ ИНФОРМАЦИИ В РАСТРОВОЕ ИЗОБРАЖЕНИЕ

А.Г. Шрубиков, О.Б. Зельманский

Для скрытой передачи информации применяется множество различных методов и инструментов. Одним из них является стеганография. Под стеганографией понимают скрытие полезных данных в контейнере таким образом, чтобы неавторизованный пользователь не имел возможности обнаружить факт наличия сообщения. В качестве контейнера может использоваться текст, изображение, аудиофайлы, видеофайлы, а также неиспользуемые биты заголовков полей TCP/IP протокола [1]. К наиболее популярным методам скрытия можно отнести пространственные методы, при использовании которых изменения вносятся в значения пикселей таким образом, чтобы быть незаметными для человеческого глаза, и методы преобразования в частотной области. В настоящей работе рассмотрен метод LSB из первой группы. LSB (Least Significant Bit – наименее значащий бит) метод заключается в изменении младших значащих битов пикселей с целью кодирования в них скрываемого сообщения. Согласно [2] изменение младших битов в каждом пикселе не влияет на восприятие изображения человеческим глазом. Таким образом, алгоритм скрытия информации может выглядеть следующим образом: преобразование скрываемого

сообщения в двоичный код, вычисление его длины, преобразование длины массива в двоичный код, кодирование длины скрываемого сообщения в младших битах первых пикселей изображения, кодирование скрываемого сообщения в последующих битах.

Следует отметить, что более высокую скрытность можно достичь, используя в качестве контейнера зашумленные изображения (фотографии, отсканированные изображения) [2]. Это происходит по причине низкой закономерности используемых цветов. Уменьшить вероятность несанкционированного обнаружения информации возможно благодаря непоследовательному использованию пикселей, например, каждого второго или третьего пикселя. Для оптимизации данного процесса предлагается внедрение в вышеописанный алгоритм условий, которые проверяют частное размера скрываемого сообщения и размера используемого контейнера. В дальнейшем это значение используется для более оптимального распределения информационных битов по контейнеру. Например, если размер информационного сообщения меньше размера контейнера в 24 раза это означает, что для скрытия должен использоваться младший бит составляющей синего цвета каждого пикселя. В случае если сообщение меньше контейнера в 48 раз, возможно использование данного бита через один пиксель и т.д. Наиболее удобным для стеганографии форматом является PNG, так как он использует сжатие без потерь, а также является широко распространенным.

**Литература**

1. Kaur H., Rani J. A Survey on different techniques of steganography // MATEC Web of Conferences. – 2016. – № 57 – 02003.

2. Конанович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. – 288 с.

## КРИПТОГРАФИЯ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Н.В. Яковчик

Криптография – это основа технологии блокчейн, обеспечивающая его стабильную работу. Участники сети могут доверять друг другу, т.к. это гарантируется математически. Этому способствуют такие фундаментальные элементы блокчейна, как хеш-функции и электронно-цифровые подписи [1].

Хэш-функция – это детерминированная функция, на вход которой подается строка битов произвольной длины, а выходом всегда является битовая строка фиксированной длины *n*. Блокчейн состоит из блоков, каждый из которых имеет хэш предыдущего блока. Таким образом получается цепочка связанных объектов. Если какой-то из блоков будет модифицирован, то его хэш не совпадет со значением, записанным в следующем блоке, что будет является признаком вмешательства в систему.

Помимо защиты блоков, хеширование используется в механизме консенсус, который позволяет определить того, кто сможет добавить новый блок в цепочку. Для добавляемого блока выставляется определенное требование к виду его хэша, например, пять последних символов должны быть нулями. Так как изначально нельзя подобрать данные для получения нужного кэша, единственный вариант – это перебор. В новом блоке создается поле (nonce), значение в котором изменяют до тех пор, пока не будет получен нужный хэш.

Для защиты транзакции применяется криптографическая система с открытым ключом [2] (электронно-цифровая подпись). Публичный ключ является номером кошелька, на адрес которого могут отправляться транзакции, которые в свою очередь должны быть подписаны приватным ключом для проверки личности отправителя.

**Литература**

1. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. – М.: Эксмо, 2018. – 256 с.

2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009 – 576 с.

## ДЛЯ ЗАМЕТОК

## ДЛЯ ЗАМЕТОК

*Научное издание*

# ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Тезисы докладов**
**XVIII Белорусско-российской научно–технической конференции**
**(Минск, 9 июня 2020 г.)**

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 01.06.2020. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 10,46. Уч.-изд. л. 9,0. Тираж 100 экз. Заказ 86.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/238 от 24.03.2014, № 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
ЛП № 02330/264 от 14.04.2014.
220013, г. Минск, ул. П. Бровки, 6