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
XVI Белорусско-российской научно–технической конференции
(Минск, 5 июня 2018 г.)

Минск БГУИР 2018

УДК 004.56 (043.2)
ББК 32.973.26–018.2

Технические средства защиты информации: Тезисы докладов XVI Белорусско-российской научно-технической конференции, 5 июня 2018 г., Минск. Минск: БГУИР, 2018. – 108 с.

Издание содержит тезисы докладов, тематика которых посвящена организационно-правовому обеспечению защиты информации, средствам обнаружения и подавления каналов утечки информации, программно-аппаратным средствам защиты информации в компьютерных и телекоммуникационных сетях, методам и средствам защиты объектов, вопросам подготовки специалистов.

ОГЛАВЛЕНИЕ

IMPORTANCE OF RISK DEFINITION FOR IT RISK CONTROL

M.A. Goman

Control of technological and security risks remains an actual problem in business. Problems in risk management include identification of the object of analysis, methods of analysis, incompleteness of information and lack of resources. Therefore, the methods should facilitate risk prioritization issue.

Concept of risk is not uniformly understood in practice and research. Available control frameworks understand the term "risk" differently. Principles of system approach were used to evaluate concepts of risk that we had found in literature. This made it possible to incorporate technological risk management as a subsystem into a wider system of business risk management. IT risk control is meaningful only as a part of overall business risk management. We revealed that the concept of risk is always related to a person (a decision-maker) or group of people who are interested in certain successful solution of their problem. The two key criteria of risk existence are "exposure" and "uncertainty". Ability to recognize existence of risk saves resources. A strong risk concept enables justification of cases where quantitative analysis is a must. Evidently, the term "risk" means a bad event (outcome), not a positive one as some sources ague. Risk metrics should reduce uncertainty and refine probabilities and impacts of events that affect outcomes of the decomposed problem.

IT or security risks exist only in a certain environment and make sense there for a set of human actors during some time interval. Risks are also connected to a problem with at least two alternative solutions, including possible negative outcomes. Risk can only emerge if there is a possibility that the problem will not be solved adequately according to perception of the decision-maker. If we fail to formulate what risk in our context is, the problem can not be addressed effectively.

We propose a new look at the problem of risk control. First, define IT risk for a given situation. Then, identify an owner of the risk, his problem and decision. Risk control should support the risk owner in his decision. Then, determine metrics that show that the level of risk is changing. Such methods and criteria should be found that one could efficiently apply available resources to risk analysis, prioritize risk treatment actions and finally verify the effect of the actions.

To sum up, risk is connected to a business situation and is a multidimensional entity. Standards need update in order to reflect the nature of risk and suggest methods accordingly. This work is the basis for the further work on IT risk analysis methods for business control models.

IMPLEMENTATION OF THE VULNERABILITY MANAGEMENT PROGRAM USING PROJECT APPROACH

S. Joe-Madu, A.M. Prudnik

A vulnerability is defined in the standard as "A weakness of an asset or group of assets that can be exploited by one or more threats" [1]. IT security regulations increasingly are the norm demonstrating a standard of care in protecting sensitive data. To serve this standard, several regulatory bodies have mandated the creation of vulnerability management programs. Examples include: the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Federal Energy Regulation Committee (FERC)

Vulnerability management is comprised of the following activities [3]: identifying / tracking assets (build asset inventory); categorizing assets into groups; scanning assets for known vulnerabilities; ranking risks; patch management; test patches; apply patches; follow-up remediation scan – confirms vulnerability addressed.

The planning phase of the vulnerability management program involves gathering company and regulatory vulnerability assessment requirements, detecting vulnerabilities, and rating and ranking their risk.

The doing phase of the vulnerability management program requires to implement the risk treatment plan. Risks are mitigated to the company's acceptable levels. The plan may include patching systems to acceptable levels, decommissioning systems (removing them from the environment), or applying compensating controls.

The checking phase of the vulnerability management program requires to monitor systems regularly to ensure vulnerability compliance requirements are met. Companies may choose to run the

minimum number of scans required to meet compliance requirements. However, more frequent scanning (e.g. weekly) provides several benefits:

The acting phase of the vulnerability management program uses the data generated from previous phases to improve program. Changes may apply to company security policies, practices and procedures. These changes may result in organizational risk reduction, increased process efficiency and improved regulatory compliance. Common areas of improvement, as outlined in [4].

References

1. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

2. Shanks W. Building a Vulnerability Management Program – A project management approach. SANS Institute, 2013.

3. Foreman P. Vulnerability Management. Auerbach Publications, 2009.

4. Manzuik S., Pfeil K., Gold A. Network Security Assessment: From Vulnerability to Patch. Syngress Media, 2006.

PROTECTION OF SPEECH INFORMATION DURING TRANSMISSION VIA MOBILE NETWORKS

Khomo Khoaba Bigde, E.A. Ogorodnikov, O.B. Zelmanski

With the growing importance of the telecommunication systems and internet, secure transmission of information is crucial [1]. Cryptography helps in providing this much needed data confidentiality by converting data into an unrecognizable form. The decryption techniques allows intended receiver to reveal the contents of previously encrypted data via secrete keys exchanged exclusively between transmitter and receiver. The encryption and decryption techniques can be applied equally to a data in any form such as text, image, audio or video.

In this research the protection of speech information during transmission via mobile networks was focused on. A voice encryption and decryption system was programmed as a real-time software application. C# programming language was used. The NAudio class library, which is an open-source library for controlling audio on Windows-based computers was also applied and evaluated. It can be used with .NET applications using a variety of languages, for the protection of speech (audio) signals the TripleDES algorithm was used.

The software application is based on the following algorithm. The original audio signal is loaded to the wave viewer software and played by a speaker system. The data loaded and displayed on the wave viewer is encrypted and the results as a wave format are stored. After this the encrypted audio is loaded to the wave viewer software, played and recorded by the microphone of another personal computer or a phone. Then the recorded encrypted audio is decrypted to the original audio and played.

Literature

1. Study of the relationship of signal/noise ratio and speech intelligibility in possible points of information leakage / Amakiri Minafuro [et al.] // Technical Means of Information Protection: materials of XV Belarusian-Russian scientific and technical conference, Minsk, June 6, 2017. P. 28.

A MODEL OF MULTI-KEY STEGANOGRAPHIC SYSTEM

P.P. Urbanovich, N.P. Shutko, A.M. Zapała

Recently, research to find new effective methods and tools of increasing the level of confidentiality of transmitted information, as well as protecting of content from unauthorized use are expanded and deepen. Main among these methods belongs to steganography. The steganographic system (steganosystem) – a set of tools and techniques that are used to form a secret channel of information transfer.

The processes of synthesis and analysis of steganographic systems are based on the use of models of such systems. The accuracy of the modeling of the steganographic systems and their investigation to obtain qualitative and quantitative estimates of the reliability of the use

of steganotransformation, as well as the construction of methods for detecting of the information embedded in a container, its modification or destruction are mainly determined by operations based on key's information (as in cryptographic transformations).

We present the formal mathematical description of multi-key steganography system. The proposed model provides using of the main or primary (basic method of data embedding/extraction) and additional keys. As additional keys of the steganographic system we will consider a specific secret value of a set of parameters of a cryptographic or other algorithm used for cryptographic encryption/decryption of a message [1], for redundant encoding/decoding of a message [2] or another operation used in the embedding/extraction of the message as an additional means of enhancing of steganographic resistance of the system.

Literature

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.

2. Multilevel turbocoding schemes on the basis of twodimensional linear iterative codes with diagonal checks/ P.P. Urbanovich [et al.] // Przeglad elektrotechniczny. 2008. Vol. 84, № 3. P. 152–154.

УГЛЕРОДСОДЕРЖАЩИЕ ПОКРЫТИЯ НА ОСНОВЕ ЛЕГКОПЛАВКИХ ЭМАЛЕЙ

А.А. Алексеенко

В настоящее время существуют технологические приемы формирования радиопоглощающих покрытий с эффективным подавлением магнитной или электрической составляющей с различными эксплуатационными характеристиками. В нашем случае были разработаны технологические приемы создания сегментов на керамической или металлической (алюминиевой, титановой) основе, покрытых модифицированным радиопоглощающим покрытием из углерода (на основе графита), активированного, в частности, ионами металлов (или восстановленным металлом). Отжиг таких сегментов в контролируемой газовой среде (аргон, водород) позволяет управлять морфологическими и структурными свойствами получаемых покрытий, а также делать их многослойными с контролируемой толщиной: с целью создания, фактически, микроволновых устройств-поглотителей. На основе сегментов разработанного состава могут быть получены защитные радиопоглощающие конструкции сложного геометрического профиля для стационарных и динамических объектов, стойкие к перепадам температур и слабоагрессивному воздействию внешних сред. Наибольший интерес в этом отношении представляют углеродсодержащие покрытия на «вулканизированной» эмалевой основе. Фактически, свойства покрытий модифицированного состава (например, состава фуллерен-полупроводник) должны быть близки по характеристикам к «идеальному поглотителю», работающему в области широких частот как с магнитной, так и с электрической составляющей внешнего электромагнитного излучения. Потенциальная область применения радиопоглощающих (экранирующих) покрытий разработанного состава – обеспечение электромагнитной совместимости аппаратуры и защиты персонала от электромагнитного излучения в неблагоприятных климатических условиях и слабоагрессивных средах в широком диапазоне рабочих температур. Для разработанных технологических приемов существует возможность получать сплошное внешнее углеродное покрытие, отделенное от металлической поверхности диэлектрическим слоем легкоплавкой эмали (в нашем случае использовались фосфатные эмали). Необходимо отметить, что покрытие может быть получено также в виде искусственно «текстурированного» внешнего слоя, линии рисунка которого состоят из спеченного порошка металла или оксокомплексов металла. Для самих эмалей, наносимых на алюминиевую основу, достижима кратковременная эксплуатация без существенного разрушения структуры покрытия при температурах, не превышающих точку плавления алюминия.

ПОИСК ЗАКЛАДНЫХ УСТРОЙСТВ КОМБИНАЦИОННЫМ МЕТОДОМ

В.М. Алефиренко, В.С. Андрушкевич

Обнаружение, поиск и локализация закладных устройств может осуществляться с помощью различных специализированных приборов, каждый из которых имеет свои преимущества и недостатки при работе в тех или иных условиях состояния электромагнитной обстановки на объекте (в помещении). К таким приборам в первую очередь относятся индикаторы электромагнитного поля, сканирующие приемники и аппаратно-программные комплексы, а также ряд дополнительных приборов, таких как интерсепторы, радиочастотомеры, радиотестеры, анализаторы спектра и др. [1]. Использование в комбинации нескольких видов приборов может повысить эффективность обнаружения, поиска и локализации закладных устройств.

Для экспериментальных исследований были использованы индикатор электромагнитного поля и интерсептор частного производства и портативный частотомер ROGER RFM-31, сканирующие приемники AR-3000A и IC-R5 промышленного производства. В качестве закладного устройства использовался имитатор радиомикрофона, работающий на частоте 509,5 МГц. Поиск и обнаружение радиомикрофона осуществлялось с помощью индикатора поля и интерсептора методом акустической завязки, а локализация – с помощью радиочастотомера и сканирующих приемников. Как показали исследования, захват сигнала радиомикрофона индикатором поля и интерсептором происходил на расстоянии 0,2–1,5 м, а захват (измерение) частоты радиочастотомером – на расстоянии 0,1–0,5 м в зависимости от взаимного расположения антенн радиомикрофона и используемых приборов. После определения радиочастотомером частоты радиомикрофона, что указывало на стабильную работу радиопередатчика в помещении, осуществлялось сканирование сканирующими приемниками только узкого диапазона частот, в который попадала измеренная частота. В результате, по звуковому фону помещения, воспроизводимому динамиком сканирующего приемника, однозначно устанавливалось наличие закладного устройства. Захват сигнала радиомикрофона сканирующими приемниками происходил на расстоянии 30–60 м в зависимости от условий распространения радиоволн (свободное пространство, наличие стен, перегородок).

Таким образом, для обнаружения, поиска и локализации закладных устройств можно использовать комбинацию различных приборов поиска, которая позволяет повысить эффективность обнаружения.

Литература

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. М. : Горячая линия – Телеком, 2013. 240 с.

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ГОЛОСОВЫХ АССИСТЕНТОВ

В.М. Алефиренко, В.В. Костюченко

В современном мире все чаще в новые смарт-устройства внедряются системы голосовых ассистентов, таких как Siri, Alexa и Google Assistant. Все крупные IT компании ведут разработку своих систем и предлагают их на рынке, встраивая в собственное оборудование. На данный момент различные голосовые системы устанавливаются на все смартфоны, некоторые автомобили и умные дома. Голосовые помощники поддерживают управление умными устройствами в доме и офисе напрямую со смартфона, имеют доступ к управлению большинством автомобильных систем. Также голосовые ассистенты уже умеют вызывать такси, оплачивать самостоятельно покупки в интернет-магазинах, отправлять сообщения, совершать звонки, настраивать параметры систем умного дома, записывать сценарии действий пользователя, прокладывать по просьбе пользователя маршруты любым транспортом и т.д. Но все эти возможности несут в себе риски безопасности и конфиденциальности. Устройство, имеющее голосовой помощник, при помощи встроенных микрофонов прослушивает

окружающий звуковой фон и реагирует на поступающие команды. Так как устройства не умеют корректно отличать голос владельца системы от голоса других людей, то любой человек может передать команду на выполнение голосовому ассистенту, например, отправить секретные документы по названному адресу почты. Эта проблема хорошо известна всем компаниям, разрабатывающим системы голосового управления, но без потери функционала для пользователя она пока не решена. Так же известен способ, при котором голосовые команды для ассистентов передаются удаленно и массово. Микрофоны современных устройств умеют улавливать звуковые колебания, неслышные человеку. Это позволяет записывать голосовые команды в любые массовые аудио и видео трансляции. Голосовые помощники интерпретируют услышанные звуки, различают буквы и составляют предложения. Благодаря этому им можно давать любые команды, например, перевести деньги на озвученный счет или зайти на сайт и заполнить форму с личными данными. Такие команды могут быть зашифрованы в ролике на YouTube, вставлены в фильм или сделаны как фоновый шум. На данный момент защитных систем от данных видов угроз не представлено.

Литература

1. Audio Adversarial Examples // University of California, Berkeley, and Georgetown University [Электронный ресурс]. –. URL https://nicholas.carlini.com/code/audio_adversarial_examples (дата обращения: 14.05.2018).

2. Ronan De Renesse – Virtual digital assistants to overtake world population by 2021 [Электронный ресурс]. – URL https://ovum.informa.com/resources/product-content/virtual-digital-assistants-to-overtake-world-population-by-2021 (дата обращения: 14.05.2018).

МОБИЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

В.М. Алефиренко, Ч.Ф. Нгуен

Мобильные системы видеонаблюдения могут широко использоваться на объектах, имеющих небольшие территории или помещения при проведении мероприятий, носящих временный характер, таких как спортивные соревнования, выставки, собрания и т.п. Эффективность таких систем может быть повышена, если они используют компьютерные технологии и возможность контроля и управления по сети Интернет.

Разработанная мобильная система видеонаблюдения предназначена для обеспечения видеоконтроля на охраняемых объектах с использованием компьютерных технологий и управлением по сети Интернет. Система построена на базе компьютерного зрения [1], протоколов MQTT и HTTP. Технология компьютерного зрения позволяет проводить обработку и анализ видеоинформации, что обеспечивает своевременное обнаружение угроз и оперативное реагирование в соответствии с обстановкой. Мозгом системы является одноплатный компьютер, на котором осуществляются обработка видеосигнала (распознавание объектов, отслеживание, обнаружение движения), управление серводвигателями, видеотрансляция с помощью протокола HTTP, ответы на запросы пользователя и оповещение о тревоге с помощью протокола MQTT. Для видеотрансляции используется веб-фреймворк Flask. С помощью Flask и Python, одноплатный компьютер становится сервером видеотрансляции. Доступ к изображениям выполняется с помощью протокола HTTP с веб-браузера или приложения. Компоненты системы включают: одноплатный компьютер Raspberry Pi 3, модуль Pi Camera, микроконтроллер ATmega 328, два серводвигателя и управляющее приложение для персонального компьютера. Программирование реализовано на языках Си, Python и Java. Конструктивно компоненты системы размещены в одном корпусе, на котором имеются соответствующие органы управления, индикации и разъемы для подключения внешних устройств и сети Интернет. Основными преимуществами разработанной системы является невысокая стоимость, мобильность, возможность быстрого развертывания и свертывания на объекте, гибкость размещения отдельных компонентов, адаптация к индивидуальным требованиям пользователя.

Литература

1. Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов. М.: Горячая линия – Телеком, 2012. 184 с.

ВИДЫ ТИПОВЫХ ОБЪЕКТОВ И СИСТЕМ ОХРАНЫ ПЕРИМЕТРА

В.М. Алефиренко, Н.В. Яненко

Защита периметра является важной составляющей комплекса мер безопасности объектов различного назначения. Выбор системы охраны периметра и ее компонентов определяется видом объекта и его особенностями [1]. Можно выделить два вида объектов: стационарный и развертываемый. Рассмотрим три типовых стационарных объекта и один развертываемый.

Таможенный склад. Относится к типу стационарных объектов. Имеет достаточно обширную территорию, расположен за городом вблизи автомобильных дорог и железнодорожных путей, что создает достаточно сильный помеховый фон для датчиков системы охраны периметра. Такой объект будет относиться к категории особо важных объектов, так как содержит достаточно большое количество материальных ценностей и информации. Установлена вибрационная система охраны периметра.

Завод. Относится к типу стационарных объектов. Территория завода расположена в черте города, рядом расположен железнодорожный переезд, который создает помеховый фон. Такой объект будет относиться к категории промышленно-коммерческих, на нем содержится большое количество материальных ценностей, а также документов и чертежей. Установлена емкостная система охраны периметра.

Загородный пансионат. Также относится к типу стационарных объектов. Территория объекта расположена за городом в сосновом бору. Помехи для системы охраны периметра могут создаваться только деревьями и обитателями леса, поэтому уровень помехового фона будет низкий. Объект относится к промышленно-коммерческой категории. Необходимость охраны периметра обусловлена нахождением на объекте людей и их имущества, а также имущества объекта. На объекте установлена инфракрасная система охраны периметра.

Полевой лагерь. Относится к развертываемому типу объектов. Для охраны периметра временного лагеря есть жесткое требование: система охраны должна быть легкой, малого объема, должна быстро устанавливаться и быстро сниматься, желательно, без оставления следов своего пребывания. Время работы такой системы от 8 часов до 3 суток в любых погодных условиях. Территория объекта расположена в лесу, помехи для системы охраны могут быть вызваны деревьями или обитателями леса. На объекте установлена радиолучевая система охраны периметра.

Исходя из сравнительной характеристики объектов видно, что выбор типа системы охраны периметра, и, следовательно, ее компонентов, определяется видом объекта и его особенностями.

Литература

1. Введенский Б.С. Современные системы охраны периметров // Специальная техника. 1999. № 3.

СИСТЕМА ЗАЩИТЫ ОТ СПАМ-БОТОВ В СОВРЕМЕННЫХ ВЕБ-СЕРВИСАХ

К.К. Алёхин, А.С. Шелягович

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – это технология, которая позволяет отличить спам-бота от настоящего пользователя. Их использование позволяет уменьшить поток спама и защитить страницы. Наиболее популярны графические капчи, т.е. в которых пользователю предлагается разобрать текст, который якобы не может прочитать машина, или определить, что изображено на картинке. Однако в последние годы технологии распознавания изображений продвинулись так далеко, что иногда компьютер улавливает зашифрованные смыслы лучше человеческого глаза: пользуясь этим, компьютерам доверяют, например, чтение едва заметных письмен на археологических находках или старых картинах. С распознаванием изображений у машин тоже все обстоит довольно неплохо: ученые, правда, до сих пор просят граждан помочь в анализе больших массивов изображений, но с более простыми задачами программы

справляются самостоятельно – Google и другие поисковики давно умеют искать по картинкам, недавно был запущен Shazam для картин, ИИ неплохо разгадывает даже очень плохие рисунки пользователей. В условиях возрастающей мощи компьютера традиционная графическая капча перестает быть помехой для серьеных злоумышленников и целеустремленных спамеров. Поэтому Google отказался от традиционной интерактивной капчи и вместо этого будет анализировать поведение пользователя самостоятельно. В частности, программа будет фиксировать движения мышки и IP-адрес пользователя. Боты, как правило, передвигают курсор кратчайшим путем, что практически невозможно сделать человеку. Новая капча отображается только в виде окошка, в котором программа сама ставит галочку и сообщает пользователю о том, что он не робот.

Литература

1. Коллинс М. Сетевая безопасность по средствам анализа данных. Чикаго: Университет Чикаго, 2014. 202 с.

2. Столингс, У. Основы сетевой безопасности: приложения и стандарты / У. Столлингс. Изд. 6-е. М.: Массачусетский технологический институт, 2016. 464 с.

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

В.В. Артемьева, Н.С. Карпович

Квантовое распределение ключей предоставляет возможность: можно передавать секретную информацию по открытому (незащищенному) каналу и при этом быть уверенным в том, что ее никто не перехватил.

Цель – обеспечить безусловную безопасность коммуникаций, основываясь на законах физики. Установлено, что существует множество квантовых криптографических алгоритмов – защищенные квантовые каналы, квантовое шифрование с открытым ключем, квантовое подбрасывание монеты, квантовое вычисление вслепую, квантовые деньги – но большинство из них требуют для своего осуществления полноценного квантового компьютера.

Предложено использование квантовых алгоритмов для формирования и передачи ключевой информации в симметричных криптосистемах. Это позволило получить «сырой» ключ, далее следует усиление секретности, исправление ошибок и согласование ключевой последовательности с помощью специальных алгоритмов. Этот метод позволяет двум сторонам, соединенным по открытому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений. Важным и уникальным свойством квантового распределения ключей является возможность обнаружить присутствие третьей стороны, пытающейся получить информацию о ключе.

ПЕРЕХОД К НЕДВОИЧНЫМ ПОМЕХОУСТОЙЧИВЫМ КОДАМ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ

Б.А. Ассанович, Ю.Н. Веретило, В. Рудалеску

В последнее время в литературе особый интерес вызывает реализация надежных криптографических систем на основе нечетких экстракторов (Fuzzy extractor), использующих ненадежные «зашумленные» данные биометрических измерений.

Известно, что если в таких системах возникающий шум, вызванный нечеткостью биометрических данных, является аддитивным и приводит к ошибкам типа замещений, эффективным решением является применение помехоустойчивых кодов с как можно большим расстояния Хэмминга d. Один из подходов при создании такой системы является использование конструкции с коррекцией кодом (Code-offset) [1], образующей вспомогательный безопасный эскиз (Secure Sketch), хранящийся в базе данных. Он применяется вместе с корректирующим ошибки (n, k, d) кодом и представляет смещение (offset) D, «сдвигающее» кодовый вектор X применяемого помехоустойчивого кода, содержащего пароль пользователя S, на значение биометрического измерения B, т. е. $D = B–X$. При последующем биометрическом измерении B’ выполняется вычитание $D–B’= Y$, декодирование Y и получение пароля S’, как правило, совпадающего с S.

Для достижения необходимой эффективности (минимизации вероятности ошибок пропуска и ложного отказа) используют «мощные» корректирующие коды, например, БЧХ, увеличивая расстояние Хемминга для исправления многократных ошибок [2], а также переходят к недвоичным помехоустойчивым кодам (Рида-Соломона, Турбо-коды) [3], где их эффективность может оцениваться расстоянием Евклида.

В данной работе предлагается реализация нечеткого экстрактора на основе схемы так называемого нечеткого обязательства (Fuzzy commitment) [4] с использованием недвоичных турбо-кодов. Предлагаемая схема обладает лучшими биометрическими характеристиками и гибкостью реализации по сравнению с [2, 3] и обладает возможностью выбора типа недвоичного кода, произвольной длины его блока и величины «предыскажения» для достижения необходимой конфиденциальности и безопасности данных.

Предлагаемая схема включает две основные процедуры: регистрация (Enrollment) и аутентификация (Authentication). Данные пользователя из бинарной формы выбранной длины *d* преобразуются в m-ичные числа, где d степень числа m.

На этапе регистрации m-ичный пароль пользователя (Secret Key) *Sm* поступает в недвоичный кодер (Non-binary Encoder), где добавляются избыточные символы для коррекции ошибок, образуя блоки данных *Xm*, которые проходят через *m*-ичный модулятор (Modulator) и вычитаются из блока биометрических квантованных данных *Bq*, образующегося на выходе квантующего преобразователя (Quantizer). Интервал квантования выбирается с учетом мощности используемого помехоустойчивого кода и заданной защищенности данных пользователя. Результирующий блок данных Dm записывается в базу (Data Base) и храниться вместе с хэшом *h*(*Sm*) в ней. На этапе аутентификации новые данные *B'q* суммируются с *Dm* и образуют вектор *Ym*, поступающий в демодулятор-декодер (Non-binary Decoder). Выходом является пароль *S'm*, хэш-функция которого *h*(*S'm*) сравнивается с *h*(*Sm*).

Применение предложенного метода позволяет значительно улучшить основные показатели эффективности биометрических систем на основе нечетких экстракторов.

Литература

1. Dodis Y., Reyzin L., Smith A. Fuzzy extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. EUROCRYPT, 2004. P. 523–540.

2. Ассанович Б.А., Веретило Ю.Н. Биометрическая база данных на основе HOG-структур и кодов БЧХ // Информационные технологии и системы 2017 : материалы междунар. науч. конф. Минск, 25 окт.2017 г. С. 286–287.

3. Maiorana E., Blasi D., Campisi P. Biometric Template Protection Using Turbo Codes and Modulation Constellations. IEEE WIFS, 2012. P. 25–30.

4. Juels A., Wattenberg M. A Fuzzy Commitment Scheme. ACM CCS, 1999. P. 28–36.

СЛОЖНЫЕ СИГНАЛЫ В СВЧ-ДИАПАЗОНЕ

И.В. Баженова

Проблема формирования сложных сигналов в СВЧ диапазоне является актуальной. С развитием электроники СВЧ и созданием класса различных твердотельных приборов (транзисторов СВЧ, диодов Ганна и ЛПД, сложных диодных и транзисторных структур) открылись широкие перспективы в разработке более эффективных устройств и функциональных узлов – модулей приемо-передающих систем и полностью твердотельных РЛС, а также в многоцелевом освоении СВЧ диапазона. Такие научные направления, связанные с вопросами формирования и обработки сложных сигналов, изучением их спектров, разработкой современных РТС с улучшенными тактико-техническими характеристиками являются актуальными и стимулируют проведение экспериментальных работ [1].

В работе исследованы возможности управления твердотельными источниками СВЧ-энергии, показаны возможности современных технических средств формировать сложные сигналы с практически любым численным значением базы. Обычно при использовании простых (импульсов) сигналов для увеличения дальности действия РЛС необходимо увеличивать энергию сигнала. При ограниченной мощности передатчика это можно сделать только за счет увеличения длительности импульса, что приводит к уменьшению точности

измерения и разрешающей способности по дальности, которые определяются длительностью отклика – его основного пика. При использовании сложных сигналов эта противоречивая взаимосвязь разрешима, т. е. можно увеличивать длительность сложного сигнала, его энергию, сохраняя неизменной ширину спектра. При этом максимальная длительность сигнала будет ограничиваться допустимой мощностью передатчика. Поэтому для повышения точности измерения и разрешающей способности по дальности можно увеличивать ширину спектра.

В рамках поставленной задачи, на основе результатов проведенных экспериментов, выполнены численные расчеты корреляционных свойств полученных сложных сигналов, которые имеют тесную взаимосвязь с двухпараметрической функцией неопределенности.

Литература

1. Лущицкий В.В., Савельев В.Я., Ткаченко Ф.А. Анализ работы и расчет основных характеристик генератора на диодах Ганна с варакторной перестройкой частоты // Радиотехника и электроника. 1984. Вып.13. С. 69–73.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

О.В. Базылева, Г.А. Пухир

Развитие высоких технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон или планшет зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Высокая концентрация деловых и персональных данных приводит к тому, что абстрактная стоимость информации перевешивает цену самого устройства.

В то время как мобильные приложения изначально предлагались как инструменты для повышения производительности и информации, рынок быстро расширялся из-за требований пользователей и наличия инструментов для разработчиков. Ежедневно люди оперируют десятками программ на смартфонах. Многие из них передают конфиденциальную информацию, которая может заинтересовать злоумышленников. Исследователи обнаружили присутствие небезопасных приложений практически в каждой отрасли, включая производственные и финансовые услуги. По оценкам экспертов RiskIQ, более 11 % приложений для банковских операций содержат вредоносное ПО или подозрительный код.

К типовым уязвимостям мобильных приложений по отношению к данным пользователей можно отнести:

1. Небезопасное хранение конфиденциальных данных в незашифрованном виде.
2. Слабые серверные элементы управления на клиентском устройстве.
3. Недостаточную защиту транспортного уровня.
4. Инъекцию на стороне клиента, позволяющую реализовать доступ пользователя к произвольному, ненадежному веб-контенту.
5. Слабую авторизацию и аутентификацию.
6. Неправильную обработку сеансов.
7. Реализацию ненадежных входов, позволяющую приложениям общаться между собой, что может быть использовано злоумышленником для атаки.
8. Утечку данных ввода/вывода, обычно используемые для административных или нефункциональных целях из сторонних каналов.
9. Плохое управление криптоключами с возможностью их восстановления.
10. Раскрытие конфиденциальной информации, учитывая, что скомпилированные исполняемые файлы могут быть подвергнуты реверс-инжинирингу.

Представленная проблема демонстрирует важность срочного решения вопроса безопасности мобильных устройств, как с точки зрения пользователей, так и разработчиков.

Со стороны разработчиков необходимо, чтобы каждое приложение разрабатывалось путем тщательного ознакомления с передовыми методами кодирования, а затем постоянно оценивалось для выявления потенциально возможных недостатков. Одним из наиболее эффективных способов повышения безопасности приложений можно отнести защиту сервисов, к которым подключаются приложения.

МАГНИТОСОПРОТИВЛЕНИЕ СПИНОВОГО ВЕНТИЛЯ С АНТИФЕРРОМАГНИТНЫМ СЛОЕМ

Г.Б. Байман, А.Л.Данилюк

Переходы ферромагнетик/антиферромагнетик (ФМ/АФМ) широко используют в спиновых вентилях для закрепления направления намагниченности фиксированного ФМ слоя. Это достигается из-за эффекта обменного смещения, за счет которого происходит смещение петли гистерезиса, или ее расширение (усиление коэрцитивности). Смещение петли гистерезиса в слоистых материалах (структурах), как правило, объясняется тем, что магнитномягкая компонента (слой ФМ) испытывает влияние одной из магнитных подрешеток антиферромагнитной компоненты. Такое влияние называется обменным подмагничиванием или пиннингом.

В работе рассматривалось влияние эффекта обменного смещения на величину магнитосопротивления спинового вентиля. Проведенные расчеты показали, что величина магнитсопротивления существенно зависит от свойств АФМ, величины поля смещения и константы обменной связи. При определенном сочетании параметров возможно увеличения магнитосопротивления спинового вентиля в несколько раз за счет вклада эффекта обменного смещения. Рост величины магнитосопротивления происходит за счет уменьшения обменной константы и роста обменного смещения. Изменение внешнего магнитного поля при этом дает немонотонную зависимость магнитосопротивления, характеризующуюся наличием максимума. При изменении отношения, характеризующего соотношение намагниченностей ФМ слоев и их толщин, указанный максимум сдвигается в область более высоких величин внешнего магнитного поля.

СОЗДАНИЕ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ВОЛОКНИСТЫХ МАТЕРИАЛОВ С СОДЕРЖАНИЕМ АЛЛОТРОПНЫХ ФОРМ УГЛЕРОДА

Е.С. Белоусова, М.С.Х. Аль-Махдави, Л.М. Лыньков

Одним из приоритетных направлений научных исследований Республики Беларусь на 2016–2020 годы является поиск новых композиционных наноматериалов, в том числе на основе аллотропных форм углерода, таких как технический углерод, графен, углеродные нанотрубоки, для различных областей радиотехнической, электронной и оптоэлектронной промышленности. При проектировании углеродосодержащих поглотителей электромагнитного излучения ставятся задачи эффективности подавления сигналов определенного частотного диапазона, уменьшения массогабаритных параметров. При этом одной из проблем является выбор основ для конструкций поглотителей электромагнитного излучения, которые должны обладать физико-механическими свойствами гибкости, прочности, легкости и т. п. С этой точки зрения можно предположить, что волокнистые материалы являются наиболее перспективными. Инкорпорирование в их структуру наноразмерных аллотропных форм углерода (технический углерод, графен, углеродные нанотрубки) может обеспечить увеличение их электропроводимости, следовательно, снизить значения коэффициентов отражения и передачи электромагнитного излучения [1, 2].

По методике, представленной в [1], предлагается использовать водные растворы для инкорпорирования мелкодисперсного углеродистого вещества в структуру волокнистого материала. Получено, что изготовленные образцы поглотителей с инкорпорированными частицами технического углерода имеют коэффициент отражения в режиме короткого замыкания порядка –4…–13,5 дБ, коэффициент передачи –2…–5 дБ в диапазоне частот 4–17 ГГц. Для закрепления частиц углерода в структуре волокнистого материала был использован термопресс с установленным значением температуры 100 °С, при этом материал помещался в конверт из огнеупорной бумаги. Время воздействия температуры составило 5 мин, при этом значения коэффициента отражения и передачи в исследуемом диапазоне частот практически не изменились. В дальнейших исследованиях планируется совершенствовать методику инкорпорирования и закрепления частиц углерода в структуре волокнистого материала.

Литература

1. Белоусова Е.С., Мохамед А.М.А., Аль-Адеми Я.Т.А. Гибкие углеродосодержащие поглотители электромагнитного излучения на основе волокнистых материалов // Докл. БГУИР. 2017. № 2 (104). С. 63–68.

2. Углеродосодержащие гибкие экраны электромагнитного излучения на основе клеевых составов / Е.С. Белоусова [и др.] // Управление информационными ресурсами : материалы XIV Междунар. науч.-практ. конф. Минск, 20 декабря 2017 г. С. 153–154.

ПРИМЕНЕНИЕ УГЛЕРОДОСОДЕРЖАЩИХ МАТЕРИАЛОВ ДЛЯ СНИЖЕНИЯ ЗАМЕТНОСТИ НАЗЕМНЫХ ОБЪЕКТОВ В ОПТИЧЕСКИХ КАНАЛАХ НАБЛЮДЕНИЯ

Е.С. Белоусова, В.В. Позняк, Л.М. Лыньков

На сегодняшний день материалы, позволяющие скрыть объекты от средств технической разведки в видимом, инфракрасном и СВЧ диапазонах являются довольно перспективными. К таким материалам предъявляются строгие требования, такие как легкость, мобильность, прочность. Использование углеродосодержащих композиционных материалов на основе технического углерода и гидрогеля являются перспективными для скрытия объектов специального назначения.

В работе [1] для создания средства снижения заметности наземных объектов предложено использовать технический углерод, представлены методика изготовления композиционных материалов на основе технического углерода и гидрогеля и результаты исследования их свойств ослабления и отражения электромагнитного излучения. Установлено, что экраны электромагнитного излучения на основе композита из гидрогеля с добавлением технического углерода (50 масс. %) обладают коэффициентом отражения –4,6…–5 дБ и коэффициентом передачи –26 дБ в диапазоне частот 8–12 ГГц. Проанализировав спектрально-поляризационные свойства углеродосодержащих материалов в видимом диапазоне длин волн (450…940 нм), можно сделать вывод, что коэффициент спектральной яркости для экрана электромагнитного излучения на основе композита с содержанием технического углерода (60 %) составляет 0,021… 0,23 отн. ед (при изменение угла наблюдения от 0º до 45º). Полученные значения коэффициента спектральной яркости коррелируют со значениями коэффициентов спектральной яркости торфяных низинных почв. При изменении процентного содержания технического углерода в композиционном материале можно изменять значения коэффициента спектральной яркости и рекомендовать использования таких материалов на фоне других поверхностей естественной среды.

Данные исследования позволяют рекомендовать использование данного композиционного материала на поверхности объектов специального назначения, так как позволяют скрыть их на фоне торфяных или подзолистых почв.

Литература

1. Белоусова Е.С., Мохамед А.М.А., Касанин С.Н. Композиционные материалы на основе технического углерода и гидрогеля для скрытия объектов от средств технической разведки // Докл. БГУИР. 2016. № 1 (95). С. 64–70.

ГРАМОТНОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОЦЕНКА И АНАЛИЗ

Т.Н. Беляцкая, В.С. Князькова

Развитие информационного общества основывается, с одной стороны, на инфраструктурной составляющей – волоконно-оптические кабели, безопасные сервера, домены высшего уровня и пр. С другой стороны, создание, реализация и использование программно-технических инноваций невозможно без определенного уровня знаний, навыков в сфере ИКТ. В них огромное значение имеют базовые знания – грамотность – в сфере информационной безопасности (ИБ). На кафедре менеджмента УО БГУИР под руководством

зав. кафедрой, Т.Н. Беляцкой была предпринята попытка оценить уровень грамотности населения Республики Беларусь в сфере ИБ.

Для этого был проведено масштабное исследование населения Беларуси, в котором приняло участие 1500 человек; репрезентативность выборки контролировалась по региональным пропорциям численности населения, пропорциями между городским и сельским населением, пропорциями между мужчинами и женщинами, а также пропорциями между возрастными группами. В спектр задач исследования входили как самооценка респондентов по базовым знаниям в сфере ИКТ, так и базовые вопросы по обеспечению безопасности платежей, выборе паролей, скачивания файлов. Отдельный блок вопросов был посвящен безопасности в социальных сетях. Анализ показал, что в целом уровень грамотности в сфере ИБ не слишком высок. Так, из числа респондентов, которые постоянно пользуются компьютером и сетью Интернет, только 32% респондентов правильно ответили на вопрос: «Вы хотите скачать песню Beatles «Yesterday» и нашли несколько вариантов в Интернете. Какие из них скачаете?». Варианты ответа были: Yesterday-Beatles-Song.scr; Beatles_All_songs.zip; Beatles_Yesterday.mp3.exe; Betles-Yesturday.wma.

Повышение грамотности населения в сфере ИБ является одной из основных задач в свете достижения целей в области информатизации. Для ее решения предлагается создать портал, посвященный основам знаний в данной области.

АСПЕКТЫ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Р.В. Берёзкин, Г.А. Власова

В настоящее время наибольшее распространение получили сетевые системы видеонаблюдения (IP-протокол) по сравнению с аналоговыми (протокол CCTV). Сетевое позволяет обеспечить быструю передачу данных, лучшее качество сигнала и помехозащищенность, такую систему проще масштабировать и интегрировать в существующие системы безопасности крупных и мелких объектов. Базовым методом защиты данных в локальных сетях является аутентификация по имени пользователя и паролю. Этого достаточно, когда сеть видеонаблюдения отделена от локальной основной сети, и посторонние физически не могут получить доступ к ней. В других случаях для повышения безопасности данные должны шифроваться, чтобы посторонние не имели возможность чтения или использования передаваемой информации.

Известно много алгоритмов шифрования. Однако не все они удовлетворяют требованиям, предъявляемым к алгоритмам для систем видеонаблюдения. В современных системах видеонаблюдения требуемая скорость передачи данных от 0,6 до 12 Мбит/с. Поскольку алгоритмы шифрования снижают скорость передачи данных, для видеонаблюдения следует использовать симметричные алгоритмы.

Массовое использование систем видеонаблюдения обусловлено развитием IoT (Internet of things – Интернет вещей). В связи с этим, возникают новые требования к алгоритмам шифрования, а именно: ограниченные вычислительные ресурсы, ценовые ограничения, определенные ограничения на энергозатратность реализации.

Среди известных алгоритмов наиболее подходящими для систем видеонаблюдения являются хорошо изученные DES, AES и ГОСТ 28147-89, а также легковесные алгоритмы PRESENT и CLEFIA. Пропускная способность при использовании алгоритма PRESENT более чем в 4 раза превосходит алгоритм CLEFIA при одинаковой сложности устройства (количестве условных логических элементов, GE). Однако PRESENT менее криптостойкий (длина ключа – 80 или 128 бит), в сравнении с CLEFIA (длина ключа – 128, 192 или 256 бит).

Поскольку в современных условиях длина ключа 128 бит не обеспечивает долговременную безопасность, предпочтительнее использовать алгоритм CLEFIA. Алгоритм PRESENT применим только для обеспечения краткосрочной безопасности.

СКРЫТНАЯ ПОМЕХОУСТОЙЧИВАЯ СИСТЕМА ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ КРИПТОКОДОВЫХ КОНСТРУКЦИЙ

Д.М. Бильдюк, С.Б. Саломатин

Рассматривается встраиваемая стохастическая система связи на основе криптокодовых конструкций. Формирование и обработка сигнала основана на стохастических кодовых конструкциях с криптографической сложностью [1, 2].

Функциональное назначение: передача данных по структурно скрытым радиоканалам; формирование помеховых сигналов со скрытым каналом передачи данных. Общая модель реализации и тестирования использует криптокодовые конструкции блочного и поточного *R*-кода. На приемной стороне применяется декодер максимального правдоподобия блоковых *R*-кодов. Оцениваются корреляционные характеристики, расстояния между вероятностными характеристиками, изменение границы эффективности при изменении длины блокового *R*-кода. Дается сравнение помехоустойчивых свойств блокового и поточного *R*-кода.

Литература

1. Бильдюк Д.М., Саломатин С.Б. Декодирование нелинейного помехоустойчивого кода на базе криптографического алгоритма Rijndael // Докл. БГУИР. 2012. № 8 (70). С. 75–81.

2. Бильдюк Д.М., Саломатин С.Б. Дистанционные свойства нелинейного помехоустойчивого кода на базе криптографического алгоритма Rijndael // Докл. БГУИР. 2012. № 7 (69). С. 105–110.

АКТИВНЫЕ ЭЛЕМЕНТЫ МЭМС НА ОСНОВЕ АНОДНОГО ОКСИДА АЛЮМИНИЯ

С.А. Биран, Д.А. Короткевич, А.В. Короткевич

Устройства на базе микроэлектромеханических систем (МЭМС) широко используются в промышленной электронике, медицине, военной и космической технике. Их функциональные характеристики определяются механическими свойствами материала, на основе которых они сформированы. В настоящее время основным материалом в МЭМС технологии является кремний и его модификации из-за хороших физических и механических свойств. Однако, использование кремния связано с высокотемпературными процессами (500–1200 ºС), что снижает его физико-механические свойства и вызывает в нем высокие механические напряжения, кроме того не всегда можно получить требуемую геометрию элемента. Одним из наиболее перспективных материалов является анодный оксид алюминия (ААО), который обладает хорошими физико-механическими свойствами, которые можно варьировать путем изменения режимов анодирования. Анизотропия травления пленок ААО позволяет формировать объемные МЭМС-элементы с высоким соотношением сторон [1]. Датчики с чувствительным элементом в форме мембраны могут быть сформированы на основе анодного оксида алюминия.

Конструктивно активный элемент МЭМС представляет собой массу алюминия цилиндрической формы, подвешенной на двух консолях из анодного оксида алюминия, свободно перемещающуюся в вертикальной плоскости. В предыдущей работе было установлено, что модуль Юнга свободных пленок анодного оксида алюминия, полученных путем анодирования в растворе на основе щавелевой кислоты, находится в пределах от 26 до 30 ГПа [2].

В ходе исследований было установлено, что добавление одной дополнительной консоли снижает чувствительность на 75 %, а двух – на 90 %. Увеличение толщины пленки анодного оксида на 10 мкм снижает чувствительность на 30 %. Изменяя параметры анодирования, можно варьировать чувствительность активных элементов МЭМС в широком диапазоне значений.

Литература

1. The MEMS handbook / edited by Mohamed Gad-el-Hak. New York: CRC Press, 2002. P. 18–21.

2. Биран С.А., Короткевич А.В., Короткевич Д.А. Механические свойства пленок анодного оксида алюминия активных элементов МЭМС // XIII Белорусско-российская научно-техническая конференция Технические средства защиты информации. Минск, 25–26 мая 2016 г. С. 48–49.

ВЛИЯНИЕ ОБЛУЧЕНИЯ НА СВОЙСТВА МДМ-СТРУКТУР НА ОСНОВЕ АНОДНОГО ОКСИДА АЛЮМИНИЯ

С.А. Биран, Д.А. Короткевич, А.В. Короткевич

Электронные устройства в процессе эксплуатации могут подвергаться различным внешним воздействиям (излучения, вибрация, температура и т.д.). Интерес для исследования представляют свойства материалов в экстремальных условиях.

В данной работе исследовали влияние низких температур и облучения γ-квантами на диэлектрические свойства пленок на основе анодного оксида алюминия.

Конструктивно образцы для исследований представляли собой МДМ-структуры. В качестве основания была выбрана пластина из алюминия толщиной 1,5 мм с пленкой анодного оксида алюминия (АОА) толщиной 50–100 мкм, полученной путем анодирования в растворе на основе щавелевой кислоты. Все образцы были разделены на две группы. В первой группе на алюмооксидное покрытие, в качестве грунтовки, напыляли пленку анодного оксида алюминия толщиной 0,2 мкм, в образцах второй группы грунтовка отсутствовала. В качестве верхнего электрода использовали напыленную пленку алюминия толщиной 1 мкм.

В ходе эксперимента измеряли зависимость электрической емкости от температуры в интервале 77–300 К [1]. После получения характеристик образцы подвергали облучению γ-квантами (параметры источника Co^{60} с $D \approx 2 \cdot 10^{17}$ $см^{-2}$) на воздухе. Время облучения для всех образцов было одинаковым. После этого повторно производили измерение.

В результате исследований было установлено, что величина электрической емкости облученных и необлученных образцов практически не отличается. У образцов без грунтового покрытия во всем температурном диапазоне замечено уменьшение величины электрической емкости. У образцов с грунтовым покрытием уменьшение электрической емкости наблюдается при температурах ниже 160 К, максимальное отклонение 1–1,5 % при 77 К. Незначительное уменьшение емкости связано с образованием в структуре диэлектрика радиационных дефектов, что ведет к уменьшению его диэлектрической проницаемости. Из полученных результатов видно, что МДМ-структуры на основе алюминия и пленок АОА устойчивы к облучению γ-квантами.

Литература

1. Короткевич А.В., Коцаренко В.А., Плешкин В.А. Расширение функциональных возможностей подложек ГИС // Технология и конструирование в электронной аппаратуре. 1993. № 1. С. 3–7.

ОСОБЕННОСТИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ МЕТОДИКИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ОТРАСЛИ СВЯЗИ

В.А. Бойправ, Л.Л. Утин

В работе [1] рассмотрены подходы к разработке программного средства, которое может быть применено в ходе аудита системы защиты информации на предприятии отрасли связи в целях поиска уязвимостей этой системы. На основе сведений об этих уязвимостях определяется перечень угроз, которые могут быть реализованы по отношению к информации, циркулирующей в информационной сети предприятия. Для того чтобы при проведении внутреннего аудита системы защиты информации предприятия отрасли связи оценить риски, связанные с реализацией угроз безопасности информации, предлагается использовать математическую модель, в которой учтены следующие параметры.

1. Весовой коэффициент, соответствующий классу критически важных объектов информатизации (КВОИ), с которыми работают сотрудники аудируемого предприятия (данный параметр может принимать значение от 0,1 до 1).

2. Годовая стоимость элементов КВОИ, которые могут быть подвержены воздействию угроз. Величина этого параметра есть частное от деления цены этих элементов на гарантийный срока их службы, измеряемый в годах.

3. Величина относительной ценности элементов КВОИ, которые могут быть подвержены воздействию угроз (данный параметр может принимать значение в интервале (0;1]).

4. Вероятность возникновения угроз, получаемая на основе матрицы причинно-

следственных связей между уязвимостями и угрозами, в которой должен быть учтен весовой коэффициент, зависящий от стажа работы сотрудника, участвующего в построении этой матрицы.

На основе результатов оценки рисков безопасности информации, циркулирующей в информационной сети предприятия отрасли связи, полученных с использованием предложенной математической модели, может разрабатываться план и очередность выполнения мероприятий, направленных на парирование угроз, а также производиться расчет экономической эффективности этих мероприятий.

Литература

1. Бойправ В.А., Утин Л.Л., Ковалёв В.В. Актуализация разработки программного средства для порведения аудита системы защиты информации организаций электросвязи // Управление информационными ресурсами: материалы XIII Международной научно-практической конференции Минск, 9 декабря 2016 г. С. 181–182.

МЕТОД ОЦЕНКИ НАДЕЖНОСТИ ПРИКЛАДНЫХ ПРОГРАММНЫХ СРЕДСТВ НА РАННИХ ЭТАПАХ ИХ РАЗРАБОТКИ

С.М. Боровиков, С.С. Дик, А.В. Будник

Надежность современных электронных систем обеспечения безопасности, в том числе информационной, зависит от надежности используемого программного обеспечения. Известные методы оценки надежности прикладных программных средств исходят из того, что устранены ошибки языка программирования, т. е. выполнена отладка кода программы и имеются определенные данные о тестировании программы. Однако в большинстве случаев проектировщиков электронных систем безопасности и разработчиков программного обеспечения для этих систем интересует ожидаемый уровень надежности прикладных программных средств еще до написания их программного кода. Возникает вопрос, как спрогнозировать ожидаемый уровень надежности программных средств на этом этапе. Наличие соответствующего метода позволит хотя бы ориентировочно оценить ожидаемый уровень надежности будущего программного средства, что даст возможность определить общую проектную надежность электронной системы безопасности (с учетом как аппаратной части, так и программного обеспечения). Для прогнозирования ожидаемой надежности разрабатываемых прикладных программных средств предлагается подход, основанный на использовании статистической модели работоспособности программных средств. Модель базируется на взятых из отечественной и зарубежной печати обобщенных статистических данных об ожидаемом числе ошибок в разрабатываемом прикладном программном средстве в зависимости от его объема, динамики уменьшения числа ошибок от времени тестирования, профессионального опыта программистов и тестировщиков. На основе указанного подхода разработан метод прогнозирования расчетным способом ожидаемой надежности прикладных программных средств на начальных этапах их разработки.

МОДЕЛИ ДЕГРАДАЦИИ ПАРАМЕТРОВ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ И ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПО ПОСТЕПЕННЫМИ ОТКАЗАМ

С.М. Боровиков, Н.И. Цырельчук, Ю.Е. Велюха, В.В. Хорошко

Деградация функционального параметра полупроводникового прибора (ППП) обуславливает появление постепенного отказа ППП. По мере развития технологии изготовления ППП причины возникновения внезапных отказов могут быть в значительной мере устранены. Постепенные отказы, отражающие внутренне присущие материалам ППП свойства, в частности старение, в принципе исключить невозможно. Этим вызван повышенный интерес к постепенным (деградационным) отказам. Для прогнозирования надежности выборки ППП по постепенным отказам необходимо располагать математической моделью деградации функционального параметра. Возникает вопрос, что собою должна представлять модель, как ее получить и как применить для прогнозирования надежности?

Для имитации деградации функционального параметра выборки однотипных ППП использована модель в виде условного (для заданной наработки) закона его распределения. Коэффициенты модели для конкретной (прогнозируемой) выборки ППП находят по уравнениям в зависимости от заданной наработки и статистических особенностей функционального параметра этой выборки. Уравнения для интересующего типа ППП получают один раз с помощью предварительных исследований выборки данного типа ППП объемом примерно 60…100 экземпляров. О надежности прогнозируемой выборки по постепенным отказам для заданной наработки судят по вероятности нахождения функционального параметра в пределах указанных норм. Прогнозное значение вероятности находят по общепринятым правилам теории вероятности, используя построенный закон распределения функционального параметра для заданной наработки.

ПРОБЛЕМА ДЕЛЕГИРОВАНИЯ ОТВЕТСТВЕННОСТИ НА ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ПЛАТЕЖНЫХ ПРИЛОЖЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

О.В. Бородюк

В настоящее время постоянно растет число пользователей, совершающих финансовые операции посредством мобильных приложений. Согласно результатам исследования, проведенного компанией «Яндекс» осенью 2016 года, 58 % пользователей смартфонов регулярно заходят на сайты и в приложения интернет-магазинов, а также из тех пользователей, которые используют смартфон для выбора товаров, большинство (72 %) имеют опыт и в оформлении заказа с телефона [1]. В связи с тем, что телефоны используются для большего количества задач, то необходимо принимать разумные меры защиты информации от вредоносных атак. Одним из важных аспектов безопасности современных мобильных устройств является наличие прав доступа уровня root. Автором было проведено исследование мобильных платежных приложений, в ходе которого проверялось запускаются ли такие приложения на устройствах с правами root и в случае, если запускаются, оповещается ли пользователь о возможных угрозах. Исследование проводилось на устройствах с операционной системой Android. В ходе исследования были протестированы популярные во всем мире приложения для совершения покупок, а также решения белорусских банков в сфере мобильного-банкинга. Всего было протестировано 17 приложений, среди которых «PayPal», «Amazon shopping», «М-банкинг» (приложение от «Беларусбанка»), «V-banking» от компании «Velcom». Все 17 приложений запустились на устройстве с правами root, 11,76 % – сократили функциональные возможности приложения, 29,41 % – оповестили пользователя о возможных рисках, 35,29 % – никак не прореагировали на наличие прав суперпользователя и 70,59 % – делегировали ответственность на пользователя добавлением новых пунктов в пользовательское соглашение. Результаты исследования показывают, что проблема делегирования ответственности на пользователя становится все более актуальной. Многие компании снимают с себя ответственность посредством добавления дополнительных пунктов в пользовательское соглашение.

Литература

1. Развитие онлайн-торговли в России: покупки со смартфонов // yandex.ru [Электронный ресурс]. – URL: https://yandex.ru/company/researches/2017/mobile_retail (дата обращения: 02.04.2018).

АРХИТЕКТУРА СИСТЕМЫ АНАЛИЗА МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ КЛАССА IaaS

А.И. Бражук

Технологическую основу уровня «Инфраструктура как услуга» (Infrastructure as a Service – IaaS) облачных компьютерных систем составляют системы виртуализации, программно-определяемые сети и хранилища, а также современные методы использования ресурсов. Системообразующий характер обуславливает актуальность проблемы моделирования

информационной безопасности данного уровня [1, 2]. Системы анализа (поддержки принятия решений), построенные на основе предметно-ориентированных моделей информационной безопасности, могут использоваться при проектировании систем защиты и анализе защищенности (детализация существующих риск-ориентированных моделей).

Архитектура системы анализа моделей информационной безопасности включает три подсистемы: база знаний (высокоуровневые и детальные модели), обеспечивающая представление и обработку знаний предметной области; подсистема анализа и защищенности (прикладные и синтезируемые модели), позволяющая потребителям создавать высокоуровневые формальные описания конкретных систем и получать рекомендации по улучшению безопасности или настройке средств защиты; подсистема интеграции с внешними источниками знаний, обеспечивающая актуальность базы знаний.

Предложенная архитектура является ориентированной на модели; также, предполагает функции автоматизированной и автоматической обработки знаний в области информационной безопасности. При этом, используемые модели являются архитектурными моделями в терминах архитектурного описания (ISO/IEC 42010); совместимы с терминологией, используемой в стандартах, литературе и реализациях средств информационной безопасности (ISO/IEC 15408-1).

Основными проблемами реализации представленной архитектуры являются построение иерархий моделей архитектур (типовые компоненты – элементы типовых компонентов) и моделей угроз (типовые угрозы – атаки, уязвимости, злоумышленники, контрмеры, метки безопасности).

Литература

1. Листопад Н.И., Олизарович Е.В., Бражук А.И. Практические аспекты внедрения облачных технологий в учреждении образования // Информатизация образования. 2014. № 2 (74). С. 55–65.

2. Управление программным обеспечением и архитектура отказоустойчивого IaaS-облака на основе универсальных узлов. / Ю.И. Воротницкий [и др.] // Электроника ИНФО. 2013. № 9. С. 21–24.

КОЛИЧЕСТВЕННЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.В. Валаханович, Л.В. Михайловская

Для лиц, принимающих решение в любой сфере деятельности, критично обеспечение оптимального соотношения доступности информации и ее надежной защиты от угроз. Первоочередной задачей управления рисками информационной безопасности становится определение наиболее значимых активов. В ходе анализа ценности активов применяются следующие методы оценки риска: в денежном выражении, вероятностный и балльный, позволяющие определить уровень уязвимости для каждой комбинации информационного актива, а также степень потенциальной опасности угроз.

Для оценки стоимости потерь используется «аддитивная модель» [1], когда информация представляется в виде конечного множества элементов и осуществляется экспертная оценка компонент исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

При использовании вероятностного метода оценивается риск вероятности обхода системы защиты, с целью чего задается формальное описание ее структуры и связности для множества элементов системы защиты и для множества элементов информационных угроз. Математическое описание связности построено на использовании теории графов и алгебраической топологии.

При оценке риска по балльному методу [2] определенным категориям угроз присваиваются значения баллов в зависимости от уровня их воздействия. Также присваивается соответствующий балл уровням уязвимости системы при действии на нее определенной

угрозы. По результатам произведения баллов воздействия на баллы уязвимости оценивается уровень риска для системы при воздействии на нее угроз определенных категорий и типов.

Данные методы позволяют оценить риски информационной безопасности с должным уровнем надежности и спланировать оптимальный комплекс мероприятий по защите информационных активов.

Литература

1. Маслов О.Н. О моделировании риска принятия решений в области обеспечения информационной безопасности // INSIDE. Защита информации. 2011. № 4 (40).

2. DPC/F4.1 Government framework on cyber security – Information Security Management Framework [ISMF], version 3.3. September 2017.

ПОДВИЖНОСТЬ ЭЛЕКТРОНОВ В МОДУЛЯЦИОННО-ЛЕГИРОВАННОЙ СТРУКТУРЕ НА ОСНОВЕ НИТРИДА ГАЛЛИЯ

В.С. Волчёк

Полевые транзисторы с модуляционно-легированной структурой (транзисторы с высокой подвижностью электронов, ТВПЭ) на основе нитрида галлия являются перспективными элементами сенсорных устройств, используемых в системах инженерно-технической защиты объектов. Высокочастотные полупроводниковые приборы требуют больших концентраций носителей заряда с максимально возможной подвижностью. Проблема частично решается в модуляционно-легированной структуре, в которой высокоподвижные электроны с большой концентрацией оказываются пространственно отделенными от положительно заряженных ионов донорной примеси, что ослабляет их рассеяние. Тем не менее, при приложении сильного электрического поля рассеяние электронов на ионизированных примесях возрастает, что приводит к ухудшению подвижности и характеристик прибора.

Для исследования влияния сильного электрического поля на подвижность электронов в ТВПЭ на основе нитрида галлия выбрана структура, состоящая из барьерного слоя $Al_xGa_{1-x}N$, буферного слоя GaN, омических контактов к истоку и стоку и затвора Шоттки. Моделирование выполнялось в программном комплексе компании Silvaco. В расчетах использовалась модель Фарахманда, позволяющая рассчитывать подвижность в зависимости от электрического поля и концентрации донорных примесей [1]. Результаты показывают, что при увеличении процентного содержания алюминия x в барьерном слое (концентрация донорной примеси равна 10^{17} см$^{-3}$) со значения 0,1 до 0,4 концентрация электронов в канале под затвором повышается в 9,8 раз, а подвижность снижается на 19,5 %. Таким образом, для увеличения произведения концентрации на подвижность требуется достижение определенного компромисса.

Литература

1. Monte Carlo Simulation of Electron Transport in the III-Nitride Wurtzite Phase Materials System: Binaries and Ternaries / M. Farahmand [et al.] // IEEE Trans. Electron Devices. 2001. Vol. 48. P. 535–542.

ТЕРМИЧЕСКАЯ СТАБИЛЬНОСТЬ НАНОКРИСТАЛЛИЧЕСКИХ КОМПОЗИТОВ НА ОСНОВЕ ПОРИСТОГО ОКСИДА АЛЮМИНИЯ ДЛЯ ЭЛЕМЕНТОВ ОБРАБОТКИ ИНФОРМАЦИИ

А.И. Воробьева, Д.Л. Шиманович, Е.А. Уткина

Необходимость в создании нанокомпозитных материалов обусловлена современной потребностью увеличения как степени интеграции электронных элементов, так объемов и скорости передачи информации. Дальнейшее уменьшение размеров активных элементов приближается к пределу, связанному с принципиальными физическими ограничениями, и последующее развитие требует привлечения новых решений и подходов, в частности к разработке нанокристаллических функциональных и композиционных материалов (например, «наносборка» с использованием пористого оксида алюминия). Особую роль в свойствах

нанокристаллических композитных материалов, в сравнении с поликристаллическими, играет большая объемная доля границ зерен и, как следствие, высокий уровень внутренних напряжений. Кроме того, поведение частиц, заключенных в поры матрицы, может отличаться от их поведения в свободном состоянии, что обусловлено влиянием межфазной границы «матрица – нанокристалл».

Основная цель исследования состояла в том, чтобы исследовать термическую стабильность магнитных нанокристаллических композитов на основе пористого оксида алюминия (ПОА). Были проведены комплексные исследования состава, структуры и термодинамических характеристик композита из нанонитей (НН) Ni в ПОА мембранах собственного изготовления. Дифференциально-термический и термогравиметрический анализ образцов проводили с использованием синхронного термического анализатора NETZSCH STA 409 PC/PG Luxx (Германия) с вертикальной загрузкой образцов.

Проведенные исследования показали, что фазовые переходы в Ni/ПОА композитах начинаются при температурах выше 250°С, то есть, термостойкость композита ниже, чем термостойкость ПОА мембраны. Механические напряжения возникают при нагревании вследствие (1): различия температурных коэффициентов линейного расширения (ТКЛР) матрицы и частицы; (2): аномального увеличения размеров кристаллитов НН в условиях ограниченного пространства (в длинных узких порах ПОА). При нагреве до 250 °С начинается заметное увеличение среднего размера зерна, а при нагреве до 350 °С нанокристаллическая структура НН трансформируется в суб-микро-кристаллическую.

ОСОБЕННОСТИ ПРИБОРНО-ТЕХНОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ЭЛЕМЕНТОВ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ В ПАКЕТЕ VICTORY

А.Ю. Воронов, И.Ю. Ловшенко

Рассматриваются особенности приборно-технологического моделирования элементов интегральных микросхем в пакете Victory программного комплекса компании Silvaco. Данный пакет позволил фирмам-проектировщикам и научно-исследовательским лабораториям использовать улучшенные модели диффузии примеси, травления и осаждения. Помимо прочего, данный пакет позволяет проектировать приборы в трехмерном пространстве без использования сторонних программ и использует улучшенный код, который организует многопоточность вычислений, что позволяет не только снизить машинно-временные затраты на вычисления, но и дает возможность использовать более продвинутые модели. Например, модель Монте-Карло при имплантации и модель диффузии дефектов при термообработке пластины.

Проведено сравнение результатов моделирования технологического процесса формирования *n*-канального МОП-транзистора с проектными нормами 0,35 мкм в пакете Victory с широко используемым ранее пакетом Athena. Показано, что без проведения калибровки используемых моделей, имеет место большое расхождение в контролируемых параметрах. Например, для *n*-кармана МОП-транзистора глубина залегания примеси при энергии вводимых ионов 405 эВ и дозе $2{,}14 \cdot 10^{13}$ $см^{-3}$ в пакете Victory составила 1 мкм, а в пакете Athena – 0,93 мкм (соответствует расхождению результатов в 8%); поверхностная концентрация в пакете Victory составила $1{,}31 \cdot 10^{15}$ $см^{-3}$, в Athena – $3{,}18 \cdot 10^{14}$ $см^{-3}$ (76 %); после проведения термического отжига пластин при температуре 950 ^{0}С в среде сухого кислорода в течение 30 минут расхождение результатов глубины залегания и поверхностной концентрации составили 6 % и 45 % соответственно. После применения методики калибровки моделей технологических операций расхождение результатов глубины залегания и поверхностной концентрации после имплантации составили 1 % и 15 % соответственно, а после диффузии – 1,5 % и 17 % соответственно. В докладе также рассматриваются методики для увеличения сходимости результатов моделирования реактивного ионного травления, окисления подложек в средах влажного и сухого кислорода.

ОБОБЩЕННЫЙ АЛГОРИТМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА

А.А. Гавришев, А.П. Жук

Защита от несанкционированного доступа тревожных и служебных сообщений в системах безопасности при их передаче по беспроводному каналу связи является актуальной задачей [1]. Авторами в работе [1] на основе перезаписываемых накопителей хаотических последовательностей (НХП) и двух одинаковых генераторов ПСП-2, инициализация которых осуществляется периодически изменяющимся псевдослучайным числом, вырабатываемым генератором ПСП-1, разработан обобщенный алгоритм защищенного информационного обмена в беспроводных системах безопасности, состоящий из следующих шагов.

1. Инициализация генератора ПСП-1 управляющего блока.
2. Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока.
3. Отправка полученного значения одновременно на генератор ПСП-2 управляющего блока и в НХП.
4. Передача произведения ПСП-1 и хаотического сигнала (ХС) из НХП на контролируемый объект.
5. Декодирование в контролируемом объекте полученного сигнала с помощью копии НХП, идентичного НХП в управляющем блоке.
6. Поступление декодированного сигнала в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока.
7. Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок.
8. Декодирование в управляющем блоке полученного сигнала с помощью копии НХП, идентичного НХП в контролируемом объекте.
9. Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в устройство сравнения (УС).
10. Выработка ПСП-2 управляющего блока и ее поступление в УС.
11. Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта.
12. Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма.
13. Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 14 алгоритма.
14. Вмешательство в работу беспроводной системы безопасности должностных лиц.

Литература

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

РАЗРАБОТКА ТОПОЛОГИЧЕСКИХ РЕШЕНИЙ АНАЛОГО-ЦИФРОВЫХ ПРЕОБРАЗОВАТЕЛЕЙ В СИСТЕМЕ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ КОМПАНИИ CADENCE

Я.Д. Галкин, Е.В. Демиденко, А.В. Кунц, А.Т. Русак, И.Ю. Ловшенко

Увеличение скорости и точности обработки информации в устройствах и системах радиоэлектронной и вычислительной техники потребовало разработки большого класса быстродействующих однокристальных схем аналого-цифровых преобразователей (АЦП) широкого применения. Микросхемы преобразователей сигналов по сравнению с цифровыми микросхемами имеют следующие особенности: высокую точность и большую стабильность выходных и входных характеристик в широком диапазоне температур; сравнительно большое число контролируемых параметров в технологическом цикле производства, при контроле готовых схем и механических и климатических испытаниях; высокие требования к контрольно-измерительной аппаратуре по точности и производительности при проверке статических и динамических параметров. [1]

Рассмотрены особенности аналого-цифрового преобразования сигналов датчиков, проведен синтез структурных схем, разработаны схемы электрические принципиальные –

параллельного трехразрядного АЦП, АЦП с промежуточным преобразованием в частоту следования импульсов (АЦП-ППЧ), цифрового преобразователя угловых перемещений и интегрального датчик угла поворота на холловских элементах с компенсацией эксцентриситета магнита. Проведено схемотехническое и топологическое проектирование с использованием системы автоматизированного проектирования микросхем компании Cadence Design Systems, которая является признанным мировой лидером в области разработки средств проектирования электронных систем. Особенностями использования учебной библиотеки компонентов с технологическими нормами 180 нм являются низкое напряжение питания ($U_{пит}$ = 1,8 В) и ток потребления (не более 1 мА), повышенное быстродействие. Проведено сравнение полученных результатов и выработаны рекомендации по использованию данных микросхем.

Литература

1. Быстродействующие интегральные микросхемы ЦАП и АЦП и измерение их параметров / А.-Й.К. Марцинкявичюс [и др.]. М. : Радио и связь, 1988. 224 с.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ПРОТИВОДЫМНОЙ ЗАЩИТЫ МНОГОЭТАЖНЫХ АДМИНИСТРАТИВНЫХ ЗДАНИЙ

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

В соответствии с [1, 2] в зданиях выше 30 м должна быть система противодымной защиты (СПДЗ). При проектировании (СПДЗ) в соответствии [2], состоящей из подпора в незадымляемые лестничные клетки Н2и Н3, а также дымоудаления (ДУ) из коридоров практически всегда перепад давления на закрытых дверях путей эвакуации $P_{ЗД}$ превышает 150 Па, что не соответствует нормам [2]. Это в первую очередь происходит из-за завышенных значений расхода воздуха системы ДУ из коридоров а также подпора в лестницы Н2и Н3.

Поскольку согласно [2] в дверях выхода из коридора на Н2 и Н3 скорость воздуха должна быть не менее 1,3 м/с, то предлагается рассчитывать расход воздуха системы ДУ $L_{ДУ}$ из коридора по формуле: $L_{ДУ} \geq 1{,}3 \cdot H \cdot B \cdot 3600 \cdot n$, где H – высота двери эвакуационного выхода, B – ширина двери эвакуационного выхода, n – количество эвакуационных выходов.

Ориентированное значение $L_{ДУ}$ составляет величину 8500 м^3/ч (что гораздо меньше чем в [2]). В том случае, когда в коридоре 2 эвакуационные двери $L_{ДУ}$ = 17000 м^3/ч. При таком значении $L_{ДУ}$ давление $P_{ЗД}$ превышает 150 Па. Для снижения давления $P_{ЗД}$ в [3] было предложено использовать компенсирующую подачу воздуха в коридор, что повышает стоимость ПДЗ. Для снижения $P_{ЗД}$ предлагается отказаться от подпора воздуха в Н2. Согласно [4], при испытании системы ДУ из коридора необходимо открыть дверь на выход из Н2, чтобы обеспечивать поток воздуха в Н2 и его движение через дверь эвакуационного выхода.

Предлагается отказаться от подпора воздуха в Н2, заменив его открывающимся окном в лестнице Н2. Это окно должно открываться автоматически. Для чего его необходимо оборудовать замком аналогичным клапану дымоудаления, который автоматически открывается при сработке ПДЗ. Кроме того, предлагается отказаться от подпора в тамбур-шлюзы, заменив его на шахту естественной вентиляции без установки в них клапанов дымоудаления.

Литература

1. ТКП 45-2.02-279-2013. Здания и сооружения. Эвакуация людей при пожаре. Строительные нормы проектирования.

2. ТКП 45-4.02-273-2012. Дымоудаление.

3. Галузо В.Е. Дымоудаление: задачи и их решение // Служба спасения 01. 2011. № 9. С. 42–43.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ СИСТЕМ ПРОТИВОДЫМНОЙ ЗАЩИТЫ ГАРАЖЕЙ-СТОЯНОК

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

В соответствии с [1, 2] в гаражах-стоянках закрытого типа следует предусматривать системы вытяжной противодымной защиты (ПДЗ). Удаление продуктов горения

осуществляется системами дымоудаления (ДУ) через дымовые шахты с искусственным побуждением тяги. В [1] приведена методика расчета весового расход дыма *G*, удаляемого из резервуара дыма над загоревшимся автомобилем. Согласно этой методики *G* следует определять по периметру очага пожара, за который принимается периметр большего из размещаемых автомобилей, но не более 12 м. Там же приведен расчет, согласно которому *G* составляет 22970 кг/ч, а объемный расход *L* вентилятора равен 45570 м^3/ч. Очевидно то, что это завышенные значения. Поскольку понятно то, что при сгорании легкового автомобиля не может выделиться такое количество дыма.

В [3] нет указаний о том, что при сработке системы пожарной сигнализации необходимо поднять ворота на въезде в гараж-стоянку. Если при запуске ДУ, обеспечивающего выше приведенное значение *L*, ворота на въезде в гараж-стоянку закрыты, то перепад давления на закрытых дверях $P_{ЗД}$ пути эвакуации существенно превышает нормируемое значение в 150 Па [1]. По рекомендации [1] для снижения этого давления делается компенсирующая подача наружного воздуха, что ведет к увеличению стоимости строительно-монтажных работ.

В ходе проведении аэродинамических испытаний систем ПДЗ гаражей-стоянок при определении фактического значения *L* системы ДУ открываются въездные ворота, чтобы обеспечить приток воздуха.

Предлагается при проектировании автоматики ПДЗ гаражей-стоянок предусматривать подъем ворот и в этом случае никакая компенсирующая подача воздуха не нужна.

В тоже время расход *L* должен быть таким, чтобы обеспечивать незадымление эвакуационных лестничных клеток из гаража-стоянки. В большинстве случаев количество таких лестничных клеток две. Для того, чтобы при пожаре дым не пошел в них необходимо подавать воздух, который при включенном ДУ обеспечивает в соответствии с [1] скорость воздуха в дверном проеме пути эвакуации не менее 1,3 м/с. При размере створки эвакуационной двери (2,0×0,9) м^2 количество воздуха подаваемого в каждую незадымлемую лестничную клетку должно быть около 8500 м^3/ч, объемный расход воздуха *L* удаляемого вентилятором ДУ должен быть кратен количеству эвакуационных выходов из гаража-стоянки. При двух эвакуационных выходах *L* = 17000 м^3/ч. При таком значении *L* компенсирующая подача воздуха не нужна.

Литература

1. ТКП 45-2.02-279-2013. Здания и сооружения. Эвакуация людей при пожаре. Строительные нормы проектирования.

2. ТКП 45-4.02-273-2012. Дымоудаление

3. ТКП 45-2.02-190-2010. Пожарная автоматика зданий и сооружений.

ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ ГРАФЕНА С ПОВЕРХНОСТЬЮ ПОДЛОЖКИ

Д.Ч. Гвоздовский, М.С. Баранова, В.А. Скачкова

Направление использования графена определяет тип материала подложки. В электронике интерес представляют в основном полупроводниковые и диэлектрические подложки. Материал подложки оказывает существенное влияние на электрофизические свойства графена, которые определяют его проводимость [1]. Кроме того, необходимое требование, предъявляемое к материалам подложек – это возможность эффективной адсорбции графена на его поверхности. Благодаря малому расхождению постоянных решеток графена и h-BN (не более 1,39%), гексагональный нитрид бора отлично подходит для использования в качестве подложки в графеновой электронике.

Расчеты периодических структур выполнялись на основании теории функционала плотности (DFT) [2], реализованной в программе Vienna Ab-initio Simulation Package (VASP) [3]. Электронные волновые функции учитывались с помощью базисного набора проекционных присоединенных волн (PAW). Интегрирование в импульсном пространстве осуществлялось по 7×7×1 сетке *k*-точек. Значение энергии обрезания составляет 520 эВ. После нахождения расстояния между графеном и поверхностью нитрида бора проведена структурная оптимизация позиций ионов без изменения объема и формы суперячейки «графен/h-BN».

Установлено, что величина энергии адсорбции не превышает 5,2 кДж/моль, расстояние между слоем графена и поверхностью подложки h-BN составляет 3,28 Å, а также отсутствует перенос заряда с атомов углерода на подложку. Анализ зонной структуры системы «графен/ h-BN» показывает, что закон распределения электронных волновых функций адсорбированного графена не испытывает серьезных изменений. Исходя из этого можно сделать предположение о наличии слабой физической адсорбции графена на поверхности нитрида бора. Связь графена с подложкой существует посредством слабых сил Ван-дер-Ваальса.

Литература

1. Preobrajenski A.B., May Ling Ng, Vinogradov A.S. // Phys. Rev. B 78, 073401 (2008).
2. Kohn W., Sham L. // Phys. Rev. B. 140, 1133–1138 (1965).
3. Kresse G., Furthmuller J. // J. Comput. Mater. Sci. 6, 15 (1996).

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ

А.А. Горелик, В.В. Безмен, О.В. Бойправ

Формирование каналов утечки информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС), может быть обусловлено такими явлениями, как изменение угла падения, изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна, оптическое туннелирование.

Разработана методика оценки защищенности информации, передаваемой по ВОЛС. В ходе реализации этой методики необходимо использовать следующие аппаратные и программные средства: ответвитель-прищепка FOD 5503, оптический модули SFP-1550-ZX и Max Link ML-10GT/D, персональные электронные вычислительные машины (условные обозначения – ПЭВМ 1, ПЭВМ 2 и ПЭВМ 3), программное обеспечение Wireshark.

Алгоритм реализации разработанной методики следующий.

1. Подключение ПЭВМ 1 к оптическому коммутатору.
2. Подключение оптического коммутатора к маршрутизатору, имеющему доступ к сети Интернет.
3. Снятие фрагмента защитной оболочки оптоволоконного кабеля, используемого для соединения ПЭВМ 1 и ПЭВМ 2.
4. Подключение ответвителя-прищепки FOD 5503 к линии связи между портом SFP-модуля коммутатора (передатчиком) и портом SFP-модуля ПЭВМ 1 (приемником). Благодаря этому, часть энергии оптического излучения, содержащего получаемые ПЭВМ 1 ответы (IP-пакеты), выделяется на обработку ПЭВМ 3. Ответвитель-прищепка подключается к тому участку оптоволоконного кабеля, с которого была снята защитная оболочка.
5. Подключение ПЭВМ 3 к линии связи через ответвитель-прищепку FOD 5503 и SFP-модуль.
6. Установка и запуск программного обеспечения Wireshark на ПЭВМ 3.
7. Реализация действий по восстановлению в исходные файлы перехваченного трафика.

В случае, если восстановление нереализуемо, то делается вывод о том, что информация, передаваемая по ВОЛС, защищена, если реализуемо, то составляются рекомендации по повышению уровня защищенности информации. Как правило, эти рекомендации представляют собой совокупность организационных и технических мер. Установлено, что наиболее эффективной организационной мерой является контроль целостности оптического волокна. Из технических мер наиболее рационально реализовывать следующие:

– мониторинг уровня сигнала;
– переключение на другой канал при обнаружении факта несанкционированного доступа;
– систематическое использование оптических рефлектометров;
– применение средств криптографической защиты информации.

АДАПТАЦИЯ ИНСТРУМЕНТАЛЬНОЙ МЕТОДИКИ ОПРЕДЕЛЕНИЯ РАЗБОРЧИВОСТИ РЕЧИ ДЛЯ АРАБСКОГО ЯЗЫКА

С.М. Горошко, С.Н. Петров

На сегодняшний день арабский язык является одним из наиболее распространенных в мире. Общее число носителей по разным оценкам варьируется от 260 до 323 миллионов человек. Как и другие языки, арабский язык обладает информативной функцией. Соответственно, возникает вопрос об оценке защищенности и необходимости защиты речи при передаче по акустическим каналам.

Поскольку анализ, перехваченной с помощью технических средств, речевой информации производит человек-оператор, в качестве показателя оценки защищенности часто используется словесная разборчивость речи. Словесная разборчивость речи определяется как отношение числа правильно понятых слов к общему числу переданных. В ряде работ предлагается использование фразовой разборчивости или даже связанных текстов.

Из числа объективных методов определения разборчивости речи был выбран расчетный метод Н.Б. Покровского, в рамках которого подробно рассмотрены русский и отчасти английский языки. Монография «Расчет и измерение разборчивости речи» вышла в 60-х гг. 20 века и на сегодняшний день хорошо изучена. В критических обзорах метода отмечается факт использования устаревшего оборудовании, а также малой выборки дикторов и аудиторов (5–10 человек). В ряде работ предлагается шаги по совершенствованию этого метода.

Целью данной работы является адаптация метода Н.Б. Покровского для определения разборчивости арабской речи с учетом ее особенностей, например, деления гласных на долгие и короткие т.п., а также с учетом известных недостатков метода, таких как малый размер бригады дикторов и аудиторов. Также исследовался вопрос оценки погрешностей при определении отношения сигнал\шум, одного из ключевых параметров указанного выше метода.

ИСПЫТАНИЯ МАРШРУТИЗАТОРОВ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ТР 2013/027/BY

В.И. Грицкевич, Д.И. Жукова, О.В. Бойправ

Проведены испытания испытаний маршрутизаторов Cisco ASR 920 и Cisco ASR 1001 на соответствие техническому регламенту Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY). Эти испытания представляются актуальными в связи с тем, что маршрутизаторы применяются для построения информационных сетей всех категорий, в том числе сетей, в которых циркулируется информация ограниченного распространения.

В ходе проведения испытаний проверялись гарантийные требования безопасности (полный перечень которых представлен в СТБ 34.101.3-2014), функциональные требования безопасности (полный перечень которых представлен в СТБ 34.101.2-2014) и требования СТБ 34.101.73-2017. Маршрутизаторы Cisco ASR 920 и Cisco ASR 1001 выполняют следующие основные заявленные функции:

- FIA_ATD.1 «Определение атрибутов пользователя» – требует, чтобы для каждого пользователя атрибуты безопасности поддерживались индивидуально;
- FIA_UAU.2 «Аутентификация до любых действий пользователя» – требует, чтобы пользователи прошли аутентификацию прежде, чем функциональные возможности безопасности объекта оценки дадут им возможность предпринимать какие- либо действия;
- FDP_IFF.1 «Простые атрибуты безопасности» – требует, чтобы осуществлялось управление информационными потоками на основании атрибутов безопасности (например, IP-адрес);
- FAU_GEN.1 «Формирование данных аудита» – определяет уровень событий, подлежащих аудиту, и перечень данных, которые должны быть представлены в каждой записи;
- FRU_PRS.2 «Полный приоритет обслуживания» – обеспечивает назначение приоритетов при использовании субъектом всех ресурсов в пределах контроля ФВБО.

На основании полученных результатов можно сделать вывод о том, что исследованные маршрутизаторы соответствуют всем заявленным гарантийным и функциональным требованиям безопасности, а также требованиям СТБ 34.101.73-2017.

Литература

1. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности: СТБ 34.101.2-2014. Введ. 28.01.2014. Минск: Госстандарт Республики Беларусь, 2014. 186 с.

2. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности: СТБ 34.101.3-2014. Введ. 28.01.2014. Минск : Госстандарт Республики Беларусь, 2014. 140 с.

КОРРЕКТИРУЕМЫЕ РЕЗИСТОРЫ МИКРОСХЕМ

Л.И. Гурский

Корректируемые резисторы микросхем (КРМ), изготовленные с использованием плазменных технологий, как правило, имеют отклонения величины сопротивления от заданного как в большую, так и в меньшую стороны. Если R – номинальное сопротивление резистора, γ_R – допустимая относительная погрешность сопротивления, $\gamma_{R\,\text{техн}}$ – технологическая погрешность изготовления, $\gamma_{R\,\text{расч}}$ – расчетное значение допустимой относительной погрешности сопротивления, R_T – номинальное значение исходного технологического сопротивления, D – диапазон корректировки, то получение заданного сопротивления резистора с помощью корректировки возможно при выполнении условия, при котором $R_{T\ max}$ должно быть меньшим или равным R_{max}, определяемым произведением номинального сопротивления резистора R и суммы единицы и расчетного значения допустимой относительной погрешности сопротивления резистора $\gamma_{R\,\text{расч}}$ [1]. Величина номинального значения исходного технологического сопротивления R_T определяется произведением номинального сопротивления резистора и отношения суммы единицы и расчетного значения допустимой относительной погрешности сопротивления к сумме единицы и технологической погрешности изготовления резистора. При изготовлении КРМ с элементом корректировки (ЭК) номинальное значение исходного технологического сопротивления определяется суммой сопротивления основной части резистора $R_{\text{осн}}$ и сопротивления корректируемой части резистора $R^0_{\text{эк}}$. Диапазон корректировки D, на величину которого должно изменяться сопротивление корректируемой части резистора, определяется разностью между заданным минимальным значением сопротивления резистора и полученным в технологическом процессе минимальным сопротивлением резистора. При расчете топологии в качестве расчетного параметра используется коэффициент формы резистора $k_ф$, который определяется отношением сопротивления резистора R к сопротивлению квадрата резистивного слоя $\rho_{\text{кв}}$. Для корректируемого резистора с элементом корректировки ЭК коэффициент формы равен сумме коэффициентов основной части резистора $k_{\text{Фосн}}$ и коэффициента формы элемента корректировки ЭК резистора $k_{\text{ФЭК}}$. Коэффициент формы исходного технологического сопротивления КРМ $k_{\text{ФТ}}$ определяется произведением коэффициента формы резистора $k_{\text{ф}}$ на отношение суммы единицы и расчетного значения допустимой относительной погрешности сопротивления к сумме единицы и технологической погрешности изготовления резистора. В данном докладе рассматриваются методы расчета топологий КРМ прямоугольной, трапециевидной и Т-образной форм, а также решетчатые КРМ и КРМ с распределенным шунтом. Проводится сравнение различных топологий КРМ и даются рекомендации по их применению в качестве элементов и компонентов микросхем для систем защиты информации.

Литература

1. Структура, топология и свойства пленочных резисторов / Л.И. Гурский [и др.]. Минск: Наука и техника, 1987. 264 с.

АСПЕКТЫ ПОДГОТОВКИ ИНЖЕНЕРОВ ПО СПЕЦИАЛЬНОСТИ «ЭЛЕКТРОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

М.С. Гурский

Подготовка специалистов по специальности «Электронные системы безопасности» (ЭСБ) осуществляется в Белорусском государственном университете информатики и радиоэлектроники с 2011 года. Для абитуриентов, делающих выбор в условиях высокой информационной избыточности и отсутствии опыта выбора, первичную значимость имеют имиджевые характеристики престижности ВУЗа и выбранной специальности. Переход на подготовку инженерных кадров по системе 4+2 года обучения требует нового подхода к организации учебного процесса, а также более полной информированности абитуриентов и студентов о реальном качестве предоставляемых образовательных услуг и возможности их дальнейшего трудоустройства. В современных экономических условиях многим приходится менять не только место работы, но и профессию, поэтому студент должен получать такое образование, которое позволит ему в дальнейшем легко осваивать новые профессии и выступать активным субъектом, свободно распоряжающимся своим образовательным капиталом.

Специальность ЭСБ на протяжении всех лет приема пользуется устойчивым спросом со стороны абитуриентов, при этом проходной балл на бюджетную форму обучения составлял 280–320 баллов в разные годы приема. В то же время выпускники данной специальности имеют определенные трудности с трудоустройством, т.е. наблюдается определенный дисбаланс между предложением специалистов с определенным уровнем подготовки и их востребованностью в экономике республики со стороны промышленных предприятий.

Решение задачи рационального поведения потребителей образовательных услуг должен быть комплексным. Одним из направлений его реализации является повышение информационной составляющей относительно обеспечения абитуриентов достаточным объемом информации, формирующей адекватные ожидания как относительно процесса обучения, так и возможности реализации приобретаемого при этом социально-трудового потенциала на рынке труда. Выпускающей кафедре необходимо установить более тесное сотрудничество с предприятиями и компаниями, работающими в области безопасности, учитывать их интересы при подготовке специалистов, оперативно реагировать на их предложения.

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ» В УЧРЕЖДЕНИИ ОБРАЗОВАНИЯ «ВОЕННАЯ АКАДЕМИЯ РЕСПУБЛИКИ БЕЛАРУСЬ»

А.В. Гусаков

Обеспечение информационной безопасности является одним из приоритетных направлений национальной безопасности Республики Беларусь и других развитых стран. Конкурентная борьба с использованием средств и методов информационного противоборства позволяет даже слабым государствам сохранять определенную независимость и возможность давать достойный ответ на недружественные вызовы. С развитием сетевой информационно-телекоммуникационной инфраструктуры любые военные или гражданские объекты независимо от их расположения могут быть подвержены информационному воздействию. Особенно это важно для командных пунктов и автоматизированных систем управления войсками и оружием. В этой связи при подготовке специалистов в области эксплуатация автоматизированных систем обработки информации представляется весьма важным изучение вопросов информационной безопасности, что являлось целью данной работы.

Целью изучения дисциплины «Методы и средства обеспечения безопасности автоматизированных систем обработки информации» является подготовка выпускника к практическому выполнению комплекса мероприятий по внедрению и эксплуатации средств и систем обеспечения безопасности информации на объектах информатизации ВС РБ и органов пограничной службы), а также формированию и контролю политики информационной безопасности.

Опыт преподавания учебной дисциплины у курсантов специальности «Эксплуатация

автоматизированных систем обработки информации» показывает, что изучаемые в рамках лекционных, семинарских и особенно практических занятий вопросы осваиваются с большим интересом. Это способствует подготовке курсантов к правильной организации мероприятий по обеспечению безопасности АСОИ и самостоятельной эксплуатации комплексных систем обеспечения безопасности АСОИ, выработке практических навыков работы с основными средствами защиты информации, формирования политики информационной безопасности.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности. Поэтому развитие и расширение дисциплины «Методы и средства обеспечения безопасности автоматизированных систем обработки информации» представляется весьма вероятной.

Литература

1. Концепция национальной безопасности Республики Беларусь. Утверждена Указом Президента РБ № 390 от 17.07.2001.

2. Жук А.П. Защита информации: учебное пособие. М., 2017. 359 с.

ПРОГРАММА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И.В. Дайняк, Н.Г. Киевец, А.М. Ярук

Программа статистического тестирования битовых последовательностей предназначена для исследования сгенерированной каким-либо способом последовательности битов, в том числе полученной от физического генератора случайных чисел, на предмет пригодности к применению в криптографических системах. В основе программы лежат алгоритмы частотных тестов, тестов подпоследовательностей, тестов аппроксимированной энтропии и других тестов, основанных на статистических характеристиках.

Программа статистического тестирования реализована в виде Windows-приложения на языке Си в среде Bloodshed Dev-C++ версии 4.9.9.2. Основными требованиями при реализации программы были: 1) реализация каждого теста в виде отдельной функции с целью возможности его запуска в отдельности; 2) возможность запуска серии тестов с отслеживанием времени, затраченного на каждый тест и тестирование в целом; 3) получение отчета о тестировании, содержащего для каждого задействованного теста описание критерия прохождения и полученных при этом значений вероятности. В программе реализованы 14 основных тестов входной битовой последовательности и 7 двухуровневых тестов подпоследовательностей.

Интерфейс программы реализован на Windows API в виде простого окна с горизонтальным меню, так как на текущем этапе разработки и отладки повышенных требований к программе не предъявляется. Меню содержит набор стандартных операций по работе с файлами (загрузка битовой последовательности из файла и формирование файла отчета с результатами тестирования), группу основных тестов и группу двухуровневых тестов, обеспечивая тем самым двухуровневое тестирование битовой последовательности [1] с отображением результатов непосредственно в окне программы.

Литература

1. Киевец Н. Г. Статистическое тестирование генераторов случайных чисел электронных пластиковых карт // Математические методы в технике и технологиях : сб. тр. Междунар. науч. конф., Санкт-Петербург, Минск, Самара, окт.–нояб. 2017 г. Ч. 2. С. 19–22.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

М.Ю. Деркач, Ю.С. Харин

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1].

Надежность любой системы криптографической защиты информации (СКЗИ) в значительной степени определяется качеством используемых генераторов случайных и псевдослучайных последовательностей. Генератор, используемый в СКЗИ, должен порождать выходную последовательность, неотличимую от равномерно распределенной случайной последовательности (РРСП) [1]. Для обнаружения отклонения от модели РРСП используются статистические тесты. Статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой случайной последовательностей и РРСП.

Для выявления зависимостей высокого порядка и выявления скрытых зависимостей требуются дополнительные исследования. Основными математическими моделями, используемыми в таких исследованиях, являются марковские модели. В НИИ ППМИ БГУ были разработаны методы и алгоритмы статистического тестирования выходных последовательностей, основанные на цепи Маркова порядка s с r частичными связями (ЦМ(s, r)) и цепи Маркова условного порядка (ЦМУП).

Данный доклад посвящен разработке программного комплекса, реализующий эффективные алгоритмы статистического анализа выходных последовательностей, основанные на оценивании таких марковских моделей, как однородная цепь Маркова, однородная цепь Маркова порядка s, скрытая марковская модель, двойная марковская модель.

Литература

1. Криптология / Ю.С Харин [и др.]. Минск: БГУ, 2013. 511 с.

СВЕТОДИОДНЫЕ СИСТЕМЫ ВЫСОКОЙ МОЩНОСТИ НА АЛЮМИНИЕВОЙ ПЛАТЕ С КОМБИНИРОВАННЫМ ДИЭЛЕКТРИКОМ

Т.Х. Динь, И.А. Врублевский, К.В. Чернякова, А.К. Тучковский

Обеспечение оптимальных температурных режимов работы активных радиоэлектронных элементов является одной из наиболее важных задач при разработке конструкций плат с высоким тепловыделением. Это особенно актуально для светодиодных модулей освещения высокой мощности. Теплота, выделяемая при *p-n* переходе светодиода, проходит от корпуса элемента к теплоотводу, а затем рассеивается в окружающем пространстве. При перегреве светодиода значительно уменьшается эффективность его светоотдачи: падает световой поток, изменяется цветовая температура, и срок службы светодиода сокращается в несколько раз. Поэтому в случае плат с высоким тепловыделением очень важно обеспечить максимальное рассеивание выделяемой теплоты. Решение этой задачи зависит от характеристик печатной платы, которые определяются как конструктивными особенностями платы, так и материалом, из которого она изготовлена. Один из способов снижения уровня тепловой нагруженности плат и эффективного отвода тепла от электронных компонентов является использование печатных плат с алюминиевым основанием.

В данной работе в качестве диэлектрического покрытия плат с алюминиевым основанием использовался комбинированный диэлектрик, состоящий из слоя пористого анодного оксида алюминия и слоя препрега, стеклоткани, пропитанной эпоксидными смолами. С целью повышения теплопроводности в слой препрега вводился керамический наполнитель. Для этого были использованы различные керамические наполнители с высокой теплопроводностью – порошки оксида алюминия, нитрида бора, оксида магния, оксида цинка и оксида титана. Тепловые характеристики печатных плат на алюминиевом основании с диэлектрическим покрытием на основе комбинированного диэлектрика исследовались с помощью термограмм поверхности, получаемых с использованием тепловизионных измерений.

ПРЕДСКАЗАНИЕ ОЦЕНОК CVE УЯЗВИМОСТЕЙ НА ОСНОВЕ ИХ ТЕКСТОВОГО ОПИСАНИЯ

А.К. Доронин, В.А. Липницкий

В мире с каждым днем появляются все новые уязвимости компьютерных систем. Американская национальная база данных уязвимостей CVE содержит около 100000 записей

о различных уязвимостях компьютерных систем почти за 20 лет развития компьютерных технологий [1]. Каждой уязвимости экспертами выставлены оценки от 0 до 10. Кроме того, содержится краткое словесное описание всех уязвимостей. Современные методы машинного обучения позволяют автоматизировать процесс выставления оценок и могут помочь найти закономерности в появлении наиболее опасных (критических уязвимостей). Использовав векторные представления слов (например, использовав словарь алгоритма GloVe [2], представляющий 400000 слов английского языка в 50-мерном векторном пространстве), получена возможность применения методов машинного обучения к задаче автоматизированного выставления оценок на основе их текстового описания. В частности, разработана модель, использующая в своей основе многослойную нейронную сеть с 2 выходами. На вход подается список из слов в виде соответствующих им индексов из словаря GloVe. Далее следуют три сверточных слоя, после них – 3 полносвязных слоя. Между тремя полносвязными слоями имеется слой, исключающий 40 % данных для лучшего обучения нейронов. По существу, построенная нейронная сеть решает задачу бинарной классификации: выход 0 означает оценку меньше 7,5, выход 1 – оценку от 7,5 до 10 включительно. Таким образом мы решили увеличить точность предсказания, оставив вместо 10 классов всего 2. После 10 эпох обучения точность модели (accuracy) на отложенной выборке составила 85 %, площадь под AUC-ROC кривой – 91 %. Дальнейшие исследования, вероятно, могут улучшить данный результат.

Литература

1. National Vulnerability Database [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

2. GloVe: Global Vectors for Word Representation [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ РАБОТА ПО ОЦЕНКЕ УЯЗВИМОСТИ ХРАНЕНИЯ ПАРОЛЕЙ В БРАУЗЕРАХ НА ОСНОВЕ ДВИЖКА CHROMIUM

И.А. Евсеенко

В настоящее время каждый пользователь Интернета имеет пароли для множества учетных записей, начиная от социальных сетей и завершая онлайн-банкингом. Одним из наиболее распространенных способов хранения паролей является система хранения в браузерах. Виртуальная работа рассматривает ситуацию, когда нужно сделать резервную копию всех паролей браузера, или нужно вспомнить давно забытые пароли, которые сохранены в браузере. Однако с другой стороны эта ситуация рассматривается как модель злоумышленника для кражи паролей в браузере.

Браузеры на движке Chromium используют систему шифрования Data Protection Application Programming Interface (DPAPI). В виртуальной лабораторной работе демонстрируются 2 режима: с использованием машинного ключа и с использованием ключа пользователя. Предусмотрена демонстрация принципа работы DPAPI, суть которой заключается в следующем. Приложение обращается к операционной системе задавая параметры Mysecret и Entropy. На выходе получаем BLOB. Приложение сохраняет его, а в дальнейшем, при необходимости, расшифровывает. DPAPI также включает криптопровайдер – это набор алгоритмов для хеширования, шифрования, ключевого обмена и ЭЦП в форме модуля и криптопровайдер объединяет их. Например, в РФ приняты ГОСТовские алгоритмы, поэтому если передать его системе, то вместо стандартных AES, SHA, RSA будут использоваться Российские ГОСТы шифрования. Все это настраивается в реестре. Для DPAPI нет разницы с какими алгоритмами работать, что делает систему универсальной.

Оценка уязвимости по перехвату и расшифровке паролей предусматривает два варианта выполнения: с использование существующих программ и написание студентами программы для расшифровки паролей как на языке высокого уровня, так и на скриптовых языках.

В данной работе рассмотрены возможные негативные последствия использования системы хранения данных в браузерах для авторизации и проведена оценка уязвимости с разработкой специализированного программного обеспечения в рамках лабораторных работ по дисциплине «Защита информации» специальности 09.03.04 «Программная инженерия» БРУ.

ОХРАНА ОБЪЕКТОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

А.В. Железняков

Все более усложняющиеся требования к надежности охраны объектов, предопределяют применение все более серьезных систем, комплексно решающих эту задачу. В процессе развития охранных систем выявилась тенденция к интеграции различных подсистем, обеспечивающих безопасность в единой системе. Основой для создания такого рода продуктов стало расширение возможностей вычислительной техники в управлении системами безопасности, обработке, хранении и передаче различных данных.

Существует множество моносистем, с помощью которых решаются разные задачи безопасности. Однако гарантировать надежную защиту человека, объектов и информации от всего комплекса возможных угроз ни одна из них не в состоянии. Решение этой проблемы во внедрении интегральных комплексов, объединяющих различные подсистемы с общими техническими средствами, каналами связи, программным обеспечением, базами данных.

Объединение систем безопасности на программно-аппаратном уровне позволяет:

– минимизировать капитальные затраты на оснащение объекта за счет уменьшения аппаратной и программной части;

– снизить объем поступающей информации и сделать ее более наглядной;

– автоматизировать принятие решений для типовых ситуаций; существенно уменьшить вероятность ошибочных действий оператора;

– повысить защищенность системы от внешнего воздействия, устойчивость ее к разрушению.

При современной организации охраны объектов вся сложнейшая аппаратура связывается в единую систему. В этом случае любой датчик обнаружения, видеокамера, шлагбаум или турникет функционируют не каждый сам по себе, а является элементом единой системы безопасности, гарантирующей невозможность преодоления линии охраны, соблюдения режима на объекте, а также контроль за несением службы.

Таким образом, применение интегрированных систем позволяет при организации системы охраны объектов добиться высокой надежности работы всего комплекса, реализовать сложные алгоритмы взаимодействия оборудования, максимально исключить влияние человеческого фактора и эффективно использовать силы и средства караулов, войсковых нарядов, подразделения охраны, администрации охраняемого объекта.

ИССЛЕДОВАНИЕ ПОГЛОЩЕНИЯ В ТОНКИХ ПЛЕНКАХ ДИОКСИДА КРЕМНИЯ

В.М. Жердецкая, Е.В. Телеш

Наиболее перспективной является обработка и передача информации в оптических линиях связи. Главные их преимущества – высокие плотность и быстродействие при передаче сигнала, а также повышенная степень защиты передаваемой информации за счет локализации оптического излучения внутри световода. В интегральной оптике по планарным тонкопленочным световодам передается лазерное излучение, следовательно, необходимо, чтобы материал световода имел низкие потери на поглощение и рассеяние.

Синтез тонких пленок диоксида кремния осуществлялся осаждением из ионных пучков, формируемых ускорителем с анодным слоем в режиме ионно-пучкового фокуса [1]. Этот метод позволяет получать покрытия с высокими плотностью и адгезией. В данной работе проведено исследование влияние технологических факторов на коэффициент поглощения k пленок SiO_2. В качестве рабочих газов использовались, смесь моносилана с аргоном (5 % SiH_4+95 % Ar) и кислород. Пленки наносились на неподвижные подложки из кремния и стекла. Измерение k осуществлялось на спектрофотометре Horiba Jobin Yvon в диапазоне 200…850 нм.

Установлено, что определяющее влияние на коэффициент поглощения имеет парциальное давление кислорода в рабочем газе. При низком содержании кислорода пленки обладали высокими показателями поглощения, что свидетельствует о недостаточном

окислении атомов кремния. Покрытия, полученные при больших скоростях нанесения, обладали и меньшим поглощением. Уменьшение энергии ионов в пучке также способствовало снижению k до 0,002. Как правило, увеличение температуры подложки стимулирует процессы химического взаимодействия между кремнием и кислородом, однако при слишком высокой температуре (320°С) происходил рост k, что можно объяснить десорбцией кислорода с поверхности подложки. Измерение спектров поглощения показало, что покрытия, полученные при $T_п$ = 250 °С, обладали минимальным поглощением (k = 0,0005) [2].

Литература

1. Технологические процессы и системы в микроэлектронике: плазменные, электронные, электронно-ионно-лучевые, ультразвуковые / А.П. Достанко [и др.]. Минск, Бестпринт, 2009. 200 с.

2. Titova V.M. Influence of substrate temperature on characteristics of silicon dioxide received deposition from ion beams // The Youth of the 21st Century: Education, Science, Innovations. The 1st Int. conf. for students, postgraduates and young scientists. Vitebsk, 4th Dec.2014. P. 58–61.

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ В ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

А.П. Жук, Е.П. Жук, А.А. Гавришев, А.Ю. Муравьев

Существующие и перспективные защищенные телекоммуникационные технологии предполагают использование широкополосных каналов связи со сложными шумоподобными сигналами (СШПС) [1]. Использование данного подхода обеспечивает ряд преимуществ [2].

Применение ансамблей многофазных ортогональных сигналов (АМФОС) возможно не только в радиоканале, но и в оптической среде. Например, в [3] разработано устройство, позволяющее передавать M-арный символ с псевдослучайной перестройкой интенсивности свечения фотоэлемента. В случае использования достаточно представительного количества ансамблей СШПС требуемого объема, вполне возможно реализовать их стохастическое применение, которое позволит повысить структурную скрытность телекоммуникационных систем. Для стохастического применения АМФОС в телекоммуникационных системах, помимо спектральных и корреляционных свойств, большое значение имеет количество используемых ансамблей. В предлагаемом докладе разработан подход к оценке количества получаемых вариантов АМФОС, описываемых собственными векторами бидиагональных Эрмитовых матриц. В работе получено выражение, определяющее верхнюю границу количества АМФОС, получаемых с использованием рассматриваемой модели.

Литература

1. Применение сложных сигналов в системах радиосвязи и управления / С.С. Кукушкин [и др.] // Современные тенденции развития науки и технологий. 2015. № 2–2. С. 94–96.

2. Бабков В.Ю., Вознюк М.А., Никитин А.Н. Системы связи с кодовым разделением каналов. СПб.: СПбГУТ, 1999. 120 с.

3. Людоговский Д.А., Филатов В.В. Проект «Световой канал передачи информации на основе сложных сигнально-кодовых конструкций». URL: http://nttm2016.ru/?p=17&pr=704. (дата обращения: 10.01.17).

ТЕСТИРОВАНИЕ СЕТЕВЫХ СКАНЕРОВ УЯЗВИМОСТЕЙ: OPENVAS, NESSUS, RAPID7 NEXPOSE

А.Ф. Жукевич

Для тестирования сетевых сканеров уязвимостей авторами был смоделирован тестовый стенд, в состав которого вошли виртуальные машины с указанными выше сканерами уязвимостей и виртуальная машина Metasploitable [1] (тестирование эксплойтов и поиск уязвимостей в операционной системе Linux и сетевых сервисах). В ходе исследования проведено тестовое сканирование каждым из сканеров виртуальной машины Metasploitable и проанализированы полученные результаты.

Конфигурация сканирования:

– OpenVAS (версия 9) запускался в режиме сканирования «Full and fast»;

– Nessus (версия 7.0.0) запускался в режиме «Advanced Scan»;

– Rapid7 Nexpose (версия 6.5) запускался в режиме «Full audit»;

– сканирование производилось с использованием атрибутов доступа.

Результаты сканирования:

– OpenVAS: обнаружил 352 уязвимости, из них: High (высокий уровень) – 126, Medium (средний уровень) – 127, Low (низкий уровень) – 21, Log (информативный уровень) – 78;

– Nessus: обнаружил 397 уязвимостей, из них: Critical (критичный уровень) – 26, High (высокий уровень) – 92, Medium (средний уровень) – 129, Low (низкий уровень) – 13, Log (информативный уровень) – 137;

– Rapid7 Nexpose: обнаружил 307 уязвимостей, из них: Critical (критичный уровень) - 80, Severe (серьезный уровень) – 197, Moderate (средний уровень) – 30.

На основании проведенного тестирования, лучшее качество сканирования по количеству опасных (Critical/High/Medium/Severe) уязвимостей показал сканер Rapid7 Nexpose (277). Наибольшее количество информативных (Low/Log/Moderate) уязвимостей обнаружил сканер Nessus (150).

Литература

1. Metasploitable // sourceforge.net [Электронный ресурс]. – URL: https://sourceforge.net/ projects/ metasploitable/?source=typ_redirect (дата обращения: 02.05.2018).

МЕТОДЫ ОРГАНИЗАЦИИ КОНТРОЛЯ ДОСТУПА ПРИ ОЦЕНКЕ СЕБЕСТОИМОСТИ ИТ-ПРОЕКТОВ

А.Д. Зайков

Рассмотрим процесс разработки ИТ-проекта. В упрощенном виде проекты выглядят так: заказчик высылает задание, программисты оценивают, сколько уйдет на выполнение задания времени и средств, далее согласуют это с заказчиком и получают необходимое финансирование, затем приступают к выполнению проекта. Данный процесс чаще всего можно встретить в небольших командах разработки или небольших проектах, где каждый новый релиз выходит регулярно [1].

В больших проектах, в которых участвует сразу несколько команд разработки, обнаружить внутренние проблемы не так просто. Эффективность и качество разработки зависят от ряда факторов: продуктивность разработчиков, стабильность релизов, гибкость проекта, уровень и способы взаимодействия между заказчиком и разработчиками. Использование инструментов управления и грамотной методики расчета себестоимости ИТ-проекта позволяет руководству компании и клиенту держать руку на пульсе проекта и иметь всегда достоверную информацию о том, как справляется команда с задачами на проекте, а также оценить степень готовности продукта.

Разработка и применение новой методики расчета себестоимости ИТ-проекта позволит оптимизировать техническую базу, подготовить оценку сроков и затрат, произвести качественную и количественную оценку рисков, создать план проекта, своевременно отслеживать эффективность производимых работ. Но полученные данные должны быть видны только руководящим лицам компании, т.к. являются конфиденциальными и не должны быть обнародованы рядовым сотрудникам компании. Система Atlassian JIRA позволяет организовать контроль доступа, подсчитать данные о себестоимости и трудозатратах на ИТ-проектах, а также ограничить видимость этих данных при помощи кастомизации прав доступа пользователей, создании дополнительных экранов для определенных групп пользователей, а также с помощью заскриптованных полей.

Литература

1. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Манн, Иванов и Фербер, 2013. 544 с.

ЗАЩИТА ЦИФРОВЫХ СТРУКТУР ОТ НЕСАНКЦИОНИРОВАННОГО ВНЕДРЕНИЯ

Л.А. Золоторевич, А.В. Павлова

В связи с высокими темпами роста объемов производства цифровых устройств в настоящее время особую остроту приобретает проблема нарушения авторских прав [1, 2]. Ущерб от пиратства и других угроз в области производства аппаратного обеспечения составляет около 4 млрд. долларов в год, что примерно в 10 раз превышает ущерб от пиратства в области программного обеспечения [2]. Кроме пиратства появляются новые виды угроз, такие как внедрение в проект дополнительных вредоносных несанкционированных операций, изменяющих функциональное наполнение системы, внедрение механизмов деградации схемных решений с целью нарушения системы синхронизации, приводящих к нарушению временной согласованности путей распространения сигналов, и, в конечном итоге, к сбою системы, включение средств для получения конфиденциальной информации (к примеру, получение криптографических ключей) через порты контроля и к подрыву безопасности и др. [3, 4].

Очевидно, что после изготовления интегральной схемы проверить ее на наличие внесенных искажений, дополненной функциональности можно путем перепроектирования «по прототипу», восстанавливая поэтапно логику устройства и сравнивая с правильным образцом. При этом восстанавливается проект, реализованный в схеме, и сравнивается с моделью исходного проекта. Этот метод обеспечивает высокую вероятность обнаружения искажений, но время и стоимость, необходимые для выполнения перепроектирования, непомерно высоки.

Одной из известных методик защиты исходных кодов программ от обратного проектирования является обфускация, основной задачей которой является затруднение понимания функционирования программы. К сожалению, применение методов обфускации теряет свою актуальность в случае языка VHDL, так как результаты их применения не приводят к изменению конечного результата синтеза, и структурные реализации устройств до и после обфускации выглядят одинаково [2].

В докладе для блокирования преднамеренных искажений структурных реализаций цифровых устройств применяются известные методы и средства технического диагностирования. Предлагаемый метод заключается в изменении логической структуры путем включения дополнительных элементов и внедрении во входную последовательность встроенных ключей, уникальных для данной схемы.

Литература

1. Security analysis of integrated circuit camouflaging / J. Rajendran [et al.]. // ACM SIGSAC conference on Computer & communications security. Germany, Berlin. 04–08 November, 2013. P. 709–720.

2. Сергейчик В.В., Иванюк А.А. Методы лексической обфускации VHDL-описаний // Information Technologies and Systems 2013 (ITS 2013): Proceeding of The International Conference. Minsk, 24th October 2013. P. 198–199.

3. Benchmarking of hardware Trojans and maliciously affected circuits / B. Shakya [et al.] // Hardw. Syst. Secur. (HaSS). 2017. № 1(1). P. 85–102.

4. Hardware Trojans: Lessons learned after one decade of research / K. Xiao [et al.] // ACM transactions on design automation of electronic system. 2016. Vol. 22, No.1. Article 6.

ПРИМЕНЕНИЕ КРЕАТИВНЫХ МЕТОДОВ В ОБУЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.В. Зубик, Н.Л. Черкас

Современные образовательные технологии вуза должны опираться на следующие принципы: приоритет мышления над запоминанием, активная познавательная деятельность, партнерские отношения преподавателя со студентом, интерактивные формы организации учебного процесса, сотрудничество. Это вызвано радикальным изменением спроса на рынке труда, критичного к компетенциям выпускника вуза, его способности действовать в условиях высокой неопределенности и быстрой динамики. В новых условиях необходимо делать ставку на когнитивные технологии обучения, позволяющие обеспечить эффективное понимание обучающимися реального мира, успешную адаптацию к жизни в информационно

перенасыщенной среде и интеллектуальное развитие. Рост хакерских атак и киберпреступлений, необходимость надежной защиты информационного актива компаний делает профессию специалиста по информационной безопасности одной из самых востребованных на рынке труда. Традиционная форма преподавания дисциплин, в которых делается упор на организационные и правовые методы, обычно не вызывает энтузиазма у студентов. На помощь приходят творческие технологии, прежде всего тризовские.

Так, метод «маленьких человечков» применим для моделирования злоумышленных атак на информационные ресурсы компании и планирования адекватных контрмер. Метод РВС развивает творческое мышление при построении надежной системы информационной безопасности предприятия. Системный оператор используется при анализе эволюции средств промышленного шпионажа для прогнозирования каналов утечки ближайшего и отдаленного будущего. Таблица основных приемов разрешения противоречий помогает при проектировании системы защиты компьютерных сетей. Опыт показывает, что студенты позитивно воспринимают деловые игры на базе творческих технологий. Внедрение тризовских методов обучения в учебный процесс позволяет выработать у студента умение ориентироваться в меняющихся условиях, навыки анализа нестандартных проблемы, самостоятельной разработки и реализации управленческих решений, что в конечном итоге позволяет существенно повысить уровень и качество профессиональной подготовки в целом.

Литература

1. Экономическая безопасность предприятия (фирмы) / В.Б. Зубик [и др.]. Минск: Вышэйшая школа, 1998. 391 с.

2. Nesbor K. Arbeit in Gruppen.Projektarbeit. – Kompetenzentrum «Hochschuldidaktik fur Niedersachsen» an der TU Braunschweig. 2010.

РЕАЛИЗАЦИЯ ШИФРОВАНИЯ С ЭЛЕМЕНТАМИ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Н.С. Иванин

Схема шифрования с элементами подписи (шифрование с ЭП) была предложена в [1] для одновременного решения задач конфиденциальности и аутентификации. Эта схема как правило является частью систем, использующих инфраструктуру с публичным ключом. В таких системах пользователи регистрируют свои публичные ключи вместе с удостоверяющим центром, которые являются независимыми между собой в отличии от разделяемых ключей в системах с симметричным шифрованием (в таких системах у пользователей хранится одинаковый ключ). При шифровании с ЭП для защиты коммуникации пользователю необходимо получить публичный ключ второго пользователя из удостоверяющего центра и зашифровать сообщение.

В качестве схемы была использована схема шифрования с ЭП без использования сертификата, основанная на использовании эллиптических кривых без вычисления функции пересчета пар. Эта схема основана на схеме Барбосы-Фашима, описанной в [2]. Такой подход позволяет шифровать сообщения любой длины и использовать одноразовый ключ симметричного шифрования. Используемая в схеме хэш-функция является устойчивой к коллизиям.

Полученная система состоит из 3 частей: сервера генерации ключей(СГК), отправителя и получателя. Сначала СГК вычисляет параметры, которые будут затем использованы в схеме шифрования. После чего пользователь на своей стороне вычисляет свой публичный ключ. На третьем этапе происходит извлечение частичного приватного ключа. Эта операция выполняется на сервере генерации ключей на основе идентификатора пользователя. Затем полученный приватный ключ и публичный ключ присваиваются пользователю также на основе его идентификатора. С помощью публичного и частичного приватного ключей пользователь зашифровывает сообщение и отправляет его в канал связи. Получатель с помощью своего публичного и полного приватного ключей расшифровывает и верифицирует полученное сообщение.

Литература

1. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost(Encryption) // Crypto'97. 1997.

2. Barbosa M., Farshim P. Certificateless Signcryption // ACM symposium on Information, computer and communications security. 2008.

РЕШЕНИЕ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н.А. Искров, Д.В. Лящук

В докладе представлен обзор наиболее актуальных угроз информационной безопасности (ИБ) и основных направлений использования искусственных нейронных сетей (ИНС) при решении задач обеспечения ИБ. Описаны основная теория построения ИНС и их принцип работы.

Наиболее актуальные угрозы по мнению специалистов в области ИБ: внедрение в сеть предприятия вирусного ПО; простота реализация и распространенность DDoS-атак; снижение эффективности автоматизированных методов защиты от спама; сложности в поиске и идентификации уязвимостей ИБ; возникновение новых способов вторжения. Поэтому следует обратить внимание на перспективные методы защиты информации, в частности, на теорию ИНС.

Преимущества ИНС в решении задач ИБ: в процессе обучения ИНС могут быть выявлены новые сведения, закономерности, использование которых возможно для коррекции топологии сети, входных данных, для получения более эффективной защиты; после обучения ИНС входной сигнал становится нечувствительным к небольшим колебаниям при правильном построении архитектуры ИНС и верном выборе качества обучения; ИНС способна обратить внимание на те сведения, которые являются несущественными для интеллектуальной системы защиты.

Основные направления внедрения ИНС в защиту информации: обнаружение вторжений и защита от DDoS-атак; криптографические методы защиты информации, автоматизация процессов криптоанализа; проведение испытаний подсистем и оборудования систем защиты, моделирование возникновения внештатных ситуаций; прогрозирование шаблонных данных с целью выявления аномалий в классификации или кластеризации операций.

ДЕТЕКТИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ СЛЕПЫМ МЕТОДОМ

А.М. Кадан, И.А. Сазановец

Стеганографические методы позволяют скрыть одну информацию, сообщение, в другой, контейнере. В работе в качестве контейнеров рассматриваются изображения. Для реализации стеганографического сокрытия информации существует множество алгоритмов. И, зная использованный в конкретном случае стегоалгоритм, можно написать программу детектирования скрытого сообщения. В работе рассмотрен метод детектирования стеганографической информации в случаях, когда алгоритм сокрытия неизвестен. Такие способы в стегоанализе называются слепыми. И их использование возможно благодаря тому факту, что внедрение информации в контейнер оставляет после себя искажения.

Решаемая задача является задачей бинарной классификации, так как нужно, имея некое изображение, определить, содержит ли оно скрытое сообщение или нет. Для ее решения предлагается использовать методы машинного обучения. Исходное изображение раскладывается на три цветовых канала: красный, зеленый и синий. Для каждого канала строится трехуровневое двумерное вейвлет-разложение (используется вейвлет-функция Хаара) [1]. Из полученных коэффициентов разложения берутся аппроксимационный, вертикальные и диагональные коэффициенты. В частотных плоскостях этих коэффициентов вычисляются моменты третьего и четвертого порядков (коэффициент асимметрии и эксцесс). Полученные моменты рассматриваются как данные входного вектора (dataset’a) для работы

искусственной нейронной сети. В работе был использован многослойный перцептрон с двумя скрытыми слоями. На первом слое 90 нейронов, на втором – 20. Результаты обучения сети показали возможность успешного детектирования до 70 % случаев наличия информации, скрытой в графических изображениях с использованием трех выбранных стегоалгоритмов.

Литература

1. Абденов А.Ж., Леонов Л.С. Использование нейронных сетей в слепых методах обнаружения встроенной стеганографической информации в цифровых изображениях // Ползуновский вестник. 2010. № 2. С. 221–225.

ВОССТАНОВЛЕНИЕ ЗАШУМЛЕННОГО ТЕКСТА С ПОМОЩЬЮ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ

М.А. Кадан

Генерирующие состязательные сети (GAN, Generative Adversarial Networks) [1] явились эффективной моделью в создании контента с помощью методов искусственного интеллекта. Особенность GAN в том, что они обучаются создавать синтетические данные, подобные эталонным данным. Классическим примером использования GAN является построение сети, которая анализируя изображения рукописных цифр, учится генерировать новые изображения с нуля – по сути, в этом случае мы учим сеть «писать».

В работе ставилась задача обучения GAN способности «читать» искаженную текстовую информацию. Предполагается, что мы располагаем набором цифровых изображений плохого качества (подготовленных при отсутствии оптической стабилизации, плохой резкости, в условиях плохой освещенности, низкой разрешающей способности и т.д.), содержащих текстовую информацию. Необходимо добиться путем обучения GAN улучшения качества таких искаженных текстов, которое позволит восстановить текст.

В качестве эталонного множества было использовано множество печатных латинских букв, представляющих различные компьютерные шрифты. Была сформирована обучающая выборка, включающая примеры написания отдельных латинских букв. Обучающая выборка представлена набором битовых аналогов для графических монохромных изображений: буквы размером 20×20 пикселей вписаны в квадрат 28×28 и отцентрированы вокруг центра масс.

Проведенный эксперимент позволил сгенерировать на основе зашумленных текстов более 25000 букв, которые модель ACGAN (Auxiliary Classifier Generative Adversarial Network) [2] посчитала неотличимыми от букв, представленных в обучающей выборке. Несмотря на использование производительной вычислительной системы, эксперимент потребовал значительных временных затрат.

Литература

1. Generative Adversarial Networks / Ian J. Goodfellow [et al.]. arXiv:1406.2661.

2. Augustus Odena, Christopher Olah, Jonathon Shlens. Conditional Image Synthesis With Auxiliary Classifier GANs. arXiv:1610.09585.

РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И ТЕХНОЛОГИЙ ОТКАЗОУСТОЙЧИВОСТИ

Камил Ихаб Абдулджаббар Камил, М.Б. Абросимов

Системы предотвращения вторжений – это программные или аппаратные системы сетевой и компьютерной безопасности, которые обслуживают распределенные информационные системы, обнаруживают информационные вторжения или нарушения политик безопасности и автоматически защищают от подобных нарушений. Ввиду роста номенклатуры информационных угроз и сокращения времени реализации внешних вторжений для распределенной вычислительной системы возникает необходимость в сокращении времени выявления и противодействия всей номенклатуре информационных угроз. Поскольку при самых неблагоприятных реализациях информационных угроз от распределенных

информационных систем требуется соблюдение надежности и безотказности, то данные условия обеспечиваются преимущественно за счет аппаратного и программного резервирования. Пусть дана распределенная информационная система, для которой необходимо обосновать состав и технические параметры подсистем резервирования (в рамках технологии отказоустойчивости) и определить параметры системы предотвращения вторжений. Для данной информационной системы моделируются экстремальные режимы функционирования по внешним и внутренним рабочим нагрузкам, а также вся известная номенклатура внешних информационных угроз. В отсутствии системы предотвращения вторжений, аппаратного и программного резервирования информационной системы отмечаются снижения эффективности ее функционирования при сочетании предельных значений диапазона рабочих нагрузок и реализаций всей номенклатуры внешних угроз. Экспериментальным путем подбираются параметры алгоритма управления параллельными вычислениями системы предотвращения вторжений на уровне данных и решаемых задач, благодаря которым добиваются своевременного определения угроз и выбора эффективных мер по противодействию им. Пострадавшие в результате реализации информационных угроз элементы информационной системы заменяются на время их восстановления на резервные элементы, которые функционировали до этого в зеркальном режиме, но без коммуникации со внешними абонентами информационной системы. Эффективность защитных мероприятий за период моделирования определяется как отношение предотвращенного ущерба информационной системе (в денежных единицах) к сумме стоимостей системы предотвращения вторжений и технологии отказоустойчивости с учетом аппаратного и программного резервирования информационной системы. По результатам имитационного моделирования обосновываются требования к системе предотвращения воздействий с параллельными вычислениями и к составу системы аппаратного и программного резервирования, реализующей технологию повышения отказоустойчивости.

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ NFC

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информации является NFC (Near field communication) – коммуникация ближнего поля либо ближняя бесконтактная связь. Это технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на близком расстоянии; анонсирована в 200 4г. Эта технология является простым расширением стандарта бесконтактных карт, которое объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC и, таким образом, совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах. NFC – это беспроводная дистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель. Инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены [1]. Но у данной технологии есть и минусы, например, эксплойт 0day, подслушивание (так как это радиосигнал), модификация данных (например, устройствами глушения RFID), атака с использованием ретрансляции и т.д. Исходя из вышеизложенного, можно сделать вывод о том, что NFC на сегодняшний день является весьма небезопасным протоколом, с помощью которого в том числе и передаются банковские данные. В связи с этим риск потерять деньги весьма велик. На сегодняшний день это самая распространенная технология в данном сегменте и остается только надеяться, что платежные данные не попадут третьим лицам.

Литература

1. Near Field Communication (NFC) Technology and Measurements [Электронный ресурс]. – URL: www.rohde-schwarz.com (дата обращения: 18.05.2018).

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ WPA2

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информациив сетях Wi-Fi является протокол WPA второго поколения. WPA2 заменил WPA. WPA2, который требует тестирования и сертификации Wi-Fi Alliance, реализует обязательные элементы IEEE 802.11i. Со стандартом 802.11i вся цепочка модуля безопасности (вход в систему, обмен полномочиями, аутентификация и шифрование данных) становится более надежной и эффективной защитой от ненаправленных и целенаправленных атак. Стандарт 802.11r является модификацией стандарта 802.11i. Данный стандарт был ратифицирован в июле 2008 года. Технология стандарта более быстро и надежно передает ключевые иерархии, основанные на технологии Handoff (передача управления) во время перемещения пользователя между точками доступа. Стандарт 802.11r является полностью совместимым с WiFi стандартами 802.11a/b/g/n. Также существует стандарт 802.11w, предназначенный для усовершенствования механизма безопасности на основе стандарта 802.11i. Этот стандарт разработан для защиты управляющих пакетов.Стандарты 802.11i и 802.11w – механизмы защиты сетей WiFi стандарта 802.11n [1]. Но в данной технологии, как и, естественно, во всем есть недостатки, а именно: слабая стойкость пароля на взлом, отсутствие прямой секретности (дешифровка по разделенному ключу), hole196 (по GTK), атака KRACK (Key Reinstallation Attack) и т.д. Также 16 октября 2017 г. эксперты по бесопасности сообщили, что WPA2 официально взломан и больше не может обеспечивать необходимый уровень безопасности. Исходя из вышеизложенного, можно сделать вывод о том, что WPA2 на сегодняшний день является весьма небезопасным протоколом, которым люди вынуждены пользоваться, так как альтернатив пока нет. С другой стороны, в январе 2018 года Wi-Fi Alliance сообщила, что ведутся работы над новым протоколом WPA3. Остается надеяться, что все эти недостатки будут устранены в новой версии.

Литература

1. Geier, J. WPA Security Enhancements. 2003. 137 p.

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА БАЗЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Е.В. Кармаз, Г.А. Пухир

Для того чтобы обезопасить информационную систему, ряд организаций регулярно проводят тестирование на проникновение в рамках аудита информационной безопасности, что позволяет получить объективную оценку возможности осуществить несанкционированный доступ к ресурсам корпоративной сети или сайта. Процесс тестирования на проникновение является моделированием реальных действий злоумышленника с целью поиска уязвимостей системы защиты. Эта услуга позволяет получить независимую оценку и экспертное заключение о состоянии защищенности информации ограниченного распространения.

Технологии тестирования на проникновение могут осуществляться на базе технических методов и/или социотехнических методов, а также с применением методов социальной инженерии. С их помощью осуществляются санкционированные попытки получения несанкционированного доступа к корпоративной сети и защищаемым активам целевой организации. Методы, как правило, направлены на пользователей конечных систем и позволяют определить реакцию персонала в штатных и нештатных ситуациях, уровень знаний персонала о требованиях безопасности. К некоторым из таких методов можно отнести:

1. Фишинг (побуждение пользователей к вводу конфиденциальных данных (например, паролей) на фальшивой веб-странице легального сервиса.
2. Троянский конь (побуждение пользователя к открытию писем с вредоносными вложениями за счет целевых сопроводительных писем, звонков, наименований файлов и др.).
3. Претекстинг (моделирование определенного сценария, предполагающего вход в доверие к пользователю (за счет предварительного сбора данных об организации, отдельных работниках и их зонах ответственности), с целью побудить выполнить определенное действие).

4. Дорожное яблоко (подбрасывание в общедоступных местах организации (лифт, столовая, парковка) инфицированных носителей информации с мотивирующими к их запуску логотипами/бирками/именами файлов).

После окончания тестирования, специалистами проводится сбор и обработка данных. Часто заказчик хочет знать, кто именно попался на ту, или иную уловку теста. Однако данная информация не передается руководству компании, т.к. проводится тестирование не одного человека, а группы лиц. Соответственно, речь идет об информационной системе, как о едином целом. Исследования показывают, что «человеческий фактор» остается одной из самых распространенных угроз информационной безопасности. Для снижения рисков, связанных с этим обстоятельством, используются различные технические и административные механизмы защиты. Один из них – повышение осведомленности работников, в области информационной безопасности.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ХЭШ-ФУНКЦИИ SHA-256 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич

Криптографическая хэш-функция SHA-256 описана в документе RFC 4634 [1] и предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется в различных приложениях, связанных с защитой информации, а также в большинстве криптовалют. В указанных приложениях возникает необходимость высокопроизводительных аппаратных реализаций SHA-256. В докладе рассматривается полностью конвейерная реализация хэш-функции SHA-256 для одного блока данных (512 бит) на базе FPGA.

Характерной особенностью алгоритма SHA-256 является длинная цепочка последовательных сложений при вычислении новых значений переменных A и E. Для уменьшения числа сложений в одном такте реализации и, следовательно, повышения тактовой частоты конвейерного процессора вычисление переменных E-H на такт опережает вычисление переменных A-D. Кроме того используется предварительное вычисление сумм W_t, K_t, H и D. Одна ступень конвейерного процессора производит вычисления за один такт частоты синхронизации. Общее число ступеней конвейера с учетом 64 раундов алгоритма SHA-256 и завершающего сложения со значением вектора инициализации равно 67.

Характеристики реализации по отчету средств синтеза пакета ISE 14.7 для кристалла FPGA семейства Kintex7 XC7K160T-3: 27477 триггеров секций, 35161 просмотровая таблица (LUT), тактовая частота – 352 МГц.

При обработке сообщения, длина которого превышает один блок SHA-256 необходимо либо последовательно включить требуемое число процессорных ядер для реализации полностью конвейерного вычислителя, либо организовать итеративные вычисления на одном процессорном ядре, коммутируя с помощью мультиплексора выходные данные процессора на его вход требуемое число раз.

Литература

1. RFC 4634. US Secure Hash Algorithms (SHA and HMAC-SHA). [Электронный ресурс]. – URL: https://tools.ietf.org/pdf/rfc4634.pdf (дата обращения: 26.04.2018).

ДОСТУП К ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Р.В. Кислинский

Под информацией ограниченного распространения в Республике Беларусь понимаются государственные секреты, т. е. сведения, защищаемые государством в целях предотвращения их несанкционированного распространения и создания угрозы национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан.

Что касается перечня сведений, составляющих государственные секреты Республики Беларусь, то он определен как совокупность категорий сведений в области экономики,

политики, экологии, оперативно-розыскной деятельности, военной сфере и других жизненно важных сферах деятельности, несанкционированное распространение которых создает или может создать угрозу национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан. Существенной мерой защиты государственных секретов является порядок допуска к ним лиц, которым она необходима для выполнения соответствующих функций. Прежде всего, этот порядок регламентируется Законом Республики Беларусь «О государственных секретах» и Положением о порядке предоставления допуска физическим лицам к государственным секретам, утвержденном Постановлением Совета министров Республики Беларусь 10 апреля 2004 года № 400. Закон «О государственных секретах» ограничивает возможность физических лиц, не достигших восемнадцатилетнего возраста, на доступ к государственным секретам со степенями секретности особой важности и совершенно секретно, за исключением лиц, достигших семнадцатилетнего возраста и поступивших в учебные заведения, где для обучения необходим доступ к государственным секретам.

Цель принятия различных мер по защите информации – обеспечить такой режим работы с информацией, при котором доступом к информации будут иметь только имеющие соответствующий уровень доступа.

Литература

1. Постановление Совета министров Республики Беларусь «Об утверждении положения о порядке предоставления допуска физическим лицам к государственным секретам» 10 апреля 2004 г. № 400.

2. Закон Республики Беларусь от 19.07.2010 г. № 170-З «О государственных секретах».

ВОПРОСЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ВОЕННЫХ ГОРОДКОВ

А.Н. Коваленко

Для каждого военного городка должна разрабатываться, на основе общих требований, своя собственная система безопасности, исходя из положений которой, разрабатывается проект оснащения объекта инженерно-техническими средствами охраны, специальными и программно-аппаратными средствами защиты. Для решения задач и проблем выбора структуры и состава комплекса инженерно-технических средств охраны необходимо, проанализировать возможные варианты действий нарушителя. Исходя из анализа возможных действий нарушителя, составляются варианты его моделей, которые и принимаются за основополагающий фактор выбора тактики защиты объекта.

При разработке проекта оборудования инженерно-техническими средствами охраны военных городков, помимо гаммы технических факторов, необходимо учитывать факторы, определяемые поведением нарушителя.

Возможность нарушителя найти маршрут, не блокированный средством обнаружения, должна быть исключена. Для предотвращения прохода нарушителя должны быть блокированы все возможные маршруты движения нарушителя. Состояние физических преград, имеющих большую стойкость и в связи с этим не блокированных средствами обнаружения, должно периодически контролироваться патрулями или системой видеонаблюдения.

Для увеличения вероятности обнаружения подготовленного и технически оснащенного нарушителя, организовываются полностью скрытные рубежи охраны. Для предотвращения возможности имитации работы средств обнаружения, соединительные линии системы сбора, обработки и отображения информации должны иметь физическую и сигнализационную защиту коммутационных шкафов, коробок и т.п. При прокладке кабелей предпочтение следует отдавать скрытой проводке в закладных устройствах, обеспечивающих дополнительное экранирование и инженерную защиту. Правильный выбор системы и способа охраны и своевременность действий должностных лиц обеспечит надежную охрану объектов военного городка.

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. 367 с.

АУДИТ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Т.Р. Колесова, Е.С. Белоусова

Для защиты информации в информационных системах необходимо проводить постоянный аудит безопасности. В настоящее время приказом Оперативно-аналитического центра при Президенте Республики Беларусь № 64 от 11 октября 2017 г. предъявляются следующие требования по обеспечению аудита безопасности в информационных системах: определение состава и содержания информации о событиях безопасности, подлежащих регистрации; сбор, запись и хранение информации о событиях безопасности в течение установленного срока хранения, но не менее шести месяцев; мониторинг (просмотр, анализ) информации о сбоях в механизмах сбора информации и о достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями; осуществление мониторинга (просмотра, анализа) событий безопасности уполномоченными субъектами информационной системы.

Для реализации данных требований можно использовать системы сбора и обработки данных событий информационной безопасности. В настоящее время на территории Республики Беларусь сертифицированы следующие системы: ArcSight Enterprise Security Manager, IBM Security Qradar SIEM, AccelOps, FortiAnalyzer, Efros Config Inspector. На мировом рынке наиболее популярны первые две системы.

ArcSight ESM поддерживает широкий перечень разнообразных источников событий, выполняет нормализацию на очень высоком уровне, имеет широкие возможности тонкой отладки, кастомизации и мощный корреляционный функционал. Однако присутствуют и минусы - сложность первичного изучения продукта и его высокая стоимость. IBM Security Qradar SIEM имеет более слабый корреляционный функционал, его возможности тонкой отладки и кастомизации ограничены, но зато он обладает более простым и понятным интерфейсом. ArcSight ESM необходимо использовать крупным организациям ввиду его гибкости и богатого функционала. IBM Security Qradar SIEM рационально использовать организациям поменьше, которые не готовы заниматься тонкой настройкой системы и которым не нужна специфичная гибкость платформы для реализации основных функций.

Литература

1. О внесении изменений в некоторые приказы Оперативно-аналитического центра при Президенте Республики Беларусь [Электронный ресурс]. – URL: http://pravo.by/upload/docs/op/T61703911_1507928400.pdf (дата обращения: 14.05.2018).

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ НА СТОРОНЕ БРАУЗЕРА ПОЛЬЗОВАТЕЛЯ

Е.А. Криштопова, О.С. Медведев, А.В. Кистюк

По многочисленным исследованиям более 80 % веб-сайтов содержат критические уязвимости, вероятность автоматизированного заражения страниц уязвимого веб-приложения вредоносным кодом составляет сегодня приблизительно 15–20 %.

Обеспечение безопасности веб-приложений – это объемный процесс, который включает выполнение действий как на уровне заинтересованных сторон, так и на уровне отдельных компонентов системы функционирования веб-приложения. Остановимся на аспектах обеспечения безопасности веб-приложения на уровне компьютера и браузера пользователя.

Так как на компьютер и браузер пользователя данные для веб-приложения поступают из недоверенного источника, то обеспечить их полноценную безопасности невозможно. В этом случае средствами обеспечения безопасности на стороне браузера являются применение правила ограничения домена, использование песочницы (Sandbox) для тестирования и работы с недоверенными или разрабатываемыми приложениями, включение блокировки вредоносных сайтов, применение механизмов аутентификации, включение изоляции вкладок, обеспечение безопасности и смягчения угроз использования компонентов веб-приложения (например, Flash, Java и др.) и дополнений.

Литература

1. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. – URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_en.pdf (дата обращения: 11.05.2018).

2. Евсеев Д. Введение в тему безопасности веб-приложений [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/Д.Евтеев_Введение_в_тему_безоп_веб_прилож.pdf. (дата обращения: 11.05.2018).

КОНТРОЛЬ БЕЗОПАСНОСТИ В КЛИЕНТ-СЕРВЕРНЫХ ПРИЛОЖЕНИЯХ ПРИ ИСПОЛЬЗОВАНИИ ФРЕЙМВОРКА MICROSOFT SIGNALR НА ОСНОВЕ КЛИЕНТСКИХ ГРУПП

В.В. Кузнецов

При разработке клиент-серверных приложений в системах информационной безопасности острой ставится задача запросов клиента к серверу, особенно учитывая проблемы связанные с несанкционированным доступом в базу данных, отправку специфических аргументов серверу и других.

Целью настоящей работы явилась разработка подхода контроля безопасности запросов клиентов к серверу.

Фреймворк Microsoft SignalR [1], обеспечивающий двустороннее взаимодействие в клиент-серверных web-приложениях позволяет на стороне сервера (backend-side) применять атрибуты клиентских групп для классов, обеспечивающих API (Application programming interface) клиентов к серверу, в результате чего исключается необходимость проверять права клиента при обработке запросов. Клиентские группы, такие как например «Пользователи» и «Администраторы» хранятся на машине (ПК) выполняющего функции сервера в разделе «Управление компьютером/Локальные пользователи и группы/Группы». Добавив соответствующие группы, предоставляется возможность их использования в добавлении аттрибутов, например [Authorize(“Custom Administrators group”)], после чего доступ к соответствующему классу или методу получат только те пользователи, имена (домены) которых включены в соответствующие группы.

Таким образом, разработан подход по контролю безопасности клиент-серверных веб-приложений при использовании фреймворка Microsoft SignalR с технологией применений атрибутов для определенных клиентских групп, указанных на серверной машине с операционной системой Windows.

Литература

1. SignalR [Электронный ресурс]. – URL: https://docs.microsoft.com/en-us/aspnet/signalr (дата обращения: 16.05.2018).

УЯЗВИМОСТИ ПОВРЕЖДЕНИЯ ПАМЯТИ В УСТРОЙСТВАХ «INTERNET OF THINGS»

В.Ф. Кулиш

Устройства «интернета вещей» используют широкий диапазон архитекур центрального процессора, но наибольшее распространение получили архитектуры ARM и MIPS. Использование таких архитектур обусловлено их низким энергопотреблением и, соответсвенно, низким количеством выделяемого тепла при работе. Однако использование таких архитектур не защищает от уязвимостей повреждения памяти. Также как и устройства с архитектурой x86, такие устройства также подвержены уязвимостям переполнения буфера и уязвимостям форматных строк.

Уязвимости переполнения буфера обнаружились еще в начале компьютерной эпохи и продолжают существовать по сей день. Уязвимостям такого типа подвержены языки программирования, в которых управление процессом выделения памяти отдано на откуп программисту (пример: C, C++). При создании программ разработчику необходимо контролировать размер помещаемых в переменную данных, память под которую была

выделена ранее специальной командой языка программирования. В случае, если размер данных будет больше, чем количество выделенной памяти произойдет переполнение буфера. В результате переполнения могут быть повреждены важные данные программы, что может вызвать падение программы. Однако перезапись данных может привести не только к краху, но и к перехвату управления над программой и выполнению произвольного кода. В зависимисти от места выделения памяти переполнение может произойти на стеке вызовов функций или в динамически выделяемой области памяти (куча).

Уязвимости форматной строки основаны на ошибках программирования, влияние которых на безопасности не всегда очевидно. Форматные строки используются для вывода определенного вида информации. В ней предварительно указывается какой тип данных предполагается выводить. Отсуствие формата позволяет злоумышленнику внедрить свой формат предварительно передав на вход программы исполняемый код. При выводе форматной строки код будет выполнен и управление будет передано злоумышленнику.

Методы противодействия атакам на повреждение памяти направлены на уменьшение последствий от атаки. Методы никак не защищают программу от падения, но позволяют предотвратить перехват управления программой с помощью специальных данных. Существуют два основных способа предотвращения: NX-бит; ALSR.

NX-бит, отвечающий за No-eXecute, – это технология, используемая в CPU для выделения пространства памяти для хранения кода процессора или данных. Однако, NX bit все больше и больше используется в архитектуре процессора фон Неймана, из-за соображений безопасности. Операционная система с помощью NX бит может точно размечать пространства памяти как не исполнимые. Процессор будет отвергать выполнение любого кода, расположенного в этих зона памяти. Общая название техники известна как executable space protection, и используется для предотвращения исполнения вредоносного программного обеспечения, которые могут «захватить» компьютер вставляя свой код в код других программ, и запуская свой код в этом разделе; один из классов таких атак известный как переполнение буфера. Однако злоумышленник может обойти защиту с помощью NX бит путем переиспользования кода программы или библиотек, используемых ей. Технологии получили название «return-to-libc» и возвратно-ориентированное программирование. Они позволяют избавиться исполняемого кода передаваемого на вход программе. Вместо этого атакующий использует для атаки функции уже имеющиеся в программе.

ASLR (англ. address space layout randomization – «рандомизация размещения адресного пространства») – технология, применяемая в операционных системах, при использовании которой случайным образом изменяется расположение в адресном пространстве процесса важных структур данных, а именно образов исполняемого файла, подгружаемых библиотек, кучи и стека. Технология ASLR позволяет размещать системные компоненты в разных областях памяти при каждом запуске операционной системы. Задача этой технологии – внесение случайности в распределение адресов оперативной памяти, используемых приложением. Использование ASLR изменяет расположение в адресном пространстве таких важных структур как образ исполняемого файла, подгружаемых библиотек, кучи и прочего. Использование ASLR приводит к тому, что целый класс атак (к примеру, переполнение буфера, возврат в библиотеку (return-to-libc)) заканчивается неудачей. Помимо этого технология позволяет обнаруживать подобные атаки, так как в результате неудачных попыток исполнение атакуемого приложения прекращается.

Уязвимостям повреждения памяти подвержены процессоры на разных архитектурах. Различаются только методы эксплуатации на разных архитектурах. Методы противодействия атакам, использующим уязвимости повреждения памяти, также используются одни и те же на разных архитектурах. Однако методы противодействия не всегда достаточны для обеспечения защищенности программы.

РЕГИСТРАЦИЯ И ОБРАБОТКА БИОМЕДИЦИНСКИХ СИГНАЛОВ

Т.П. Куль

Для регистрации речевых сигналов используется следующее аппаратное обеспечение:

1. Беспроводная Bluetooth гарнитура с чувствительным микрофоном для записи речевых тестов. Беспроводная Bluetooth гарнитура обеспечивает: одинаковое расстояние от речевого аппарата всех испытуемых до записывающего устройства (микрофона), что позволяет в последствии анализировать абсолютные значения амплитуды речевого сигнала, а также его динамику в процессе теста; высокое качество записи речи при проведении диагностики; комфортные условия для испытуемых.

2. Мобильное устройство со специально разработанным мобильным приложением для воспроизведения испытуемому видеоряда с речевыми тестами и одновременной регистрацией данных с микрофона посредством Bluetooth-интерфейса.

Мобильное приложение работает на платформе Android и реализует следующие функции: демонстрация ранее описанного видеоряда с речевыми тестами; одновременная по отношению к воспроизведению видеоряда регистрация речевого сигнала через беспроводную Bluetooth гарнитуру; автоматическое сохранение записанных речевых сигналов в формате .wav; воспроизведение и удаление записи.

Далее записанный в единый файл речевой сигнал разделяется на отдельные речевые тесты и подвергается цифровой обработке посредством специально разработанного программного обеспечения в среде MatLab [1, 2].

Литература

1. Метод диагностики и контроля эффективности лечения бульбарных нарушений на основе цифровой обработки речевых сигналов / А.Н. Осипов [и др.] // Новости медико-биологических наук. 2017. Т.15, № 2. С. 65–75.

2. Цифровая обработка речевых сигналов в диагностике бульбарных нарушений. / А.Н. Осипов [и др.] // Материалы третьей Междунар. конф. «BIG DATA and Advanced Analytics. BIG DATA и анализ высокого уровня». Минск, 2017. С. 312–318.

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

С.Г. Кульгавик, П.М. Буй

В Республике Беларусь в последнее время наблюдается процесс стремительной информатизации и компьютеризации практически всех отраслей народного хозяйства. В рамках этого процесса на вооружение принимаются информационные системы – системы, предназначенные для хранения, поиска и обработки информации, которые, помимо прочего, включают человеческие, технические и прочие организационные ресурсы, взаимодействующие с информацией. Особое место занимают информационные системы, выполняющие функции автоматизированных систем управления технологическими процессами (АСУ ТП).

Вместе с тем процессы информатизации и компьютеризации, а также использование современных сетевых технологий таят в себе множество потенциальных опасностей, область реализации которых касается исключительно сферы высоких технологий. При отсутствии адекватной системы защиты опасности такого рода могут привести к нарушению штатной работы информационных систем, что особенно критично для АСУ ТП. В таких условиях обязательным является проведение анализа опасностей характерных как для самих информационных систем, так и для среды их функционирования.

Для защиты информационных систем от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

В реальной среде функционирования любой информационной системы независимо от нее существует множество угроз его безопасности – возможных воздействий на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Следует разделять угрозы

функциональной и информационной безопасности исходя из функций информационных систем, на которые они нацелены.

Оптимальным методом анализа угроз является метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз. В качестве критериев оценки опасности конкретной угрозы можно выбрать возможность возникновения источника угрозы, степень его готовности произвести атаку, а также фатальность для объекта от реализации угрозы.

При наличии множества уязвимостей информационной системы и множества угроз ее безопасности в реальных условиях функционирования велика вероятность реализации одной из угроз, нацеленной на процесс функционирования объекта или безопасность информации, которая в нем используется. Анализируя коэффициенты опасности совокупности уязвимостей, можно произвести их ранжирование и определить те из них, устранением которых необходимо заняться в первую очередь.

Для защиты информационных систем от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

Учитывая многообразие угроз современного информационного мира, построить абсолютно адекватную систему защиты не представляется возможным, ведь затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз. Таким образом, необходимо выбрать методику, которая позволит выбрать наиболее опасные для исследуемой информационной системы угрозы и защищаться только от них. Также важным является определение наиболее опасных уязвимостей, устранение которых позволит существенно повысить уровень безопасности информационной системы.

В реальных условиях функционирования одна и та же уязвимость безопасности информационной системы может стать причиной реализации сразу нескольких угроз.

ЭЛЕКТРИЧЕСКИЕ СВОЙСТВА ГЕТЕРОСТРУКТУРЫ ОКСИД ТИТАНА–КРЕМНИЙ ПРИ ОБЛУЧЕНИИ СОЛНЕЧНЫМ СВЕТОМ

А.А. Курапцова

Диоксид титана (TiO_2) достаточно широко используется в разных устройствах фотовольтаики: в процессах фотокатализа, при фотолизе воды, очистке воздуха и воды от загрязнений, в том числе от тяжелых металлов и органических соединений. Также композитные материалы на основе диоксида титана находит применение для экранирования помещений от электромагнитного излучения и создания физических ультрафиолетовых фильтров.

Было проведено моделирование электрических параметров гетероструктуры оксид титана / кремний (n-TiO2/p-Si) с помощью программы PC1D 5.9. Толщина диоксида титана – 1 мкм, кремния – 5 мкм. Ширине запрещенной зоны оксида титана (анатаз) 3,2 эВ соответствует энергия кванта с длиной волны 388 нм, что попадает в ультрафиолетовую часть спектра. Получены зависимости скорости генерации носителей заряда от расстояния от фронтальной поверхности и вольт-амперные характеристики структуры n-TiO_2/p-Si для различных длин волн солнечного излучения (мощность излучения 0,06 Вт/см^2).

Сравнение зависимости тока короткого замыкания структуры от длины волны излучения со спектром солнечного излучения показало, что его максимум в гетероструктуре приблизительно соответствует максимуму мощности солнечного излучения.

Таким образом, проведенное моделирование электрических характеристик гетероструктуры показало, что ВАХ в условиях освещения солнечным светом характеризуется насыщением тока, величина которого нелинейным образом зависит от длины волны солнечного света. Ток короткого замыкания характеризуется максимумом при длине волны, соответствующей генерации носителей заряда в кремнии.

Полученные результаты необходимы для исследования электронных процессов, протекающих на поверхности оксида титана, которые обусловливают его фотокаталитические свойства.

МИКРОМАГНИТНОЕ МОДЕЛИРОВАНИЕ НАМАГНИЧЕННОСТИ ФЕРРОМАГНИТНЫХ ЧАСТИЦ, ЗАКЛЮЧЕННЫХ В УГЛЕРОДНЫЕ НАНОТРУБКИ

А.В. Кухарев

Нанокомпозиты на основе ферромагнетиков и углеродных нанотрубок (УНТ) привлекательны с практической точки зрения за счет своих уникальных физических свойств. В частности, интерес для исследования представляют структуры, состоящие из многослойных УНТ с осажденными в их внутреннюю полость ферромагнитными частицами [1]. Ввиду высокого предела прочности нанотрубок, измеряемого десятками гигапаскалей [2], после термического воздействия (нагрева/охлаждения) в такой структуре могут возникать магнитоупругие напряжения, достаточные для изменения магнитного состояния ферромагнитных частиц.

В работе посредством микромагнитного моделирования в пакете Nmag изучалось распределение намагниченности в цилиндрических частицах кобальта с гексагональной (*hcp*) и кубической (*fcc*) кристаллической решеткой, на которые действует сжимающее напряжение со стороны внешней среды (т.е. нанотрубки). Длина цилиндра 50–200 нм, диаметр – 10–20 нм. Для обоих решеток в отсутствие внешних воздействий магнитное состояние частиц определяется анизотропией формой, и является однодоменным, причем вектор намагниченности направлен параллельно оси цилиндра.

Показано, что радиальное сжатие цилиндра *hcp*-кобальта напряжением выше 5 ГПа приводит к переходу магнитного состояния цилиндра в неоднородное, причем вид распределения намагниченности определяется величиной напряжений и направлением гексагональной оси кобальта.

Литература

1. Impact of CNT medium on the interaction between ferromagnetic nanoparticles / A.L. Danilyuk [et al.] // EPL. 2017. Vol. 117. P. 27007.

2. Ruoff R.S., Qian D., Liu W.K. Mechanical properties of carbon nanotubes: theoretical predictions // C. R. Physique. 2003. Vol. 4. P. 993–1008.

ТЕРМИЧЕСКОЕ ИНИЦИИРОВАНИЕ РЕАКЦИЙ БЫСТРОГО ОКИСЛЕНИЯ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ

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

В настоящее время большинство информации хранится в цифровом виде на электронных накопителях. На основе энергетических свойств пористого наноструктурированного кремния могут быть разработаны разнообразные микроэлектромеханические системы (МЭМС) для средств самоуничтожения микросхем при несанкционированном доступе.

В работе исследовались энергетические свойства нанопористого кремния с межпоровым пространством, заполненным окислителем. При изготовлении пористого кремния особое внимание уделили пористым структурам, получаемым на основе кремниевых пластин р-типа с удельным сопротивлением кремния 10 Ом·см. Так как на данных пластинах образуется нанопористый кремний с диаметром пор от 2 до 50 нм. Анодирование проводили при плотности тока 25–75 мА/см^2 в 33 % растворе плавиковой кислоты (HF) и этанола. Для каждой плотности анодного тока было изготовлено по 3 образца с различным временем анодирования. В качестве окислителя применяли 20 % раствор перхлората натрия. Выбранный окислитель имеет большой энергетический выход реакции окисления и способность оставаться в порах после испарения раствора. Инициирование процессов горения и взрыва слоев пористого кремния, для определения условий разрушения кремниевой подложки, осуществляли путем помещения образцов на нагретую до 500 °С поверхность.

Атомы водорода, покрывающие пористый кремний, являются буферным слоем между атомом Si и молекулярным кислородом, который предотвращает взаимодействие кислорода с кремнием. При инициировании реакции окисления поверхностные Si-H связи разрываются, создавая оборванные связи Si, а водород удаляется с поверхности. В результате происходит

взаимодействие поверхностных атомов Si непосредственно с атомами кислорода из окислителя, приводящее и окислению наноструктур кремния.

Определены режимы формовки нанопористого кремния, его структурные параметры и условия термического инициирования реакций быстрого окисления, обеспечивающие разрушение кремниевого чипа. Полученные результаты могут быть использованы при изготовлении саморазрушающихся МЭМС для самоуничтожения микросхем, жестких дисков, CD, DVD в полупроводниковой и компьютерной технике.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СВЕТОДИОДОВ ИЗ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ КАК ИСТОЧНИКОВ ЕДИНИЧНЫХ ФОТОНОВ

С.К. Лазарук, А.А. Лешок, Ле Динь Ви, А.И. Мацкевич, А.С. Хиневич, А.Г. Черных

Идеальный излучатель одиночных фотонов определяется как фотонный источник, в котором исключительно под действием управляющего сигнала излучается только один фотон. Для создания подобных источников света применяются одиночные излучатели (атомы, ионы, молекулы, квантовые точки, центры окраски), которые при возбуждении испускают одиночные фотоны. Эффективные однофотонные источники света являются ключевыми элементами систем квантовой криптографии и квантовых вычислений. Помимо этого они представляют значительный интерес для создания прецизионного спектрального оборудования и эталонов оптической мощности.

Нами разработано оптоэлектронное устройство на основе светодиодов из наноструктурированного кремния. Конструкция разработанного устройства состоит из двух контактов Шоттки, а также из слоя анодного оксида алюминия, разделяющего алюминиевые электроды. Нижний слой анодного оксида алюминия содержит кремниевые наночастицы, излучающие свет в режиме лавинного пробоя контакта Шоттки, образуя таким образом светодиодный элемент на основу наночастиц кремния. При подаче обратного смещения на диоды величиной 4В и выше их излучение регистрировалось интегрированными фотодетекторами. Минимальные размеры светоизлучающих элементов (порядка 5×5 мкм) и широкий диапазон рабочих напряжений светодиодов позволяют регистрировать оптические сигналы в диапазоне от мкВт/см^2 до Вт/см^2. Нижний предел интенсивности светоизлучения соизмерим с мощностью излучения индивидуальных фотонов видимого диапазона, что позволяет рассматривать разработанную конструкцию как перспективную для ее использования в качестве генератора индивидуальных фотонов.

Разработанная система способна работать в гигаргерцевом диапазоне частот, что достигается за счет миниатюризации рабочей площади светодиодов. Данная разработка открывает новые возможности для развития как кремниевой оптоэлектроники, так и квантовых систем.

МЕЖДУЧИПОВЫЕ ОПТИЧЕСКИЕ МЕЖСОЕДИНЕНИЯ НА ОСНОВЕ СВЕТОДИОДОВ ИЗ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ И ОПТИЧЕСКОГО ИНТЕРПОЗЕРА ИЗ МИКРОКАНАЛЬНОЙ КРЕМНИЕВОЙ ПЛАСТИНЫ

С.К. Лазарук, А.А. Лешок, Ле Динь Ви, А.И. Мацкевич, А.С. Хиневич, А.Г. Черных

Оптические межсоединения осуществляют передачу сигнала от источника света через световод к фотодетектору, что обеспечивает высокую степень защиты передаваемой информации за счет локализации информационного потока внутри данной микросистемы.

Нами разработана система междучиповых оптических межсоединений на основе светодиодов из наноструктурированного кремния, микроканальной кремниевой пластины в качестве оптического интерпозера, выполняющего роль световода, и фотодетекторов. Минимальные размеры светоизлучающих диодов составляют несколько микрометров, что вместе с микронными размерами отверстий (диаметр микроканалов составляет 2–10 мкм) в кремниевых пластинах позволяют достичь рекордно высокой плотности передачи оптической информации. Проведена оценка потерь оптического сигнала после его прохождения через микроканалы оптического интерпозера. Величина потерь оптического сигнала составила

10–20% в зависимости от длины волны видимого диапазона. Уровень выходного оптического сигнала достаточен для его регистрации фотодетекторами.

Разработанная система способна работать в гигаргерцевом диапазоне частот, что достигается за счет миниатюризации рабочей площади светодиодов. Данная разработка открывает новые возможности для развития кремниевой оптоэлектроники и интегральной электроники в целом.

ИССЛЕДОВАНИЕ ЗАРЯДОВЫХ СВОЙСТВ АНОДНЫХ ПЛЕНОК, ИСПОЛЬЗУЕМЫХ В МЕМРИСТОРНЫХ СТРУКТУРАХ

С.К. Лазарук, В.В. Дудич, Г.Г. Рабатуев, А.С. Хиневич, В.В. Фиалковский

Развитие современной электроники создает постоянный спрос на разработку новых технологий и принципов формирования устройств обработки, хранения и защиты информации, так как возможности кремниевой технологии в области дальнейшей миниатюризации и снижения энергопотребления ячеек памяти ограничены фундаментальными физическими свойствами. Для защиты информации предлагается использование мемристороных структур (энергонезависимых ячеек памяти). Мемристоры демонстрируют эффект переключения сопротивления между высокоомным и низкоомным состояниями под действием внешнего электрического поля. Данный тип памяти способен обеспечить надежное хранение и защиту информации.

Проведено исследование зарядовых свойств анодных пленок оксидов титана и алюминия. Было установлено наличие подвижных и фиксированных зарядов в оксидных пленках, которые в зависимости от условий формирования, могут быть как положительными, так и отрицательными. Было проведено обсуждение влияния зарядовых состояний на мемристорный эффект и выявлено, что данные заряды увеличивают коэффициент переключения, что положительно сказывается на увеличении отказоустойчивости ячеек памяти.

Проведенные исследования позволили увеличить коэффициента переключения на порядок в мемристорной структуре, что открывает новые возможности для практического применения.

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО СПОСОБУ МЫШЛЕНИЯ

А.С. Левковский

По статистике, 40 % системных администраторов хранят свои важные данные в незашифрованном виде, что дает возможность злоумышленнику воспользоваться информацией после несанкционированного доступа в систему. В целях защиты информации могут применяться следующие способы аутентификации: по отпечатку пальца, радужной оболочке или сетчатке глаза, геометрии руки или лица, голосу, рукописному или клавиатурному почерку и др.

В 2010 году на взлом пароля при входе в систему с помощью SSD-устройств на ОС Windows XP требовалось 2–11 секунд. На сегодняшний день на аналогичный способ проникновения в систему требуется гораздо меньше времени.

Одним из эффективных способов решения проблемы защиты информации ограниченного распространения может послужить устройство, созданное в Массачусетском университете и способное с вероятностью до 92 % сканировать мысли человека. С научной точки зрения данные, которые генерирует мозг во время мыслительных процессов, уникальны и их нельзя подменить.

Устройство работает следующим образом. На начальном этапе выполняется его калибровка для того, чтобы определить, как мозг реагирует на различного рода информацию. При этом на челюсть человека передаются вибрации. Они являются сигналами, несущими информацию, предназначенную для обработки мозгом человека. Результаты такой обработки анализируются устройством, на основании чего формируется эталон, который заносится в базу данных и в последующем используется для подтверждения идентификации.

Передавая с помощью устройства информацию в мозг, можно отследить обратную связь и логику мышления. Алгоритм функционирования – по принципу игры в ассоциации. В последующем, когда потребуется получить доступ, будет посылаться информация, которая будет схожа с той, которая использовалась при калибровке, и устройство проанализирует реакцию, определив, кто пытается получить доступ. Вся информация должна шифроваться и передаваться через проводное соединение, чтобы избежать перехвата и дальнейшей расшифровки. Для высокого уровня безопасности дополнительно можно использовать сканер отпечатка пальца / сетчатки глаза / другой известный и удобный способ идентификации.

Кроме того, идентификацию пользователя по способу мышления можно попробовать реализовать с помощью высокоскоростной камеры, делающей 10 тысяч кадров в секунду.

УЧЕБНЫЙ СТЕНД КОНВЕЙЕРНОЙ ОБРАБОТКИ ДАННЫХ СТРУКТУРОЙ ПРОЦЕССОРНЫХ ЭЛЕМЕНТОВ, СВЯЗАННЫХ КОММУТИРУЕМЫМИ ПРОВОДНЫМИ И ЛАЗЕРНЫМИ ОПТОВОЛОКОННЫМИ ЛИНИЯМИ СВЯЗИ

С.В. Лешкевич, В.А. Саечников

В настоящее время мультигигабитные скорости обмена информацией в современных средствах коммуникации уже никого не пугают. Относительно невысокая стоимость каналов связи и упрощение операций обмена информацией позволяют по новому взглянуть на возможности распределенных вычислительных систем. В таких системах за счет упрощения функциональности отдельных вычислительных узлов может быть значительно увеличена скорость обработки данных. Архитектура вычислительной системы будет напоминать конвейер (datastream-архитектура). В результате могут быть созданы системы управления процессами радиочастотного быстродействия.

Не менее важным является то, что шифрование (при использовании аппаратных средств его ускорения) не является узким местом в мультигигабитных системах коммуникации. Большой объем шифрованного трафика благоприятно влияет на защищенность системы в целом. Это одна из причин по которой такие системы прижились в локальных вычистительных сетях центра управления полетом МКС, крупных вычислительных центров.

Демонстрация возможностей современных средств коммуникации в лабораторном практикуме в вузе, использование современной элементной базы и опыт решения на этой базе задач обработки сигналов, управления процессами и коммуникации должны будут способствовать подготовке высококвалифицированных специалистов в области радиоэлектроники и аэрокосмических систем. Студенты приобретут навыки работы с современной электроникой, которая быстро устаревает и обычно недостаточно документирована.

Наряду с проводными линиями связи для изготовления стенда предполагается использовать лазерные оптические передатчики совместно с многомодовым волокном. Гибкость и программируемость системы будет обеспечена возможностью коммутации вычислительных узлов между собой.

Литература

1. Optical network and FPGA/DSP based control system for free electron laser / R.S. Romaniuk [et al.] // Bulletin of the Polish academy of sciences. Technical sciences. 2005. Vol. 53, No. 2.

ПРИНЯТИЕ ЭКОНОМИЧЕСКИХ РЕШЕНИЙ В УСЛОВИЯХ РИСКА И НЕОПРЕДЕЛЕННОСТИ

М.В. Лобашинский

При принятии экономических решения в условиях риска и неопределенности особую роль играет анализ и прогнозирование принимаемых решений. При этом возникает необходимость учета и анализа влияния факторов неопределенности и разработки соответствующих методик.

Целью исследования состоит в определении и реконструкции основных принципов процесса принятия экономического решения на базе анализа фактора неопределенности.

Принятие решений в условиях неопределенности характерны тем, что субъекту, принимающему рискованное решение неизвестны вероятности различных вариантов развития событий, связанных с принимаемым решением. В этом случае при выборе альтернативы принимаемого решения субъект руководствуется, с одной стороны, своим рисковым предпочтением, а с другой – соответствующим критерием выбора из всех альтернатив по составленной им матрице решений.

Принятие решений в условиях риска основано на том, что каждой возможной ситуации развития событий может быть задана определенная вероятность его осуществления. Это позволяет установить весовые коэффициенты каждого из конкретных значений эффективности по альтернативам и по значению вероятности. В результате можно получить на этой основе интегральный показатель уровня риска, соответствующий каждой из альтернатив принятия решений. Сравнение этого интегрального показателя по отдельным альтернативам позволяет избрать для реализации ту из них, которая приводит к заданному показателю эффективности с наименьшим уровнем риска.

Литература

1. Диев В.С. Рациональный выбор в условиях риска: модели и парадоксы // Вестн. Новосиб. гос. ун-та. Серия: Философия. 2010. Т. 8, вып. 2. С. 24–31.

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ ЗАЩИЩЕННОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

С.Ю. Лоскот, А.В. Мурашко, О.А. Хацкевич

Для эффективной разработки и внедрения в эксплуатацию мультисервисных сетей связи необходимо предусмотреть своевременную защиту программ и баз данных, средств хранения, обработки и передачи информации. Основные требования предъявляемые к мультисервисной сети связи заключаются в следующем: высокий уровень информационной безопасности; организация четкой аутентификации и идентификации всех пользователей автоматизированной информационной системы; организация системы централизованного управления и др. [1].

В качестве объекта исследования в данной работе была выбрана сеть связи крупного государственного предприятия ЗАО «Технопром». Компания имеет два офиса. Каждый офис имеет собственную локальную сеть. Суммарное количество рабочих станций в двух локальных сетях 500. Пользователи имеют доступ к серверу базы данных, где хранится информация о клиентах, электронной почте и HTTP-серверу. Некоторые сотрудники компании загружают мультимедиа контент, замедляя доступ к сети Интернет другим сотрудникам. В целях обеспечения необходимо уровня безопасности и оптимизации работы мультисервисной сети компания решает установить брандмауэр.

Моделирование мультисервисной сети производилось в программе Riverbed Modeler 17.5. Программный продукт Riverbed Modeler 17.5 – это объектно-ориентированный инструмент моделирования сетей связи. Данная программа имеет обширный пакет различных моделей сетевых элементов, библиотеки различных протоколов сетей связи и позволяет производить расчет основных характеристик с учетом параметров QoS для различных типов трафика [2]. Результаты моделирования представлены в виде графиков, которые отражают процент загрузки WAN соединения, время отклика приложения базы данных и время отклика web страницы.

Было смоделировано два случая работы сети: без установки брандмауэра и с установленным брандмауэром. При моделировании в первом случае были получены следующие данные: время отклика приложения базы данных составляет более 1 сек.; время отклика web страницы – более 3 сек.; процент загрузки WAN соединения равен в среднем 80 %, что приводит к некорректной работе приложений в сети. При моделировании во втором случае были получены следующие данные: время отклика приложения базы данных составляет 1 сек.; время отклика web страницы 3 сек.; процент загрузки WAN соединения уменьшился с 80 % до 40 %.

Результаты исследований показывают, что при использовании в сети устройства защиты от несанкционированного доступа и его правильной конфигурации удалось оптимизировать работу мультисервисной сети, улучшить ее производительность и обеспечить необходимый уровень безопасности.

Литература

1. Мультисервисные сети следующего поколения [Электронный ресурс]. – URL: http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html (дата обращения: 16.05.2018).

2. Проектирование и моделирование сетей связи в системе Riverbed Modeler / В.Н. Тарасов [и др.]. Самара, 2016. 260 с.

ПОДХОДЫ К ДЕТЕКЦИИ ОБЪЕКТОВ НА ДИНАМИЧЕСКИХ ИЗОБРАЖЕНИЯХ

М.М. Лукашевич

Видеоанатитика в целом и задача детекции объектов на видео в частности являются важными элементами инженерно-технической защиты объектов. Традиционные подходы к детекции объектов на статических или динамических изображениях (видео) включают в себя следующие этапы: сегментация, извлечение признаков и детекция. На этапе сегментации возможно преобразование цветового пространства и применение различных алгоритмов пороговой обработки. В качестве информативных признаков могу использоваться детекторы границ, HOG-признаки, вейвлеты Хаара, Фурье-дескрипторы и др. Детекция и/или распознавание объектов реализуется на базе таких алгоритмов, как SVM классификатор, kNN классификатор, сравнение с эталоном и др.

Типовые схемы не всегда дают требуемую точность детекции. Последние результаты в области глубоких нейронных сетей позволяют улучшить точность детекции объектов. В настоящее время предложено большое число моделей глубоких нейронных сетей. Предложена схема детекции объектов на основе RCNN-детектора [1], состоящего из CNN (сверточной нейронной сети) и классификатора. В частности, предполагается рассмотрение гипотез о метаположении объекта (~2000 К). Гипотезами считаются вырезанные фрагменты изображения, которые подвергаются перемасштабированию. Далее функционирует CNN и вычисляются признаки, на основе которых на следующем этапе выполняется литейная классификация для каждого класса и уточнение местоположения гипотезы. При этом обучается только линейная классификация. Успешность применения глубоких нейронных сетей подтверждена результатами, полученными на массивной базе аннотированных изображений, предназначенной для отработки и тестирования методов распознавания образов и машинного зрения ImageNet [2].

Литература

1. Ross Girshick, Jeff Donahue, Trevor Darrell, Jitendra Malik. Rich feature hierarchies for accurate object detection and semantic segmentation Tech report (v5). 22 Oct. 2016.

2. ImageNet [Электронный ресурс]. – URL: http://image-net.org (дата обращения: 16.05.2018).

МАЙНИНГ КРИПТОВАЛЮТ: НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.М. Лыньков, В.С. Князькова

Распространение технологии блокчейн и рост популярности майнинга привели к появлению новых видов угроз информационной безопасности. Сам майнинг представляет собой деятельность по поддержанию работы распределительной сети путем закрытия и создания блоков в технологии блокчейн на основе использования вычислительных мощностей. На данный момент наибольшее распространение получили виды угроз, связанные со скрытым майнингом, а также краже данных криптовалютных кошельков и обменных сервисов.

Скрытый майнинг обычно реализуется через заражение браузерным майнером. Одним из вирусов такого типа является JS/CoinMiner, уровень распространенности которого по мнению специалистов компании ESET на сентябрь 2017 года составил 12,45%. Задачей злоумышленника при использовании вируса такого типа является включение зараженного компьютера пользователя в часть распределенной сети, вычислительные мощности которой используются для добычи криптовалюты (Bitcoin, Monero, Zcash и т.п.). Заражению могут быть подвержены не только стационарные компьютеры, но и смартфоны. Основной способ распространения майнинговых скриптов является вредоносная реклама. В наибольшей степени такой вид угрозы актуален для России, Украины и Беларуси из-за выбора языка сайтов, в которые были внедрены скрипты – доменная зона.ru и .by.

Распространение получили также схемы создания фишинговых приложений-кошельков для перехвата закрытых ключей и SEED-фраз; создаются также фишинговые приложения криптовалютных бирж.

Рекомендации по защите от угроз такого типа стандартны: следует выбирать приложения для обмена криптовалют и криптовалютные кошельки аналогично тому, как выбирается для загрузки приложение мобильного банка; при загрузке такого приложения следует убедиться, что оно официальное; при возможности следует использовать двухфакторную аутентификацию для защиты эккаунта криптовалютной биржи/кошелька; своевременно обновлять установленное антивирусное ПО; периодически проверять свое устройство на наличие вирусов.

Литература

1. ESET: криптовалютные мошенники переходят на Android [Электронный ресурс]. – URL: https://www.esetnod32.ru/company/press/center/eset-kriptovalyutnye-moshenniki-perekhodyat-na-android-/. – (дата обращения: 20.04.2018).

2. Компьтеры белорусов используются для тайного майнинга [Электронный ресурс]. – URL: https://42.tut.by/560515/. – (дата обращения: 20.04.2018).

3. Скрытый майнинг на компьютерах белорусов стал массовым [Электронный ресурс]. – URL: https://42.tut.by/577203/. (дата обращения: 20.04.2018).

ОРГАНИЗАЦИЯ БЕЗОПОСНОСТИ БОЛЬШИХ ДАННЫХ

Д.В. Лящук, Н.А. Искров, В.Е. Проволоцкий

Существующие на данный момент подходы к обеспечению защиты технологий больших данных в большинстве своем основаны на использовании точечных мер при отсутствии единой полномасштабной защиты. Сегодня отсутствуют четко сформулированные методы, полностью описывающие шаги и действия по защите больших данных, структурированных и неструктурированных, для которых характерны свои особенности сбора, агрегирования, хранения и анализа. На данный момент можно определить четыре основных направления по защите данных на всех этапах работы с ними.

Первый этап заключается в обеспечении безопасности инфраструктуры. На данном этапе должны применятся лучшие практики по безопасности хранилищ данных и защите вычислений для распределенных программных платформ.

Второй этап защиты – конфиденциальность данных. Сохранение конфиденциальности при обработке и анализе данных, обеспечение безопасности данных, используя криптографические возможности, а также гранулированных контроль доступа к данным помогу наладить безопасность на данном уровне.

Управление данными является третьим этапом защиты. Если существует возможности определения происхождения данных, управления ключами и реализация открытого процесса жизненного цикла данных, аудит использования больших данных, в таком случае можно говорить об успешном выполнении задач данного этапа.

Заключительным шагом к реализации защиты больших данных является целостность данных и процедуры реагирования. На данном этапе будут полезны проверка и фильтрация конечных точек и мониторинг безопасности в режиме реального времени.

Выполнение данных шагов в полном объеме поможет не только избежать

потенциальных проблем в будущем, но и сэкономить достаточно большие средства, что в первую очередь важно для бизнеса.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ И ПРОГРАММНАЯ ЗАЩИТА ИНФОРМАЦИИ

А.Н. Макаров, Ю.А. Скудняков

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты для исполнения своих противоправных интересов и получения конфиденциальной информации. Все средства инженерно-технической защиты применяются для различных объектов взаимодействия: людей, информации, финансовых и материальных средств. По назначению средства инженерно-технической защиты делятся на группы: 1) физические средства включают различные средства и сооружения, которые могут препятствовать физическому проникновению или доступу злоумышленников на объекты защиты, к материальным носителям конфиденциальной информации, и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий; 2) аппаратные средства, в которые входит оборудование, содержащее различные приборы, приспособления и устройства, выполняющее функцию защиты информации. На любом предприятии применяется различная аппаратура и системы, которые обеспечивают производственную деятельность. Основной задачей аппаратных средств является обеспечение надежной и уверенной защиты от утечки информации и несанкционированного доступа к ней через технические средства, находящиеся на предприятии; 3) криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования [1]; 4) программные средства, которые охватывают специальные программы и комплексы, а также информационные системы обработки данных, включающие в себя защиту информации. Приведенные выше средства инженерно-технической и программной защиты являются базовыми для обеспечения защиты информации. В современном мире информационное поле становится основой взаимодействия внутри и между объектами и имеет глобальный доступ по всему миру. Средства защиты находятся в постоянном совершенствовании и развитии для предотвращения доступа в исполнении противоправных действий. Исходя из вышеизложенного, авторами работы разработана система защиты, алгоритм функционирования которой постоянно изменяется и совершенствуется. Только комплексное использование всех групп инженерно-технической и программной защиты позволяет предотвратить несанкционированный доступ к защищаемой информации.

Литература

1. Партыка Т.Л., Попов И.И. Информационная безопасность. М.: ФОРУМ: ИНФРА-М., 2005. 243 с.

ТЕСТИРОВАНИЕ СЕТЕВЫХ РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, М.А. Бабич, В.Н. Ярошевич

Исследован уровень информационной безопасности (ИБ) сервисов/ресурсов в сети интернет на примере кредитно-финансовых организаций (КФО) Республики Беларусь. Для проведения исследования были выбраны 25 белорусских КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности.

На основании проведенного тестирования можно сделать следующие выводы:

1. Наиболее часто используемые AS для КФО: ASN 12406 (ООО «Деловая сеть») – 7 сетевых ресурсов, ASN 6697 (РУП «Белтелеком») – 5 сетевых ресурсов.

2. Структура сервисов/ресурсов ДБО КФО, как правило, имеет уязвимости:

– только 7 (35 %) из 20 КФО не имеют в своей структуре уязвимых referrer-файлов;

– на 6 (30 %) из 20 КФО тип вредоносных функции уязвимых referrer-файлов детектируется явным образом как вредоносное ПО (malware, exploit, trojan);

– выявлены 7 уязвимых файлов/приложений, которые наиболее часто используются на сетевых сервисах/ресурсах ДБО КФО;

– только 9 КФО (36 %) не имеют уязвимости к реализации метода социальной инженерии (киберсквоттинг, тайпсквоттинг, фишинг).

3. Из используемых SSL-сертификатов максимальный уровень валидации (EV SSL) на основном домене КФО имеет 7 организаций (28 %).

ТЕСТИРОВАНИЕ СЕТЕВЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

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

Проведено статистическое исследование и тестирование уровня информационной безопасности (ИБ) сетевых систем видеонаблюдения (ССВН) по результатам которого можно сделать следующие выводы:

1. По результатам статистического исследования (опроса) по критерию близости: преимущественное использование на объектах различных категорий в Республике Беларусь, основными вендорами по ССВН в Беларуси являются: «Hikvision» (34,6 %), «Dahua Technology» (10,3 %), «Axis» (9 %).

2. Тестирование ССВН на предмет наличия уязвимостей, а также способов их эксплуатации через сетевые каналы сопряжения и коммуникации показало:

общее количество устройств ССВН (DVR, NVR, NAS и IP-камер) доступных через сеть – 2066 шт., из них 866 шт. (41,9 %) – имеют потенциальные уязвимости;

– общее количество доступных через сеть устройств ССВН (DVR, NVR, NAS и IP-камер) производителей: «Hikvision» – 34 шт. (1,7 %), «Dahua Technology» – 33 шт. (1,6 %), «Axis» – 1 шт. (0,05 %);

– как минимум 1 веб-сервер ССВН имеет заводские (по умолчанию) настройки «логин-пароль» администратора;

– показан пример успешной эксплуатации уязвимости «Heartbleed» (CVE-2014-0160) на типовой уязвимой ССВН, выявленной по результатам тестирования.

МОДУЛЬ ОБМЕНА ДАННЫМИ ДЛЯ ERP-СИСТЕМЫ MICROSOFT DYNAMICS 365 FOR OPERATIONS С ВНЕШНИМИ ПРИЛОЖЕНИЯМИ

А.С. Манин

В работе рассматривается программный модуль для интеграции ERP-системы Microsoft Dynamics 365 for Operations с внешними приложениями, такими как внешние web-сервисы и мобильные приложения. Проблемы обеспечения безопасности являются критическими для ERP-систем, так как оные используются в финансовой сфере. Кроме того, в рамках данной работы, существует необходимость обечения безопасности данных, исходящих из ERP-системы и используемых извне.

Большинство современных ERP-систем, в том числе Microsoft Dynamics 365 for Operations, адаптируют традиционную модель управления доступом на базе ролей как основное средство обеспечения безопасности в системе. Данная модель позволяет пользователям выполнять строго определенные транзакции и получать доступ к установленным бизнес-объектам [1]. Модель, представленная в ERP-системе Microsoft Dynamics 365 for Operations, не является избыточной, что обуславливает необходимость ее доработки. Для этого были созданы набор специфичных для модуля ролей, привилегий и технологических циклов – сущностей модели безопасности.

Обмен между ERP-системой и внешней средой обеспечивается средствами стандартизированнного протокола для создания и обмена данными OData [2]. Доступ к данным средствами сего протокола порождает ряд проблем безопасности, таких как пользовательский доступ к web-сервисам на базе OData на обоих конечных узлах (ERP-система и внешнее приложение). Для обеспечения постоянства доступа пользователя как внутри ERP-системы, так и во внешнем приложении, используется открытый протокол авторизации OAuth [3]:

внешнее приложение запрашивает маркер доступа в Azure Active Directory – службе управления удостоверениями и доступа ERP-системы Microsoft Dynamics 365 for Operations, который впоследствие используется для получения данных из ERP-системы.

Несмотря на использованные средства обеспечения безопасного соединения между узлами распределенной системы, использованных в работе, следует отметить возможность улучшения безопасности с использованием на стороне пользователей методов многофакторной аутентификаци: биометрическая аутентификация, использование одноразовых паролей, смарт-карт и т.д.

Литература

1. Петренко С.А., Курбатов В.А. Политики информационной безопасности. Москва: ДМК Пресс, 2006 400 с.

2. OData Version 4.01 Part 1: Protocol [Электронный ресурс]. – URL: http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html (дата обращения: 18.05.2018).

3. The OAuth 2.0 Authorization Framework [Электронный ресурс]. – URL: https://tools.ietf.org/html/rfc6749 (дата обращения: 18.05.2018).

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЕРИФИКАЦИИ ЦЕЛОСТНОСТИ

А.Ф. Марко

При работе с системами, отвечающими за безопасность людей, необходимо обеспечивать контроль над целостностью программного обеспечения данных систем в процессе эксплуатации.

Целью данной работы является разработка программного средства, обеспечивающее верификацию целостности программной части программно-аппаратной системы автоматизированного управления транспортным узлом.

На этапе проектирования программного средства был принят следующий алгоритм обеспечения целостности программной части системы:

– формирование контрольных сумм от различных категорий объектов данных и программирования с помощью алгоритма MD5;

– сохранение контрольных сумм в базу данных SQL в качестве эталонных;

– повторное формирование контрольных сумм и сравнение с эталонными.

Формирование контрольных сумм осуществляется для различных категорий объектов баз данных и файлов программы.

Контрольные суммы для процедур и функций, формируются через построчное суммирование кода, за исключением пробельных и других символов, не изменяющих функциональность программы, а также подсчета для полученного результата MD5. Для получения контрольных сумм от SQL-таблиц суммируется содержание всех ячеек и формируется MD5 от полученного результата.

Для повышения вероятности обнаружения непредвиденных изменений в системе помимо расчета контрольных сумм для объектов каждой категории в отдельности, рассчитываются контрольные суммы от всей категории в целом.

Разработка программного средства велась на языке C# с использованием среды Visual Studio. Для формирования контрольных сумм от таблиц, процедур и функций баз данных применялись процедуры, реализованные на языке структурированных запросов SQL.

По результатам разработки было получено программное решение, позволяющее при запуске системы автоматически верифицировать ее целостность.

ПРОГРАММИРОВАНИЕ РАСШИРЕНИЯ ИНТЕГРИРОВАННОЙ СРЕДЫ РАЗРАБОТКИ VS2017

А.Ф. Марко, К.В. Чеушев

При работе с системами контроля версий Team Foundation Server (TFS) от компании Microsoft [1], возникает необходимость верификации номера версии при сохранении выполненной работы (check In, commit), которую осуществляет TFS, присваивая унифицированный номер (Id) каждому сохранению. Однако данная система контроля версий

не верифицирует версии файлов проектов после многократных сборок и выпусков программных продуктов.

Целью настоящей работы явилась разработка программного продукта, интегрируемого в TFS, обеспечивающего верификацию изменений версий файлов.

При разработке программного продукта использовалась возможность от компании Microsoft [1] расширения интегрированной среды разработки Visual Studio с внедрением в систему контроля версий TFS с целью расширения ее функционала. Для создания необходимых графических окон представления программного продукта, использовалась технология Windows Presentation Foundation (WPF). Встраивание в систему контроля версий TFS осуществлялась один из подходов объектно-ориентированного программирования Application Programming Interface.

Таким образом разработан программный продукт как расширение (plugin) для интегрированной среды разработки (Integrated Development Environment) Visual Studio 2017, который путем интегрирования с системой контроля версий Team Foundation Server позволяет верифицировать изменения файлов при выпуске новой сборки программного продукта.

Литература

1. Arora T Microsoft Team Foundation Server Cookbook. UK: Birmingham B3 2PB, 2016. 309 p.

ПРОБЛЕМЫ КОДИРОВАНИЯ И ПЕРЕДАЧИ ВИДЕОИНФОРМАЦИИ В БЕСПИЛОТНЫХ АВИАЦИОННЫХ КОМПЛЕКСАХ

Г. Марун, Б.А. Голищев, В.В. Позняк, Г.А. Розум

В беспилотных летательных аппаратах используется одна или несколько видеокамер для передачи видеоизображений оператору. Высокая скорость формирования видеоинформации требует высоких коэффициентов сжатия при приемлемом качестве восстановления изображений. Известные кодеки, основанные на блочной, пиксельной и кадровой компенсации движения, обеспечивают сжатие в сотни – тысячи раз. Формируемый в результате сжатия видеопоток имеет сложную структуру с большим числом блоков, размножающих ошибки, и высокой зависимостью значений, принадлежащих различным блоков. Это требует использования помехоустойчивого кодирования, вносящего дополнительную избыточность в видеопоток, достигающую 30 %. В результате скорость передачи видеоданных возрастает, снижая положительный эффект от сжатия. Высокая скорость формирования видеоданных требует использования для их передачи высоких частот. При этом необходимо обеспечение прямой видимости между передатчиком и приемником данных, а также компенсация доплеровского эффекта. Кроме того, возникают ограничения со стороны элементной базы – требуется высокая скорость обработки сигналов в модуляторе, кодере, декодере и демодуляторе, что приводит к высокому энергопотреблению. Перечисленные особенности свидетельствуют об актуальности задачи разработки новых эффективных методов сжатия видеоинформации, позволяющих существенно снизить скорость видеопотока, использовать для передачи относительно низкие частоты и низкоскоростную элементную базу. Исследования в данном направлении связаны, как с повышением эффективности кодирования результатов прогнозирования, так и с учетом новых видов избыточности видеоинформации, специфичных для определенных условий использования беспилотных авиационных комплексов. Последний подход позволяет достичь более высоких коэффициентов сжатия, но связан с существенной вычислительной сложностью, ограничивающей возможности бортовой обработки видеоинформации.

ПРИМЕНЕНИЕ НЕЛИНЕЙНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ В КАНАЛЕ С ПОДСЛУШИВАНИЕМ

А.И. Митюхин

Одно из применений нелинейных ортогональных конструкций $[N, M, d]$-кодов длиной N и кодовым расстоянием d заключается в обеспечении определенного уровня защиты информации. Свойство нелинейности кода позволяет иметь значительно больший ансамбль

M кодовых слов $\boldsymbol{X}$ над полем Галуа в сравнении с линейными кодами, что важно для защиты информации. Рассматривается подход защиты кодированной информации в предположении, что преднамеренно генерируемые ошибки $\boldsymbol{E}$ в принятом сигнале и шумы n в канале с подслушиванием должны существенно увеличить значение вероятности ошибки декодирования кодового слова в условиях ограничения времени на анализ и обработку перехватываемого сигнала. В этом случае на входе декодера канала с подслушиванием формируется вектор наблюдения $\boldsymbol{Y}$ в виде трехкомпонентного аддитивного процесса: векторов слов кода $\boldsymbol{X}$, векторов ошибок $\boldsymbol{E}$ и векторов шума n канала. Так как значения вероятностей $P(x)$ входа и $P(y)$ выхода основного канала априори известны и практически равны, то в соответствии с теоремой Байеса, зная переходные вероятности $P(\boldsymbol{Y} \mid \boldsymbol{X})$ канала, легко можно найти вероятность $P(X \mid Y)$ правильного декодирования информации по основному каналу. Наилучшая процедура декодирования вектора наблюдения $\boldsymbol{Y}$ по каналу подслушивателя состоит в нахождении такого значения номера кодового слова, при котором значение вероятности $P(\boldsymbol{Y} \mid \boldsymbol{X})$ достигает максимума [1]. Поскольку в канале подслушивателя функция $\max P(\boldsymbol{Y} \mid X)$ зависит от большого числа M, от структуры векторов внедряемых ошибок $\boldsymbol{E}$ и векторов шума n, байесовская процедура нахождения вектора $\boldsymbol{X}$ ближайшего по расстоянию d к принятому вектору Y становится затратной с точки зрения необходимости значительных вычислительных, временных и технических ресурсов для успешного перехвата кодированной информации.

Литература

1. Митюхин А.И., Якубенко П.Н. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей // Докл. БГУИР. 2015. № 4 (90). С. 5–9.

ИСПОЛЬЗОВАНИЕ МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день практически все организации осуществляют информационную безопасность своей корпоративной сети, используя различные средства. К таким средствам можно отнести: антивирусные ПО, межсетевые экраны, DLP-системы, системы обнаружения и предотвращения вторжений. Проблема заключается в том, что если использовать комплексное решение по обеспечению информационной безопасности сети, то могут возникнуть случаи, когда одно средство по безопасности будем считать другое средство угрозой для сети. Данная проблема может возникнуть, если в качестве комплексного решения использовались средства по информационной безопасности различных производителей. Для решения проблемы предлагается использовать набирающие популярность в последнее время межсетевые экраны нового поколения (МЭНП).

Межсетевые экраны нового поколения (англ. Next-Generation Firewall) – это совокупность средств, в которые входят: межсетевой экран, система обнаружения и предотвращения вторжений, DPI-технология, DLP-система. Некоторые МЭНП, например Fortigate 3810A, могут поддерживать антивирусное ПО, а также обнаружения DoS-атак. Отличие от обычного межсетевого экрана заключается в том, что МЭНП включает в себя больше уровней модели OSI, улучшая фильтрацию сетевого трафика, зависящую от содержимого пакета.

ОПЫТ ПРИМЕНЕНИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.В. Моженкова, А.И. Парамонов

Корпоративная информационная система (КИС) должна обеспечивать не только ведение учета и формирование отчетов по национальным и международным стандартам, а также предупреждать попытки несанкционированного доступа к информации. Для определения угроз безопасности персональных данных (ПДн) при их обработке в информационных системах (ИС) в Российской Федерации разработана «Методика

определения угроз безопасности информации в информационных системах» [1]. Документ устанавливает единый подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в ИС.

В докладе обсуждается опыт применения методики для КИС предприятия на этапе сопровождения. Для КИС характерны следующие исходные данные: имеет подключение к сетям общего доступа; является многопользовательской ИС; является системой с разграничением прав доступа; предназначена для обработки конфиденциальной информации, в том числе ПДн категории «Иные» сотрудников и пользователей системы.

Согласно критериям оценки, уровень защищенности оценивается как «средний», в связи с тем, что более 70% характеристик соответствуют уровню не ниже «средний» определенными характеристиками КИС. Данному уровню исходной защищенности ставится в соответствие числовой коэффициент Y1=5. Таким образом, в отношении ПДн, обрабатываемых в КИС, актуальными являются следующие угрозы безопасности: действия вредоносных программ; утрата ключей и атрибутов доступа; доступ к информации, копирование, модификация, уничтожение лицами, не допущенными к ее обработке; разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке. По результатам анализа определен состав и содержание организационных и технических мер по обеспечению безопасности ПДн.

Литература

1 Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/812 (дата обращения: 17.05.2018).

ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ НЕЙРОННОЙ АКТИВНОСТИ МОЗГА

А.О. Молчан

Случайные числа в современном мире имеют огромное значение и являются его неотъемлемой частью. Они получили широкое применение в IT сфере, криптографии и других сферах жизни. Почти всем системам компьютерной безопасности, в которых применяется криптография, необходимы случайные числа – для ключей, уникальных чисел в протоколах и т.п. – и безопасность таких систем часто зависит от произвольности случайных чисел. Если генератор случайных чисел ненадежен, вся система выходит из строя.

В общем случае все генераторы случайных чисел можно разделить на генераторы псевдослучайных чисел, как правило, реализованы программами, и генераторы случайных чисел, реализуемые в большинстве своем как аппаратно-программные решения. Аппаратный генератор случайных чисел – устройство, которое генерирует последовательность случайных чисел на основе измеряемых, хаотически изменяющихся параметров протекающего физического процесса. Например, генерация на основе теплового шума в резисторе.

Цель исследования: выявить возможность использования нейронной активности мозга в качестве источника случайной величины для аппаратно-программного генератора случайных чисел. В качестве источника случайной величины предполагается использование электроэнцефалограммы головного мозга человека.

В ходе математического анализа электроэнцефалограмм будет определена возможность использования активности головного мозга человека в качестве источника случайной величины для генератора случайных чисел. Данные исследования могут открыть новое направление развития генераторов случайных чисел и использоваться в системах шифрования данных.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ

Б.А. Монич

Программно-конфигурируемые сети представляют собой сети, в которых разделены уровни управления сетью и коммутации потоков данных. Данная архитектура сети предоставляет возможность программного управления пересылкой данных, которое логически

и физически отделено от коммутаторов и маршрутизаторов. Все функции управления сетью выполняются приложениями на отдельном физическом сервере-контроллере. В архитектуре программно-определяемых сетях можно выделить три уровня: инфраструктурный уровень, представляющий набор сетевых устройств (коммутаторов, маршрутизаторов, каналов передачи данных); уровень управления, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью; уровень сетевых приложений для более гибкого и эффективного управления сетью, позволяет выполнять различные изменения и настройки сети без прерывания сервисов и видимых изменений со стороны пользователей сети. Основными требованиями к безопасности в программно-определяемых сетях являются требования к обеспечению защиты управляющего контроллера. В первую очередь контроллер требуется защитить физическим образом и ограничить к нему доступ рабочего персонала. Работа по настройке и изменениям конфигурации сети должна проводиться в выделенной защищенной виртуальной сети. Для обеспечения отказоустойчивости, программно-определяемой сети, существует необходимость предусмотреть физическое резервирование управляющего контроллера, который должен вступать в работу, в случае взлома или отказа основного контроллера. В типичном сегменте программно-определяемой сети между контроллером и коммутатором используется безопасное соединение SSL (Secure Sockets Layer), данные методы шифрования могут быть достаточными для передачи информации внутри ЦОД, но вряд ли подойдут для внешних сетей, поскольку возникают проблемы, связанные с управлением ключами, возрастанием расходов и задержки шифрования.

Литература

1. Heller R. Sherwood, McKeown N. The controller placement problem // Proceedings of the first workshop on Hot topics in software defined networks, ser. HotSDN'12. ACM, 2012.

2. Smeliansky R.L., Gamaynov D. The model of network applications behavior. Moscow: Proggraming and Computer software, 2007.

3. Основы программно-конфигурируемых сетей / Н.Ф. Бахарева [и др.]. Самара: ПГУТИ, 2015. 111 с.

ПОЛЯРИЗАЦИОННАЯ МОДУЛЯЦИЯ В СВЧ МОДУЛЕ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

В.В. Муравьёв, С.А. Кореневский, Н.М. Наумович, А.А. Стануль, П.И. Карпович

В настоящее время для обеспечения защиты передаваемой информации в системах телекоммуникаций все более широкое применение находит миллиметровый диапазон длин волн. В этом диапазоне частот имеется возможность обеспечения большой полосы частот излучаемого сигнала и узкой диаграммы направленности при малых габаритах антенных устройств, что повышает скрытность работы системы связи. Ширина диаграммы направленности определяется диаметром антенного устройства. Для повышения защищенности передаваемой информации СВЧ модуль может работать с фазовой и поляризационной модуляцией. Современная элементная база позволяет разрабатывать модули, обеспечивающие мощность выходного сигнала 2 Вт, в диапазоне частот 36–37 ГГц [1]. Дальнейшее увеличение мощности выходного сигнала передающего устройства может быть обеспечено путем суммирование мощностей двух усилителей. Применение сумматоров на мостовых схемах приводит к уменьшению к.п.д. выходного сигнала. Для повышения суммарного к.п.д. передающего устройства, суммирование мощностей осуществляется в полосковом облучателе антенного устройства. Поляризации сигналов, возбуждаемых каждым из усилителей ортогональны, что позволяет обеспечить хорошее согласования выходных сопротивлений усилителей и полоскового излучателя. Это позволяет обеспечивать поляризационную модуляцию путем изменения разности фаз выходных сигналов усилителей

Литература

1. СВЧ модуль полудуплексной системы связи миллиметрового диапазона длин волн / В.В. Муравьёв [и др.]. // Технические средства защиты информации : тезисы докладов XV Белорусско-российской науч.-техн. конф. Минск, 6 июня 2017 г. С. 94.

ШИРОКОПОЛОСНЫЙ ПРИЕМНЫЙ МОДУЛЬ КОГНИТИВНЫХ РАДИОСИСТЕМ ДЛЯ МОНИТОРИНГА СПЕКТРА

В.В. Муравьёв, С.А. Кореневский, Н.М. Наумович, А.А. Стануль, П.И. Карпович

Одной из важнейших задач когнитивного радио является мониторинг спектра в широком диапазоне частот и обнаружение частотных полос, не используемых в настоящий момент времени. Это является основой для работы алгоритма динамического доступа к спектру и управления уровнем излучаемой мощности [1]. К приемному устройству, обеспечивающему мониторинг спектра, предъявляются требования определения не используемых в настоящее время полос в диапазоне частот до18 ГГц. Время анализа указанного диапазона частот должно составлять не более 2 с. На основании проведенного анализа доступной современной элементной базы, проведена разработка схемы широкополосного приемного устройства, работающего в диапазоне частот от 1 МГц до 18 ГГц. При разработке приемного устройства решалась проблема уменьшения влияния интермодуляционных каналов приема и обеспечения большого динамического диапазона. Разработана схема широкополосного синтезатора частот и формирования фиксированных частот, требуемых для преобразователей частот приемного устройства. Мгновенная полоса анализируемых частот 300 МГц. Сигнал в полосе частот 1 – 300 МГц оцифровывается и поступает на устройство цифровой обработки и принятия решения о наличии свободной полосы частот и допустимого значения мощности излучаемого сигнала когнитивного радио. При отсутствии результатов принятого решения несанкционированный прием сообщения передаваемого системой когнитивного радио невозможен.

Литература

1. Джеральд Корнуэл. Проектирование широкополосных преобразователей частоты // Электронные компоненты. 2016. № 6. С. 18–23.

МОДЕЛИРОВАНИЕ ВЫХОДНЫХ ХАРАКТЕРИСТИК ПОЛЕВЫХ ТРАНЗИСТОРОВ С ИСПОЛЬЗОВАНИЕМ МОНОСЛОЯ ГРАФЕНА

В.В. Муравьёв, В.Н. Мищенко

Рассмотрены вопросы моделирования выходных характеристик полевых транзисторов с использованием монослоя графена. Исследованы закономерности физического процесса переноса носителей заряда в слое графена, а также в объемной области полупроводниковой структуры, для создания которой используются соединения группы карбида кремния, и в частности, материал 4H-SiC. Высокая подвижность носителей заряда (максимальная подвижность электронов среди всех известных материалов) и другие его свойства позволяют рассматривать графен как один из наиболее перспективных материалов для широкого применения в интегральных приборах и микросхемах. Разработан алгоритм моделирования, составлена и отлажена программа моделирования выходных характеристик методом Монте-Карло. Для моделирования использовался метод Монте-Карло совместно с решением уравнения Пуассона для трехмерной области приборной структуры. Для исследования влияния слоя графена было выполнено моделирование выходного тока стока от напряжения на затворе с использованием разработанной программы, которая учитывает свойства и параметры всех использованных материалов. Анализ полученных данных показал, что использование слоя графена позволяет значительно увеличить выходной ток, крутизну выходной характеристики и ряд других параметров исследованного транзистора. Исследовано влияния особенностей формирования контактных областей стока, истока и затвора транзисторных структур на величину тока стока и выходные характеристики. Исходя из полученных результатов моделирования, выработаны рекомендации по созданию и совершенствованию технологии формирования приборов с улучшенными выходными параметрами в диапазонах СВЧ и КВЧ. Использование исследованных полевых транзисторов со слоями графена позволит создать устройства, которые найдут применение в системах приема, усиления и обработки сигналов на крайне высоких частотах.

СОВРЕМЕННАЯ ПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Навроцкий, Л.С. Стригалев

Возникновение «интернета вещей» (Internet of Things, IoT) расширяет пространство свободы и семантические возможности современных систем. Это требует совершенствования и технологий защиты информации, поскольку аналогичные возможности приобретает и атакующая сторона, которая значительно мобильней жертвы в применении современных технологий, таких Big Data и Data Mining (Text Mining, Web Mining, Call Mining, Audio Mining, Video Mining). Возникает разрыв между технологиями атакующей защищающей систем.

Необходима доработка политики информационной безопасности системы с последующим внедрением искусственных нейронных сетей (ИНС), которые обладают возможностью обучаться и самообучаться. Современное применение ИНС в сфере информационной безопасности носит, как правило, «лоскутный» характер, в то время как необходимо структурированное иерархическое внедрение ИНС по всем «болевым» точкам системы, согласно разработанной политике информационной безопасности с возможностью последующей самоорганизации.

Технологической нишей ИНС при построении систем безопасности в настоящее время является досемантическая обработка информации, охватывающая такие аспекты технологии восприятия информации как обнаружение, распознавание и анализ. Для эффективной информационной защиты системы на современном этапе необходим симбиоз традиционных технологий [1] и ИНС.

Литература

1. Навроцкий А.А. Герман О.В., Стригалев Л.С. Методы оценки качества средств защиты информации // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф. Минск, 28–29 мая 2014 г. С. 7.

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ МЕТОДОМ DECEPTION

А.И. Наумович, А.С. Шелягович

Многочисленные публикации и открытые кейсы успешных взломов самых защищенных систем в разных странах мира свидетельствуют о том, что традиционные превентивные техники защиты информации в компьютерных сетях уже не работают. Перед направленными атаками, такими как APT или Zero-day, современные методы и стратегии защиты корпоративного периметра оказались бессильны. Кроме того, современные решения оказались недостаточно гибкими для минимизации рисков, связанных с этими угрозами. Подобные проблемы могут быть решены с применением технологии Deception. Технология Deception – это использование техник активного обмана атакующих с применением специализированных ловушек, приманок и других методов дезинформации. Применение техник обмана внутри корпоративного периметра предоставляет предприятиям возможность раннего обнаружения наиболее опасных направленных атак, которые не были отслежены превентивными механизмами, такими как межсетевые экраны, системы предотвращения вторжений и антивирусные решения. Например, если атакующий сканирует сеть или осуществляет пассивный сбор сетевых пакетов, его можно обмануть, показав множество поддельных устройств, привлекательных для атаки, на которых активны сервисы с уязвимостями. Современные Deception-решения позволяют генерировать такие ловушки, которые невозможно отличить от реальных Windows/Linux/Mac-устройств, сетевого оборудования, банкоматов, POS-устройств, SCADA-устройств, баз данных, корпоративных приложений (Oracle, SAP, CyberArk и т. п.) и даже SWIFT-инфраструктуры. Любая попытка взаимодействия с этими «сенсорами» приведет к обнаружению атакующего. В отличие от существующих средств защиты, для которых высока вероятность обхода, решения, использующие технологии ловушек – позволяют максимально быстро обнаружить злоумышленника в случае успешной атаки. Это дает возможность специалистам по информационной безопасности поймать злоумышленника фактически с поличным, остановить дальнейшее распространение атаки и предупредить кражу конфиденциальных данных в автоматическом режиме.

Литература

1. Интернет-портал Российской Федерации [Электронный ресурс]. – URL: https://www.anti-malware.ru (дата обращения: 10.05.2018).
2. Интернет-портал Dark Reading [Электронный ресурс]. – URL: https://www.darkreading.com (дата обращения: 10.05.2018).

ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ НА ОСНОВЕ ЖЕЛЕЗОСОДЕРЖАЩИХ ПОРОШКООБРАЗНЫХ МАТЕРИАЛОВ

Н.А. Неверов, О.В. Бойправ, Н.В. Богуш, Т.В. Полуян

Один из путей предотвращения утечки информации по каналу побочного электромагнитного излучения заключается в электромагнитном экранировании устройств, с помощью которых выполняется обработка этой информации. Для этого используются материалы, обеспечивающие ослабление напряженности электромагнитного излучения. Основной недостаток таких материалов заключается в их высокой стоимости. В настоящей работе для получения низкостоимостных электромагнитных экранов предложено использование железосодержащей пыли, являющейся отходом различный стадий производства лифтовых изделий:

– лазерная резка металла;

– рихтовка направляющих лифтовых изделий;

– двухступенчатая дробеметная очистка металлических изделий.

Определено, что указанная железосодержащая пыль характеризуется высокими значениями относительной магнитной проницаемости (от 30 до 90 отн. ед. в зависимости от того, в результате реализации какой стадии производства она была получена).

Выполнен синтез электромагнитных экранов на основе железосодержащей пыли. Для этого реализованы ее смешивание со связующим веществом (цементным раствором) и формовка полученной смеси в плиты с плоской поверхностью. Исследованы характеристики передачи и отражения электромагнитного излучения (ЭМИ) синтезированных экранов. Установлено, что величина коэффициента передачи ЭМИ в диапазоне частот 0,7…17 ГГц экранов на основе железосодержащей пыли, полученной в результате лазерной резки металла, изменяется в пределах от –2 до –14 дБ, а экранов на основе железосодержащей пыли, полученной в результате рихтовки направляющих лифтовых изделий и двухступенчатой дробеметной очистки металлических изделий – соответственно от –2 до –12 дБ и от –2 до –25 дБ (при толщине, равной 1 см). Средняя величина коэффициента отражения ЭМИ указанных экранов составляет –8 дБ (при условии их закрепления на металлических подложках).

На основе представленных результатов можно сделать вывод о перспективности применения железосодержащей пыли в целях изготовления устройств для архитектурного электромагнитного экранирования.

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Т.С. Немов, Ю.А. Скудняков

Для обеспечения защиты информации необходимо строгое разделение обязанностей на предприятии. В зависимости от степени секретности необходимо наличие особых служб безопасности, которые подчиняются непосредственно руководству организации и контролируют соблюдение всех правил. Залог успеха в борьбе с несанкционированным доступом к информации – это четкое представление о каналах утечки информации. В общем виде необходимо разделить весь комплекс мер по защите информации на 3 больших блока: 1) ограничение доступа; 2) разграничение доступа; 3) контроль доступа. Ограничение доступа должно осуществляться в зависимости от степени секретности. Наиболее простым способом контроля является введение пропускной системы, при которой каждый отдел работает в ограниченной изолированной зоне [1]. Разграничение доступа заключается в распределении узких функциональных задач. Каждый сотрудник должен выполнять строго определенные функции [2]. Ограничение полномочий каждого пользователя позволит защитить информацию в случае проникновения злоумышленника в отдельно взятый отдел. Даже если один участок

будет уязвим, вся система продолжит функционировать в нормальном режиме. Контроль доступа должен быть основан на идентификации. В этом случае необходимо присваивать каждому субъекту уникальный образ, имя и число. В обязанности службы безопасности входит проверка соответствия всем требованиям. Приведенные выше организационные методы являются лишь базовыми для обеспечения защиты информации на предприятии. Данный список может дополняться в зависимости от конфиденциальности информации, которая используется при работе предприятия, объема выполняемых работ и опыта работы сотрудников предприятия в сфере защиты информации. Эффективность каждого блока полностью зависит от руководства предприятия, которое должно обеспечить предприятие финансовыми и человеческими ресурсами. Финансовые вложения позволяют обеспечить предприятие необходимыми техническими и криптографическими средствами защиты информации.

Литература

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1. М.: Энергоатомиздат, 1994. 400 с.

ПРОГРАММНОЕ СРЕДСТВО ПРЕДПРОСМОТРА НАСТРОЕК ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ MICROSOFT DYNAMICS AX

В.Н. Нестеренко

В работе представлено расширение для модуля «Безопасность» ERP-системы Microsoft Dynamics AX [1], позволяющее осуществлять предпросмотр отдельных частей интерфейса системы с учетом привилегий конкретного пользователя.

Разработанное программное средство предназначено для оптимизации процесса обеспечения безопасности путем определения прав доступа пользователей ERP-системы. С его помощью разработчики и менеджеры безопасности могут увидеть, как будет выглядеть та или иная форма для указанного пользователя Microsoft Dynamics AX в соответствии с предоставленными ему привилегиями. Программное средство позволяет учитывать общие настройки доступа пользователей, особенности отображения форм, связанные с привилегиями точки входа, а также воздействия «Record-level security». Для случаев, когда вызов формы осуществляется из родительской формы, предусмотрена возможность настройки и передачи необходимых входных данных в вызываемую форму, в том числе привилегии формы-родителя, что позволяет в полной мере эмулировать такого рода ситуации. Расширение представлено графическим интерфейсом, выполненным в соответствии с правилами, принятыми для Microsoft Dynamics AX. В ходе работы были реализованы алгоритмы обхода элементов форм, определения действующих прав доступа к элементам форм на основе ролей пользователя и установленной привилегии точки входа, фильтрации данных по правилам «Record-level security» с учетом текущих ролей пользователя и других особенностей этой технологии. Для этого использовались встроенный фреймворк для обработки узлов дерева объектов Microsoft Dynamics AX, стандартные методы и классы модуля «Безопасность», а также утилиты для работы с «Record-level security». В результате удалось получить эффективное средство для контроля проделываемой работы по установке привилегий пользователей.

Литература

1. The Microsoft Dynamics AX Team. Inside Microsoft Dynamics AX 2012 R3. Redmond: Microsoft Press, 2014. 371 p.

МЕТОДИКА ТЕСТИРОВАНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Омуару Алвелл Эллингтон, Е.С. Белоусова

С быстрым развитием технологий меняется и характер вирусных угроз для данных. Технологии, которые должны обеспечить защиту от этих угроз, должны адаптироваться.

Разработчики антивирусных программ утверждают, что они обеспечивают эффективное реагирование на компьютерные вирусные инциденты. Однако в настоящее время мало указаний относительно наилучшего способа оценки эффективности таких требований. Поэтому особенно актуальным является разработка тестов антивирусных программных продуктов, которые измеряют эффективность функциональных возможностей антивируса. Используя этот подход, была разработана методика тестирования выполнения требований к функциональности антивирусных программ. В настоящее время существует 4 метода тестирования антивирусных программ: статическое тестирование, динамическое тестирование; тестирование скорости реакции, ретроспектива. Тесты продолжают развиваться по мере развития отрасли, продукты становятся более сложными, требуются более сложные тесты. важно расширить методологию тестирования в областях, которые наиболее важны для защиты пользователей, используя индикаторы, которые важны как для пользователей, так и для разработчиков.

Методика тестирования антивирусных продуктов заключалась в диагностики сканирующих механизмов, защиты от вредоносных веб-приложений, фишинга, дополнительных сканеров. Для тестирования были выбраны следующие программные продукты: Kaspersky, Avira, Avast, Eset NOD32. На основе проведенных тестов можно заметить, что не один из тестируемых продуктов не обнаружил 100 % зараженных файлов, при этом все продукты осуществляли попытку лечения некоторых файлов, а не просто удалять обнаруженные ими угрозы. Антивирусный продукт Kaspersky обнаружил 97,65 % зараженных файлов, при этом из них более 60 % было удалено. Антивирусный продукт Eset NOD32 обнаружил 77,88 % зараженных файлов, восстановлено было около 55 % файлов.

ЗАЩИТА АВТОРСКИХ ПРАВ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЦВЗ

Н.В. Орлов

1. *Проблема.* Вопрос защиты авторских прав на цифровые изображения актуален в наше время, т.к. графические материалы, разработанные автором, могут быть легко скопированы или распространены. Простота кражи чужих графических изображений привело к тому, что каждый день увеличивается их хищение. Исходя из этого, проблема защиты авторских прав на графические изображения актуальна в наше время, и техническим решением данной проблемы является программный продукт, предотвращающий копирование, искажение или распространение авторских материалов.

2. *Метод решения.* Для защиты графических материалов широко используется применение цифровых водяных знаков. Таким образом, для защиты графических материалов от копирования и распространения используется программное обеспечение, основанное на графической защите с применением ЦВЗ на основе криптографического метода Куттер-Джордона-Боссена.[1]

В данном методе ЦВЗ внедряются с помощью изменения цветовых компонентов пикселя. Отдельно взятые биты ЦВЗ неоднократно внедряются в изображение с помощью изменения показателей синего канала в пикселе. Внедрение информации производится по одному биту в один пиксель контейнера. С помощью секретного ключа задаются координаты пикселей, в которые будет произведено встраивание. При внедрении цветовые показатели красного и зеленого цветов остаются неизменными, а цветовые показатели синего – будут изменяться по следующей формуле: $Bx,y^* = \begin{cases} Bx,y + \lambda Yx,y, \text{ при } Mi = 1 \\ Bx,y - \lambda Yx,y, \text{ при } Mi = 0 \end{cases}$, где $\lambda = 0{,}1$; $Yx,y = 0{,}3*Rx,y+0{,}59*Gx,y+0{,}11*Bx,y$. Обозначения: Bx,y – показатель яркости синего цвета с координатами (x, y); Bx,y^* – показатель изменения яркости синего цвета пикселя; Yx,y – показатель яркости пикселя; Mi – i-й бит встраиваемой информации; λ – коэффициент, задающий энергию встраиваемого бита данных [2].

3. *Эффективность.* ЦВЗ должен отвечать следующим свойствам: незримость для человеческого глаз, стойкость к искажению контейнера. Метод Куттера-Джордана-Боссена выполняет необходимые свойства. Достижение незримости для человеческого глаза осуществляется с помощью внедрения битов ЦВЗ именно в синий канал пикселя, так как к данному цвету, человеческий глаз обладает наименьшей чувствительностью.

Достижение стойкости к изменениям графического материала достигается с помощью неоднократного внедрения битов ЦВЗ в разных частях защищаемого изображения.[3]

Таким образом, программное обеспечение, основанное на графической защите с применением ЦВЗ на основе криптографического метода Куттера-Джордана-Боссена, позволяет решать задачу защиты авторской графической информации от несанкционированных кражи и распространения.

Литература

1. Стеганографические системы. Критерии и методическое обеспечение / под ред. В.Г. Грибунина. Саров, ФГУП «РФЯЦ-ВНИИЭФ», 2016. С. 10–29

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: ДМК-Пресс, 2006. С. 106–110

3. Грибунин Г.Ф., Пузыренко А.Ю., Туринцев И.В. Цифровая стеганография. Москва: СОЛОН-ПРЕСС, 2009. С. 8–15.

ТОНКОПЛЕНОЧНАЯ МИКРОСБОРКА С ПОВЫШЕННЫМ ТЕПЛООТВОДОМ И ПОМЕХОЗАЩИЩЕННОСТЬЮ БЕСКОРПУСНЫХ КРИСТАЛЛОВ

А.С. Осипович, А.Г. Черных, В.В. Шульгов

Малый удельный вес, высокие коэффициент теплопроводности, электрические и прочностные свойства алюминиевых анодированных подложек (ААП) наиболее полно удовлетворяют жестким требованиям, предъявляемым к массогабаритным характеристикам и тепловым режимам функционирования схем[1]. Применение ААП при создании микроэлектронных устройств позволяет компоновать их без дополнительного основания.

Основанием разработанной микросборки является анодированная алюминиевая подложка с несквозными углублениями, размеры которых с допуском в большую сторону соответствуют размерам монтируемых в них кристаллов. На дне углубления анодный оксид алюминия отсутствует. Предварительное лужение дна углубления позволяет осуществить пайку кристаллов низкотемпературной припойной пастой, обеспечивая при этом хороший электрический и тепловой контакт. Один уровень металлизации обеспечивает электрическую разводку схемы и возможность монтажа поверхностно-монтируемых компонентов на подложку (SMT) и кристаллов в одном цикле.

Углубление имеет высоту, равную сумме толщины кристалла и толщины припойной прокладки. Это сделано с целью автоматизации процесса разварки кристаллов. После монтажа всех кристаллов и SMD компонентов микросборка закрывается гибкой крышкой из безадгезивного алюминий-полиимидного лакофольгового диэлектрика типа ФДИ-А (ЫУО.037.042 ТУ) производства ООО «Тэтраэдр» (г. Москва, Россия) и соединяется с основанием сваркой в местах, свободных от полиимида. Предпочтительна установка микросборки в герметизированных отсеках(аппаратуре).

Литература

1. Sokol V., Shulgov V. Aluminiumunterlagen für die mikroelektronischen Einrichtungen / 9.Chemnitzer Fachtagung Mikromechanik & Mikroelektronik, Chemnitz, 5./6. November 2009. S. 138–140.

ОБУЧАЮЩИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ «КВАНТОВЫЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

С.А. Павлюковец, М.П. Патапович, И.В. Бычек

В современных условиях инновационного развития Республики Беларусь, перехода к экономике знаний, научные исследования в учреждениях высшего образования и их связь с потребностями реального сектора экономики приобретают особую значимость, так как, являясь составной частью учебного процесса, они в первую очередь обеспечивают основу образования и его практико-ориентированную направленность.

Совокупность инфокоммуникационных технологий и проводимых научных исследований

позволяет повысить качество и эффективность подготовки специалистов. К таким инструментам относится электронный учебно-методический комплекс (ЭУМК), представляющий собой программно-методический обучающий комплекс, включающий систематизированные учебные, научные и методические материалы по учебной дисциплине и призван обеспечить реализацию учебных целей и задач на всех этапах образовательного процесса.

В данной работе авторы рассматривают использование материалов авторского ЭУМК как возможные пути повышения эффективности учебного процесса в рамках перехода на двухуровневую систему высшего образования «бакалавр-магистр».

Дисциплина «Квантовые системы для обеспечения информационной безопасности» II-ой ступени высшего образования заочной формы обучения учреждения образования «Белорусская государственная академия связи» специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности» призвана формировать у обучающихся теоретические знания и практические навыки, необходимые для разработки и проектирования квантовых систем безопасности различного уровня и назначения.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

В.И. Пачинин, В.А. Пуйдак, Г.В. Сечко, М.А. Тимонович, И.С. Харкевич

Рассматривается защита конфиденциальной персональной информации пациентов в белорусских медицинских учреждениях. Источником такой информации может быть электронная медицинская карта (ЭМК), широкое внедрение которой в поликлиниках Минска началось в 2018 г. и согласно планам Министерства здравоохранения Республики Беларусь должно полностью завершиться к 2020 г. По мнению авторов доклада, внедрение ЭМК в Беларуси будет осложнено отсутствием белорусского закона «О персональных данных», проект которого Национальное собрание Республики Беларусь планирует обсуждать только в 2019 г. Таким образом, сегодня в Беларуси никто не требует у пациента согласия на обработку его персональных данных из ЭМК, что предусмотрено статьей 6 (пункт 1 подпункт 1.1) закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ. Следовательно, доступ к персональным данным пациента при обработке ЭМК автоматически получает целый круг медицинских работников, обрабатывающих данные [1], а правовой гарантии защиты этих данных в Беларуси пока нет. В этом аспекте в России у пациента больше возможностей: не согласившись на обработку своих данных без своего участия пациент может разместить эти данные в архиве, доступ к которому будет иметь только он с помощью системы распознавания личности по радужной оболочке глаза (РОГ) [1]. Стоимость такой системы в последние годы резко снижается за счет сканирования РОГ с помощью смартфона. Обработку данных из архива медицинский работник сможет вести только в присутствии пациента и под его контролем (либо в присутствии доверенного лица пациента, имеющего доступ к архиву). Тем самым пациент получит высокий уровень защиты своих данных (если ему это, конечно, необходимо).

Литература

1. Ситник, М. Ю. Состояние защиты персонифицированных медицинских данных в Беларуси в 2018 году // Материалы 54-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8 «Информационные системы и технологии». Минск, 21 апреля 2018 г. С. 92–94.

ИСПОЛЬЗОВАНИЕ МОДУЛЯЦИИ ПОЛОЖЕНИЕМ ИМПУЛЬСА В ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

В.Т. Першин

Система радиочастотной идентификации (Radio Frequency IDentification, RFID) объектов в общем случае содержит три компонента: считыватель (ридер), идентификатор (карта, метка, тег) и компьютер. Считыватель излучает в окружающее пространство электромагнитную энергию. Идентификатор принимает сигнал считывателя и формирует

ответный сигнал, который принимается антенной считывателя, обрабатывается его электронным блоком и по интерфейсу направляется в компьютер. Таким образом, ридер имеет приемо-передающее устройство и антенну, которая посылает сигнал идентификатору и принимает ответный сигнал. До последнего времени RFID-системы были более дорогими по сравнению со штрих-кодовыми системами бесконтактной идентификации. Однако прогресс в области идентификаторов и использование новых радиоинформационных технологий привели к тому, что они стали применяться в областях, в которых раньше использовались только штрих-коды.

Мы предлагаем использовать управление системой обратной связи с ридером RFID, применяя модуляцию положением импульса (Pulse Position Modulation, PPM) путем генерирования временных перескоков сверхширокополосных сигналов (Ultra Wide Band, UWB). Использование таких сигналов является наиболее эффективным способом борьбы с подслушиванием, так как злоумышленник практически не может обнаружить выполнение обмена информацией в работающей системе радиочастотной идентификации объектов, поскольку сигналы UWB дают возможность восстановить данные, даже если мощность сигнала вплотную подходит к уровню теплового шума. В докладе изложены результаты моделирования сигналов UWB гауссовской формы и их корреляционной обработки, выполненного в математическом пакете прикладных программ MATLAB. Расчеты проведены для импульсов длительностью от 0,2 до 0,8 пс гауссовсой формы.

ФОРМИРОВАНИЕ ФРЕЙМА ДАННЫХ ДЛЯ ЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

В.Т. Першин

В докладе предлагается использовать фрейм длительностью 10 мс для защищенных систем радиочастотной идентификации (Radio Frequency IDentification, RFID) объетов, отводя при этом интервал длительностью 2 мс на преамбулу для обеспечения синхронизации ридера с идентификатором, а оставшуюся часть фрейма отвести под передачу данных. Позиции импульса выбираются посредством криптографического секретного псевдослучайного генератора чисел (Cryptographically Secure Pseudo Random Number Generator, CSPRNG), так как CSPRNG используется для выбора кода модуляции более эффективно, чем для шифрования. В этом случае можно использовать простой блок шифра, работающего в цепи обратной связи. В предлагаемом формате фрейма можно использовать 16-битный блок шифра, так как никакой стандартный код не использует коды такой длины блока, и выбирать его можно вместо достаточно широко применяемого 64-битного кода, формируя выход каждого шифра для 4 подпоследовательностей позиций импульса в сверхширокополосных сигналах (Ultra Wide Band, UWB). Ключ блока шифра предопределяется секретом, известным ридеру и идентификатору. декодирование сигнала требует, чтобы декодер имел надежную синхронизацию передатчика и приемника. В большинстве случаев реализовать этот механизм не получается, так как собственно используемый сигнал не обеспечивает уверенное декодирование, поэтому для восстановления синхронизации можно использовать манчестерское кодирование информации или применять дифференциальную PPM, так как такая версия кодирования фактически передает данные без использования синхронизации. В этом случае задержка между импульсами не опирается на передний фронт импульса синхронизации. Вместо этого каждая задержка опирается на задний фронт предыдущего импульса. При дифференциальной PPM длительность кодированного сигнала не фиксируется, в то время, как простая PPM всегда создает кодированный сигнал фиксированной длительности, которая формируется только количеством битов и периодом синхронизации.

СИСТЕМА ОХРАННОГО ТЕЛЕВИДЕНИЯ С ДОПОЛНЕНИЕМ ВИДЕОНАЛИТИКИ

С.Н. Петров, Д.В. Ахраменко, С.В. Власюк

Система охранного телевидения предназначена для визуального контроля обстановки на охраняемом объекте с использованием средств телевизионной техники и формирования сигнала тревоги при детектировании проникновения на объект. При попытке

несанкционированного проникновения нарушителя на территорию охраняемого объекта происходит оповещение подразделения охраны.

На сегодняшний день видеонаблюдение стало неотъемлемой частью комплексной системы безопасности любого объекта. Если охраняемый объект большой, то оператору сложно уследить за всеми событиями, происходящими в защищаемой зоне. В таких случаях оправдано использование систем видеоаналитики, которые позволяют анализировать материал, поступающий с видеокамер, в режиме реального времени либо в виде архивных записей, а затем в автоматическом режиме собирать данные и формировать отчеты по различным инцидентам информационной безопасности. Также широко используется возможность создавать визуальные зоны охраняемого объекта и при нарушении их, формировать сигнал тревоги. Сбор данных проходит без участия оператора, однако при фиксации инцидентов, связанных с безопасностью, системы видеоаналитики извещают об этом сотрудника службы безопасности.

Программная часть может включать в себя модули распознания лиц (интеграция с базой МВД), распознания автомобильных номеров, отслеживания движущихся объектов, детекции дыма, огня и звука, контроля активности персонала, обнаружения оставленных предметом и прочие, а также кодеки для сжатия видеосигнала. Аппаратная часть включает серверы видеозаписи, коммутаторы, мониторы, дисковые массивы, камеры различного типа (PTZ- и IP-камеры, тепловизоры).

Архитектура территориально-распределенной системы защиты периметра с использованием видеоаналитики предполагает передачу данных по IP-сетям, а также возможность интеграции с облачными сервисами. При этом возникают такие угрозы информационной безопасности, как несанкционированное прослушивание трафика, его модификация, проведение атаки типа отказ в обслуживании (DoS). Наиболее эффективным решением этих проблем является использование криптографической защиты. Однако, применение криптографии приводит к увеличению объема передаваемого трафика (так называемый IPsec Overhead при использовании VPN-тоннелей), а значит требуются каналы связи с высокой пропускной способностью. Также актуальным вопросом становится аппаратная поддержка алгоритмов шифрования используемым процессором.

ПРИМЕНЕНИЕ СЕРВИСА SELFPORTAL ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО КОНТРОЛЯ РЕСУРСОВ ПРЕДПРИЯТИЯ

А.С. Петрович, И.С. Зайкина

Применение в корпоративных сетях технологий виртуализации получило большую популярность. Предприятие занимается ИТ-аутсорсингом и предоставляет ресурсы сотрудников сторонним организациям. В связи с данной спецификой работы, в рабочем процессе может применяется нескольких систем виртуализации: VMWare, vSphere и OpenStack. Для удобного управления, обеспечения безопасного контроля ресурсов и экономии бюджета предприятия используется бесплатная система SelfPortal [1].

Безопасный контроль достигался за счет решения двух основных проблем, возникших при росте количества виртуальных машин на предприятии. Первая проблема заключается в неконтролируемом росте числа машин ввиду отсутствия правильной системы контроля за высвобождением неиспользуемых вычислительных мощностей. С увеличением количества виртуальных машин пропорционально увеличивалось количество векторов атак, которые могли бы быть потенциально использованы злоумышленниками. Вторая проблема – это необходимость построения закрытого участка инфраструктуры, который считался бы небезопасной зоной для проведения тестирования. Ресурсы такой зоны могли бы свободно выделяться пользователям без риска для основной системы.

В докладе обсуждается эффективность применения системы SelfPortal в вычислительной сети крупного предприятия. Данное средство позволило не только обеспечить контроль ресурсов предприятия, но и сократить время на развертывание виртуальных машин (конечный пользователь может получать доступ к сложным системам всего за 15 минут, до применения системы – в среднем 45 минут). Эффективность возросла

за счет упрощения настройки виртуальной машины, предоставляя «из коробки» самые распространенные конфигурации. Таким образом, около 70% запросов на проведение работ по развертыванию виртуальных машин отпадают за счет самообслуживания пользователей, что значительно облегчает работу системного администратора.

Литература

1. Open-sourcing SelfPortal [Электронный ресурс]. – URL: https://www.altoros.com/blog/introducing-selfportal-the-panel-to-launch-virtual-machines-in-a-few-clicks/. (дата обращения: 14.05.2018).

УЛУЧШЕНИЕ ХАРАКТЕРИСТИК ДАТЧИКОВ ЗВЕЗДНОГО НЕБА ПУТЕМ ЭЛЕКТРОХИМИЧЕСКОГО ОКРАШИВАНИЯ

А.А. Повжик, А.А. Устименко

Формирование механически прочных и стойких к ультрафиолетовому излучению анодных покрытий на основе пористого оксида алюминия с упорядоченными сквозными порами – капиллярами микро- и наноразмеров является актуальной задачей. Значительный интерес вызывает использование таких покрытий для элементов конструкции датчика звездного неба с минимальным коэффициентом отражения в оптическом диапазоне.

Возможность контролируемого изменения размеров пор и толщины пористой структуры делает пористый оксид алюминия идеальным материалом для создания наноструктур с заданными структурными параметрами и свойствами. Широкие возможности управления структурными параметрами пористого оксида алюминия и получения на его основе различных наноструктурированных материалов делают исследования в данном направлении весьма актуальными.

Одним из важнейших показателей качества датчика звездного неба является коэффициент отражения, который должен стремиться к нулю. Для достижения этой цели проводят электрохимическое окрашивание алюминиевой конструкции датчика. Электрохимическое окрашивание по сравнению с химическим окрашиванием имеет ряд преимуществ. К примеру, исследование воздействия УФ излучения на покрытия с электрохимической окраской и химической окраской красителями показало, что покрытия, окрашенные электрохимическим методом, не изменяют своей способности к поглощению света после воздействия УФ, что позволяет нам говорить об использовании данных покрытий в условиях космоса, в то время, как у покрытий с химическим окрашиванием после воздействия УФ-излучением наблюдается снижение коэффициента поглощения.

ПРИМЕНЕНИЕ VPN ДЛЯ ЗАЩИТЫ ТРАФИКА

В.М. Прудников, Е.А. Якимов

Технология виртуальных частных сетей Virtual Private Network (VPN) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях, позволяет реализовать совокупность различных самостоятельных механизмов безопасности [1, 2].

Безопасная передача данных по незащищенной вычислительной сети использует понятие защищенного канала. Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях эталонной модели OSI взаимодействия открытых систем. Используемый уровень OSI в основном определяет достижимые функции применяемой VPN, ее совместимость с программами информационной системы и взаимодействие со средствами защиты других реализаций. В соответствии с уровнями модели OSI различают VPN второго (канального) уровня, третьего (сетевого) уровня, пятого (сеансового) уровня.

Для защиты передаваемого трафика при построении VPN применяются протоколы нижних уровней модели OSI, что обеспечивает прозрачность для приложений и прикладных протоколов информационной системы. При этом обнаруживается проблема корреляции протоколов защиты от используемых стандартов сетей. При применении протоколов верхних уровней способ защиты трафика теряет корреляцию с сетевыми технологиями, что дает определенные преимущества, но при этом протокол теряет прозрачность и приложение зависит

от реализуемого протокола защиты. Чтобы компенсировать негативные последствия предлагается реализовывать способы защиты трафика, которые комбинируют протокольные сущности разных уровней модели OSI.

Литература

1. Комплексная система защиты информации на предприятии: учебно-методическое пособие / Ю.Н. Загинайлов [и др.]. Барнаул: АлтГТУ. 2010. 287 с.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2006. 958 с.

МЕТОДИКА ОПЕРАТИВНОГО КОНТРОЛЯ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ОПЕРАТОРСКИМИ ГРУППАМИ

Н.В. Пушкарева, В.А. Гущо

Контроль психофизиологического состояния (ПФС) операторов иерархических систем высокой ответственности (ИСВО) выполняется поэтапно. На первом этапе производится отбор операторов боевых расчетов (БР). Кандидаты, отвечающие требованиям относительно низких профессионально важных качеств операторов (относительно низкого ранга), не допускаются ко второму уровню тестирования.

Отобранные операторы, отвечающие требованиям относительно высоких и относительно средних профессионально важных качеств операторов (относительно высокого и среднего рангов), переходят ко второму этапу – определению критерия для подбора психологически совместимых операторов БР. Разрабатываются математические модели подбора расчетов ИСВО на базе ПЭВМ. Коэффициенты полученной регрессионной модели операторов относительно высокого уровня профессионально важных качеств принимаются в качестве максимального уровня ($K_{\max}$) критерия подбора. Коэффициенты полученной регрессионной модели операторов относительно среднего уровня профессионально важных качеств принимаются в качестве минимального уровня ($K_{\min}$) данного критерия подбора.

На третьем этапе методики контроля производится подбор психологически совместимых операторов ИСВО на основе критерия оптимальной согласованности. Боевые расчеты, укомплектованные подобранными операторами, приступают к выполнению возложенных на них обязанностей.

На четвертом этапе выполнения методики проводится периодический контроль деятельности операторов ИСВО и оценка их ПФС по полученному критерию. Если коэффициенты полученной математической модели находятся за пределами полученного критерия, то принимается решение о проведении повторного контроля и необходимости анализа правильности принимаемых управленческих решений.

ДЕТЕКТИРОВАНИЕ ОБЪЕКТОВ НА АЭРОКОСМИЧЕСКИХ СНИМКАХ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Н.А. Радевич

Задача детектирования объектов на спутниковых снимках обусловлена необходимостью систематизированного учета состояния сельскохозяйственных и жилых территорий, а также ведения иных видов государственной статистики. Существует интерес в проведении структурированного аудита сельскохозяйственных и жилых территорий и последующем мониторинге их состояния.

Для решения существующей задачи по автоматизированной оценке территорий на основании данных, полученных при помощи спутниковой съемки, понадобится обрабатывать и хранить информацию (аэрокосмические снимки) в видимом и ближнем инфракрасном диапазоне для заданных дат и геолокации, которые предварительно необходимо обработать с использованием техник и алгоритмов машинного распознавания образов. Стоит отметить, что для проверки качества нейронной сети необходимо подготовить образцы для обучения с масками и метриками. Визуализация результатов будет происходить на основе методов выделения контуров изображений и полигонального моделирование объектов.

В ходе исследований было определены основные направления в работе, а также методы и необходимый инструментарий для работы над приложением. Данное приложение позволит автоматизировать процесс сбора информации со спутниковых снимков и создавать карты, предоставляющие данные о местоположении интересующих объектов, отслеживая динамику роста/снижения площадей под застройки, а также снизить трудозатраты аналитиков (решение задачи по оценке территории).

ОСНОВНЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО УЧЕТА РУКОВОДЯЩИХ КАДРОВ (АИС «РЕЗЕРВ»)

С.М. Радыно

Главной целью обеспечения информационной безопасности АИС «Резерв» является защита интересов субъектов информационных отношений при создании и функционировании информационных ресурсов органов государственного управления от возможного нанесения недопустимого ущерба активам посредством незаконного использования информационных ресурсов, несанкционированного вмешательства в процесс функционирования или несанкционированного доступа к обрабатываемой, передаваемой или хранящейся в ней информации. Это достигается путем решения следующих задач:

1. Соблюдение требований нормативных правовых актов Республики Беларусь, регламентирующих порядок обработки и хранения документированной информации;
2. Предотвращение доступа неавторизованных пользователей и разграничение прав зарегистрированных пользователей к активам АИС «Резерв»;
3. Обеспечение доступности информации в случаях преднамеренных воздействий на объект с целью отказа в обслуживании пользователей информационных ресурсов, а также отказов технологического оборудования;
4. Обеспечение конфиденциальности, целостности, доступности и подлинности информации при ее хранении, обработке и передаче по защищенным каналам связи;
5. Защита от несанкционированной модификации и контроль целостности используемых в АИС «Резерв» программных средств;
6. Регистрация действий пользователей в системных журналах и периодический контроль корректности действий путем анализа содержимого этих журналов;
7. Обеспечение аутентификации пользователей АИС «Резерв»;
8. Обнаружение и деактивация вредоносных программ;
9. Выявление источников угроз безопасности информации, причин и условий, способствующих реализации угроз, создание механизма оперативного реагирования на угрозы безопасности информации.

БЕЗОПАСНОЕ ПРЕРЫВАНИЕ ПРОЦЕДУР КООРДИНАЦИИ СЕРВИСОВ

М.П. Ревотюк, О.В. Кот

Предмет рассмотрения – способ компактного представления в произвольный момент состояния распараллеливаемых и мигрируемых процедур оптимальной координации 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. № 25 (1). P. 1–25.

ПРОАКТИВНЫЙ АЛГОРИТМ КООРДИНАЦИИ СИСТЕМ АГЕНТОВ

М.П. Ревотюк, А.К. Пушкина

В процессе координации систем взаимодействующих агентов необходимо регулярно решать задачу о динамическом назначении свободным агентам новых возникающих задач [1] с учетом реальных ограничений и возможной коррекции плана назначения с учетом текущего состояния. Традиционно задачи координации агентов сводятся к известным задачам дискретной оптимизации, таким как линейная задача о назначении или задача нескольких странствующих коммивояжеров. Однако необходимость учета реальных отношений между агентами и задачами приводит к экспоненциальной сложности алгоритма формирования оптимального назначения и часто делает их практически не реализуемыми.

Используя понятия наиболее раннего и позднего срока начала решения задачи, можно проводить жадный упреждающий поиск 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. Предлагается дополнить такую процедуру накоплением на интервалах ожидания заявок информации о множествах альтернативных кратчайших путей для дальнейшего сокращения задержки на обработку прогнозируемых заявок.

Реализация предлагаемой схемы проактивного управления возможна на рекуррентных сетевых моделях, 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.

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.

КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ КАК КОДЫ ХЕММИНГА И ОБОБЩЕННЫЕ КОДЫ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

Е.В. Реентович, В.А. Липницкий

Квадратично-вычетные коды являются обобщением кодов Боуза-Чоудхури-Хоквингем. В настоящее время БЧХ коды являются наиболее распространенными по сравнению с остальными видами кодов. Они нашли свое применение в различных областях информатики и радиоэлектроники, таких как сети и системы телекоммуникаций, системы радионавигации, радиолокации, телевидения, вычислительные машины и системы, компьютерных сетях, связана с теорией групп, колец и полей, теорией чисел и полиномов и т.д. Однако, в общем случае, с ростом длины, параметры БЧХ кодов (скорость, минимальное расстояние) становятся хуже.

В свою очередь, известно, что с ростом длины параметры КВ-кодов становятся только лучше или, как минимум, не ухудшаются, что сделало множество КВ-кодов популярным объектом для исследований. Однако процесс исследования этих объектов весьма затруднителен, КВ-коды плохо поддаются декодированию.

В данной работе строится способ декодирования квадратично-вычетных кодов при помощи теории норм синдромов, основанной на инвариантности норменных и полиномиальных орбит ошибок. Были изучены квадратично-вычетные коды длины 31 и 73. Для них были построены норменные, полиномиальные орбиты, построен алгоритм декодирования данных кодов в системе компьютерной алгебры Wolfram Mathematica. Данный алгоритм отличается своей простотой, скоростью и эффективностью.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ АУТЕНТИФИКАЦИИ В СИСТЕМАХ IoT

Н.С. Руденко, Г.А. Власова

Тенденция массового перехода от интернета персональных компьютеров к интернету вещей (Internet of Things, IoT) ставит новые задачи по обеспечению надежности и безопасности работы сетей. Одним из основных средств защиты информации для IoT является использование криптографических алгоритмов. В связи с тем, что многие приспособления в сети мобильны и зачастую имеют небольшие размеры, существуют общие ограничения на ресурсы времени и памяти. Эти ограничения распространяются и на криптографические схемы, открывая новое направление – разработки и исследования алгоритмов малоресурсной криптографии (Lightweight Cryptography, LWC).

В настоящее время наиболее «легковесными» являются алгоритмы асимметричной криптографии, работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography). Типичными значениями параметров различных процессоров, предназначенных для вычислений с эллиптическими кривыми, являются величины энергопотребления в пределах 10–40 μW и размеров микросхемы 10,000–20,000 GE (условных логических элементов, Gate Equivalent). Известные реализации алгоритма RSA значительно превышают 15,000 GE. По сравнению с симметричной криптографией, асимметричная криптография с безопасной длиной ключа, реализованная на аппаратном уровне, по прежнему требует значительно больших ресурсов (по крайней мере 10000 дополнительных логических элементов), при этом реализуется вполне приемлемая скорость работы. Для криптографии с открытым ключом верхняя граница на размер микросхемы устанавливается в 15,000 GE. Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 секунду, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, создает наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Одним из наиболее надежных симметричных алгоритмов является ГОСТ 28147-89. Результаты сравнений популярных симметричных шифров показывают, что ГОСТ 28147-89 при аналогичной криптостойкости обладает достаточным для IoT быстродействием. Также хорошие результаты показывают отечественные алгоритмы, собранные в библиотеке bee2.

В результате можно сделать вывод о том, что использование малоресурсных криптографических алгоритмов для аутентификации в сетях IoT вполне возможно и не практически не влияет на удобство их эксплуатации пользователем.

ЛЕГКОВЕСНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Т.Х. Рустамов

Легковесная криптография – раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования. Области блочного шифрования наиболее популярными легковесными алгоритмами считаются CLEFIA и PRESENT. Оба алгоритма известны еще с 2007 г. В 2012 г. организации ISO и IEC включили алгоритмы PRESENT и CLEFIA в международный стандарт

облегченного шифрования ISO/IEC 29192-2:2012. В феврале 2014г. стало известно о разработке нового легковесного блочного шифра Halka. Его основное отличие − использование восьмибитных *S*-боксов, в то время как большинство других блочных алгоритмов с легковесными свойствами используют четырехбитные *S*-боксы. Использование же восьмибитных *S*-боксов гарантирует более высокую криптостойкость. В рамках проекта eSTREAM, существовавшего с 2004г. по 2008г. в качестве конкурса на разработку поточных шифров, в числе «победителей» оказались такие легковесные поточные шифры, как Grain (версия 1), MICKEY (версия 2) и Trivium.

На сегодняшний день известны такие механизмы легковесной хэш-функции, как S-Quark и D-Quark, PHOTON и SPONGENT. Все эти алгоритмы, как и победитель конкурса SHA-3 Keccak, основываются на принципе криптографической губки, что позволяет оперировать с данными произвольной длины, как на входе, так и на выходе алгоритма. В конце декабря прошлого года криптографическому сообществу стало известно еще об одной разработке легковесной хэш-функции под названием LHash. Авторы заявляют, что созданный ими механизм, расширяющий описанный ранее принцип криптографической губки, позволил разработать компромиссный по безопасности, скорости, энергозатратам и стоимости реализации алгоритм.

В области криптографии с открытым ключом вопрос поиска оптимального легковесного алгоритма, сравнимого по надежности с RSA или с алгоритмами, основанными на эллиптических кривых, остается открытым, поскольку асимметричные системы более требовательны к временным ресурсам, чем симметричные. Однако некоторые достижения в этом направлении все же имеются, например, в работе для пассивных RFID-систем.

В настоящее время наиболее «легковесными» являются алгоритмы асимметричной криптографии, работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography). Типичными значениями параметров различных процессоров, предназначенных для вычислений с эллиптическими кривыми, являются величины в пределах 10–40 μW и 10000–20000 GE. Близкими к ним являются и значения параметров у процессоров, предназначенных для вычислений с гиперэллиптическими кривыми (HECC – HyperElliptic Curves Cryptography).

Таким образом, по сравнению с симметричной криптографией, асимметричная криптография с безопасной длиной ключа, реализованная на аппаратном уровне, по-прежнему требует значительно больших ресурсов (по крайней мере, 10000 дополнительных логических элементов), при этом реализуется вполне приемлемая скорость работы. Для криптографии с открытым ключом верхняя граница на размер микросхемы устанавливается в 15000 GE.

Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 с, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, по-видимому, создает наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Литература

1. Жуков А.Е. Легковесная криптография: нетребовательная к ресурсам и стойкая к атакам // Материалы форума PositiveHackDays 2012.

2. PRESENT: An Ultra-Lightweight Block Cipher. CHES / A. Bogdanov [et al.]. 2007. № 4727. P. 450−466.

НОВЫЕ СРЕДСТВА БЕЗОПАСНОСТИ WINDOWS SERVER 2012/16. ДИНАМИЧЕСКИЙ КОНТРОЛЬ ДОСТУПА

В.Т. Садовский, В.Д. Мильто, Е.А. Зайченко

Изучение свойств, функций операционных систем семейства Windows Server является актуальной задачей для дисциплин «Администрирование и программирование распределенных приложений», «Системное программное обеспечение» по специальности «Автоматизированные системы обработки информации». В практике применения Windows Server 2012/16 [1, 2] динамический контроль доступа представляет собой наиболее фундаментальное изменение по безопасности доступа к ресурсам сети. В более ранних версиях

доступ к ресурсам файлового сервера, к принтерам и другим устройствам в доменной сети с контроллером домена и службой каталогов Active Directory осуществлялся при помощи списков доступа Access Control List (ACL), а для более защищенных ресурсов с применением шифрования – службы управления правами (Rights Management Services). С помощью этих средств администратор мог назначить права доступа к папкам, файлам для определенного пользователя, используя только его членство в определенной группе безопасности домена. При большом количестве общих папок и других ресурсов приходилось создавать большое количество групп в домене.

Динамический контроль доступа Dynamic Access Control Windows Server (DAC) создает дополнительный уровень безопасности, применение этой технологии позволяет сконфигурировать права доступа к папкам и файлам, учитывая не только членство в группах безопасности, но и другие параметры пользователей и устройств, зафиксированные в Active Directory сервера, например: Department (Отдел), Country (Страна) и т. п. Технология базируется на трех основных понятиях: классификация документов (на основе свойств файлов, например, местоположение файла); утверждение (сформулированное условие, которое соответствует значениям атрибута пользователя или компьютера); аудит (политика аудита позволяет получить информацию о попытках доступа к конфиденциальной информации).

Литература

1. Microsoft Windows Server 2012. Полное руководство / Р. Моримото [и др.]. М.: ООО «И.Д. Вильямс», 2013. 1456 с.

2. Windows Server 2012 R2. Полное руководство / М. Минаси [и др.]. М.: ООО «И.Д. Вильямс», 2015. 960 с.

ОДНОСТОРОННЯЯ ФУНКЦИЯ НА ОСНОВЕ ТЕОРИИ СЛУЧАЙНЫХ РЕШЕТОК

С.Б. Саломатин

Основные задачи, связанные с построением односторонних функций на основе теории решеток связаны с решением двух задач. Первая – задача декодирования на абсолютном расстоянии d. Если d больше определенной величины, то решение гарантированно существует. Вторая задача связана с декодированием на граничном расстоянии: если решение существует, то оно единственно. Решение этих двух задач на случайных решетках может быть сформулировано в рамках задачи инвертирования функции $f(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod p$.

Определим решетку L как подгруппу векторов по модулю p целых чисел. Дуальную (ортогональную) к ней решетку обозначим как D. Конечное множество точек Q решеток образуют множество с координатами в $\{0, 1, \ldots, p-1\}$.

Дуальные решетки могут быть использованы для получения различных (эквивалентных) конструкций односторонних функций. Образуем решетку $L(\mathbf{A})$ из случайной матрицы $\mathbf{A}$ массива целых чисел с модулярной операцией. Тогда решение двух основных задач криптографических решеток в рамках выбора случайной точки $\mathbf{v}$ и вектора ошибки $\mathbf{x}$ и получения целевого показателя $\mathbf{t} = \mathbf{v}+\mathbf{x}$. Решетки периодичны по модулю p, все векторы редуцированы по модулю p и точка решетки может быть выбрана из массива конечного множества $L \bmod p$ с равномерным распределением. Случайная точка представляется как $v = \mathbf{A}\mathbf{s} \bmod p$. Односторонняя функция имеет вид A’$\mathbf{s} + \mathbf{x} \bmod p$, где вектор $\mathbf{s}$ принадлежит векторному массиву целых чисел. Односторонняя функция имеет два входа: вектор $\mathbf{s}$ из массива случайных чисел с равномерным распределением и вектор ошибки $\mathbf{x}$, соответствующий заданной функции f. Функция становится свободной от коллизий при достаточно большом размере вектора $\mathbf{x}$.

Односторонняя функция на основе случайных решеток может быть использована в схемах сетевого кодирования и системах связи.

ИНСТРУМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЯЗЫКЕ GOLANG

С.М. Сацук, Д.В. Брынза

В последние годы происходит серьезное развитие языка программирования Go или Golang. Это компилируемый многопоточный язык программирования, разработанный внутри компании Google для совершенствования микросервисной архитектуры веб приложений, работы с большими базами данных, развития параллелизма (concurrency). В настоящее время Golang начинает использоваться во многих компаниях, позволяя переходить от монолитных приложений к микросервисам, быстрее осуществлять транзакции, обрабатывать больше данных и экономить на серверном оборудовании.

В связи с этим, одной из серьезных проблем, связанной с использованием языка программирования Go является защита web-приложений от взлома. Наиболее типичными способами взлома таких приложений являются: предсказуемое значение идентификатора сессии (Credential/Session Prediction); межсайтовая подделка запроса (CSRF); межсайтовое выполнение сценариев (Cross-site Scripting, XSS); внедрение операторов SQL (SQL Injection).
Для непосредственной защиты инструментариев языка можно использовать правильную защиту сессий и cookie с помощью технологии JSON WebTokens, CSRF (борьбу с межсайтовой подделкой запроса или CSRF атаками на сайт). С этой задачей в Go очень хорошо справляется библиотека NoSurf. На основе контекста запроса формируется токен, который впоследствии вставляется в необходимые поля и заголовки. Атака XSS или межсайтинговый скриптинг – это тип атаки на веб-систему, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода. Самый известный пример – это угон пользовательских cookies злоумышленником. Secure – небольшая прослойка для удобной настройки безопасных параметров сервиса. Secure умеет работать как с большим количеством фреймворков, так и со стандартным пакетом net/http. SQl-injection – один из распространенных способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SafeSQL – это статический анализатор кода для Go, который позволяет находить SQL injections.

Несмотря на то, что Golang довольно новый язык программирования, комьюнити очень быстро разрастается и реализует базовые решения, которые встречаются почти в каждом проекте, в том числе и решения, основанные на безопасности веб-приложения.

ОЦЕНКА ИНТЕНСИВНОСТИ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ, СОЗДАВАЕМОГО АБОНЕНТСКИМ ОБОРУДОВАНИЕМ СОТОВЫХ РАДИОСЕТЕЙ В МЕСТАХ С ВЫСОКОЙ ПЛОТНОСТЬЮ НАСЕЛЕНИЯ

А.С. Свистунов

В настоящее время в связи с увеличением территориальной плотности радиооборудования сетей сотовой связи и массовым активным пользованием различными услугами сотовой радиосвязи большой интерес представляет вопрос об электромагнитной безопасности сотовых радиосетей в часы наибольшей абонентской нагрузки в местах с высокой плотностью населения, особенно в местах скопления абонентов.

В работе выполнены оценки уровня суммарной интенсивности электромагнитного поля (ЭМП), создаваемого электромагнитным излучением абонентских устройств (АУ) сотовых радиосетей стандарта GSM на городских территориях. Результаты получены путем компьютерного моделирования распространения радиоволн (РРВ) с применением трехмерной модели РРВ (X3D-модель) и трехмерной модели фрагмента типовой городской застройки с высотой зданий 6–20 м. Моделирование проводилось при следующих системных параметрах сотовой радиосети: территориальная плотность АУ в активном состоянии $\rho_{MS} = 0{,}32$ АУ/м^2, территориальная плотность базовых станций (БС) $\rho_{BS} = 3$ БС/км^2, высота подвеса антенн $H_{BS} = 25$ м, высота антенны АУ над земной поверхностью $H_{MS} = 1{,}5$ м, значение отношения «несущая/помеха» на входе радиоприемника БС $C/I = 15$ дБ. Суммарная интенсивность ЭМП анализировалась на уровне 1,5 м от земной поверхности; минимальное расстояние от АУ до точки наблюдения составляет 0,4 м.

При относительно плохих условиях РРВ от АУ к БС (условиях затенения мест скопления абонентов зданиями) суммарная интенсивность ЭМП, создаваемая электромагнитным излучением АУ, может достигать 0,08 Вт/м^2. Предельно допустимый уровень ЭМП сотовой связи, ограничивающий вынужденный риск для здоровья населения, в Республике Беларусь составляет 0,1 Вт/м^2. При ρ_{MS} = 0,16 АУ/м^2 верхняя граница диапазона суммарной интенсивности ЭМП, создаваемого электромагнитным излучением АУ, составляет 0,06 Вт/м^2. В случае нахождения АУ в прямой видимости с ближайшей БС этот уровень снижается до 0,001 Вт/м^2.

Таким образом, при относительно плохих условиях РРВ от АУ к БС в местах скопления абонентов излучение АУ в активном состоянии может вносить существенный вклад в общий уровень ЭМП, создаваемый многими другими источниками электромагнитного излучения.

ПРОТОКОЛ ЗАЩИТЫ ТРАНСПОРТНОГО УРОВНЯ

М.А. Севостьянюк, А.С. Шелягович

Протокол TLS шифрует интернет-трафик любого вида, тем самым делая безопасными общение и транзакции в сети. Если ваши данные не шифруются, любой может проанализировать их и прочитать конфиденциальную информацию. Кроме веб-трафика, TLS также используется в почте и системах телеконференций. TLS использует самый безопасный метод шифрования – асимметричный. Так как в асимметричном шифровании применяются сложные математические расчеты, нужно много вычислительных ресурсов, поэтому TLS решает эту проблему, используя шифрование только в начале сессии, чтобы зашифровать общение между сервером и клиентом. Сервер и клиент должны договориться об одном ключе сессии, который они будут вдвоем использовать, чтобы зашифровать пакеты данных. Основной целью создания данного протокола являлось получение относительно безопасного канала для осуществления покупок или управления банковским счетом. В современном Интернете на TLS полагаются не только в коммерческой деятельности, но и при решении гораздо более общей задачи сохранения приватности и конфиденциальности важной информации. Одним из самых распространенных применений TLS является HTTPS. HTTPS стремительно вытесняет незащищенную версию (HTTP): доля зашифрованного веб-трафика растет, скорее всего, в скором будущем ожидается, что, практически весь веб-трафик будет зашифрован. Сегодня SSL/TLS – один из самых изученных, исследованных протоколов современного Интернета. Ключевым отличием TLS от SSL является наличие поддержки целого ряда расширений протокола, позволяющих реализовать современные методы защиты информации. На сегодняшний день TLS 1.2 является самой распространенной версией протокола. В новой версии TLS 1.3 будет совместимость с предыдущими версиями: например, соединение откатится до версии TLS 1.2, если одна из сторон не сможет использовать более новую систему шифрования в списке разрешенных алгоритмов протокола версии 1.3. Однако при атаке типа активного вмешательства в соединение, если хакер принудительно попытается откатить версию протокола до 1.2 посреди сессии, это действие будет замечено, и соединение прервется. Версия 1.3 протокола TLS, которая скоро будет выпущена, решает множество проблем с уязвимостями тем, что отказывается от поддержки устаревших систем шифрования [1, 2].

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. М.: ЗАО Компьютерное издательство «Диалектика», 2016. 221 с.

2. Бабаш А. Криптографические методы защиты информации. Т. 1. М.: Инфра-М, 2013. 124 с.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ РЕЧЕПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА КАЗАХСКОМ ЯЗЫКЕ

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

Методы формирования речеподобных сигналов на русском и белорусском языках рассматриваются в работах [1–3]. Для формирования речеподобных последовательностей на казахском языке за основу можно использовать метод синтеза речеподобных сигналов

на русском и белорусском языках. Особенности формирования речеподобных последовательностей на казахском языке связано с законом сингармонизма (гармонии гласных звуков и гармонии согласных звуков).

Для казахского языка в слове могут сочетаться только твердые, либо только мягкие гласные. Слова иностранного происхождения арабские, персидские и русские могут содержать как мягкие, так и твердые гласные. При формировании речеподобных последовательностей казахского языка использовалось ограничение на применение в одном слове (в корне слова и производных основах) либо мягких либо твердых гласных.

Для согласных звуков используется ассимиляция согласных по звонкости и глухости. Если последний звук корня слова глухой или оканчивается на звонкие *б, в, г, д,* то начальный согласный звук аффикса глухой. Если последний звук корня слова глухой согласный *қ, к, п*, а начальный звук аффикса гласный, то глухие *қ, к, п* переходят в *ғ, г, б*.

Звук *а* не употребляется в словах с гласными *ә, е, і, Ө, ү*, а также с мягкими согласными *г, к*. Звук *г* в начале и конце казахских слов, а также с гласными *а, о, у, ы* не употребляется. Его не употребляют в словах и в сочетании с твердыми согласными *ғ, қ*. *Л* в начале слова в казахском языке пишется, но не произносится, поэтому в речеподобных последовательностях она в начале слова не используется. Звук *о* в конце казахских слов не употребляется.

Указанные особенности казахского языка использовались при формировании речеподобных последовательностей, которые преобразовывались в акустические речеподобные сигналы для маскирования речи. Для защиты речевой информации путем ее маскирования рекомендуется использовать комбинированные помехи, включающие «белый» шум и речеподобные сигналы.

В работе рассматривается механизм формирования речеподобных последовательностей с использованием базы аллофонов казахского языка, а также базы суффиксов и окончаний.

При формировании базы структурных элементов казахского языка для синтеза речеподобных сигналов необходимо использовать статистические данные о частотности длины слов в казахском языке, частотности появления букв в начале слова и частотности появления букв в текстах на казахском языке. По формальным признакам речеподобные сигналы должны соответствовать статистическим характеристикам языка.

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

Литература

1. Воробьев В.И., Давыдов А.Г., Давыдов Г.В. Речеподобные сигналы: разновидности, основные параметры, способы формирования, области применения // Доклады БГУИР. 2009. № 3 (41). С. 9–16.

2. Сейткулов Е.Н., Давыдов Г.В., Потапович А.В. База аллофонов для компиляционного синтеза речеподобных сигналов на русском языке // Современные средства связи: материалы XIX Междунар. науч.-техн. конф. Минск, 14–15 октября 2014 г. С. 193–195.

3. Синтез речеподобных сигналов на белорусском языке / Г.В Давыдов [и др.] // Доклады БГУИР. 2015. № 4. С. 27–32.

СОХРАНЕНИЕ ИНФОРМАЦИИ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

А.С. Сиденко, В.П. Бурцева

Система охлаждения (СО) оборудования в центрах обработки данных (ЦОД) имеет сложную конструкцию. Первым, можно сказать, основным недостатком этой СО является ее ненадежность в вопросе защиты информации. Так как в случае отключения электроэнергии СО дает сбой, что может привести к перегреванию серверов, а, следовательно, ставит под удар сохранение на них информации. Вторым недостатком СО в ЦОД является низкая теплопроводность охлаждающего вещества (воздуха), которая влечет за собой низкую эффективность охлаждения. Предложенный способ охлаждения серверов с помощью тепловых трубок (ТТ) одновременно устраняет эти два недостатка. ТТ представляет собой устройство, в основе которого лежит фазовый переход (жидкость–пар) и в настоящее время используется

для отвода тепла и охлаждения, в частности, в ноутбуках. Принцип работы ТТ аналогичен принципу работы термосифона (ТС). Однако ТТ имеет капиллярную структуру, в отличие от ТС. И поэтому работа по охлаждению объекта может происходить в любых положениях ТТ, так как конденсат возвращается в зону поглощения тепла под действием капиллярных сил. К тому же, ТТ имеют ряд преимуществ, таких как: автономность и надежность, столь важные для защиты информации, а также эффективность, бесшумность и компактность. Для увеличения площади контакта ТТ с сервером конструктивно лучше использовать ТТ с квадратным либо прямоугольным сечениями. Все выше перечисленное приводит к концепции расположения сервера на поверхности ТТ. Для проведения исследований изготовлены: экспериментальный ТС и два конструктивно отличающихся друг от друга рабочих радиатора. На основании экспериментальных данных рассчитаны: эффективный коэффициент теплопроводности и термическое сопротивление ТС, что подтверждает правильность выбора ТТ в качестве нового охладительного элемента для оборудования в ЦОД.

ВВЕДЕНИЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ПРИ ФОРМИРОВАНИИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Сидоренко, И.В. Шакинко

На современном этапе развития информационных технологий большинство веб-приложений и интернет-ресурсов обеспечивают передачу изображений. Возникает необходимость в решении задач связанных с защитой цифровых изображений из-за невозможности обеспечения требуемых уровней безопасности передаваемой информации в телекоммуникационных каналах [1]. Для этих целей традиционно используется подход, получивший название цифровые водяные знаки (ЦВЗ). Это специальные метки, встроенные в изображение (или другие цифровые данные) для обеспечения контроля его применения [2].

В данной работе приводятся результаты анализа разработанного алгоритма формирования, встраивания и извлечения ЦВЗ. ЦВЗ формируются при использовании следующих хаотических отображений: логистического, тент-отображения и отображения Бернулли.

Установлено, что ЦВЗ, формируемые на основе различных хаотических отображений, при встраивание в изображение практически не меняют его статистические характеристики.

Результаты тестирования предлагаемого алгоритма свидетельствуют о том, что данный алгоритм является стойким к атакам копирования. При использовании алгоритма допустимы потери фрагмента изображений, а также наличие шумов в канале передачи. При этом в последнем случае возможны изменения более 10 % элементов изображения.

Варьируя пороговым значением уровня шума, изменяя размеры блоков изображения становится возможным различать искажения и модификацию областей изображения, произведенных злоумышленником.

Литература

1. Robust Image Watermarking Theories and Techniques: A Review / H. Tao [et al.] // Journal of Applied Research and Technology. 2014. Vol. 12. P. 122–138.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002 . С. 5.

ОБЗОР МЕТОДОВ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

В.О. Сидорович, А.Е. Варюшина

Провал или успех наших повседневных дел в той или иной степени определяется корректностью функционирования программного обеспечения (ПО), что ставит современное общество в зависимость от уязвимостей в ПО[1].

Уязвимости ПО – критические ошибки, не выявленные в ходе тестирования и не декларированные спецификацией разработчика или заложенные преднамеренно, предоставляющие злоумышленникам исключительные возможности по разглашению

информации, ее модификации, блокированию использования и безостаточному уничтожению без возможности восстановления.

Возможность изменения основных свойств защищенности (доступность, целостность, конфиденциальность) информационных ресурсов и дестабилизации процессов функционирования информационно-вычислительных систем различного назначения посредством применения злоумышленниками несанкционированных воздействий деструктивного характера (атак) на уязвимости ПО предопределяют острую потребность в своевременном обнаружении уязвимостей на этапах разработки и проектирования ПО, проверки соответствия их заявленной политики безопасности и реализации механизмов защиты [2].

При статическом анализе можно обнаружить уязвимости кода даже до того, как код будет готов для запуска. С другой стороны, динамический анализ происходит на работающем программном обеспечении и обнаруживает уязвимости по мере их возникновения, обычно используя сложные инструментальные средства. Кто-то может возразить, что одна форма анализа предваряет другую, но разработчики могут комбинировать оба способа для ускорения процессов разработки и тестирования, а также для повышения качества выдаваемого продукта [3].

Литература

1. Истинная цена программных ошибок [Электронный ресурс]. URL: https://www.osp.ru/os/2009/03/8158133/ (дата обращения: 30.04.2018).

2. Технологии статического и динамического анализа уязвимостей программного обеспечения [Электронный ресурс]. URL: http://cyberrus.com/wp-content/uploads/2014/11/vkb_04_04.pdf (дата обращения: 30.04.2018).

3. Использование статического и динамического анализа для повышения качества продукции и эффективности разработки [Электронный ресурс]. URL: http://www.swd.ru/print.php3?pid=828/ (дата обращения: 30.04.2018).

ЭЛЕКТРОННЫЕ СВОЙСТВА ФОСФОРЕНА, ЛЕГИРОВАННОГО АЗОТОМ

В.А. Скачкова, М.С. Баранова, Д.Ч. Гвоздовский

Последнее десятилетие, важное место в микро- и наноэлектронике занимают двумерные материалы, такие как графен, силицен, германен, гексагональный BN, дихалькогениды переходных металлов и др., благодаря их выдающимся свойствам. Монослой черного фосфора (фосфорен), представляет собой перспективный 2D-материал, который, в отличие от графена, является прямозонным полупроводником с запрещенной зоной, равной ~ 0,3–2 эВ, в зависимости от количества слоев в структуре [1]. Из-за своей «сморщенной» структуры фосфорен обладает сильной анизотропией электронных и оптических свойств [2, 3], и высокой подвижностью носителей заряда. Для исследования электронных свойств монослоя фосфорена, легированного азотом, который замещает один атом фосфора в суперячейке, состоящей из 4×4 элементарных ячейки фосфорена, использовалась теория функционала электронной плотности, реализованная в программе VASP (Vienna An initio Simulation Package)[4]. Энергия связи рассчитывалась путем вычитания из полной энергии легированного фосфорена полной энергии фосфорена с вакансией и полной энергии отдельного атома азота, и составила –6,72 эВ. Такая большая энергия связи говорит о том, что данный процесс легирования энергетически выгоден. Легирование атомом азота не ведет к возникновению магнитного момента. Таким образом, исследование электронных свойств фосфорена, легированного азота показало сильные связи легирующего атома, что говорит о высокой вероятности присутствия этой частицы в образцах фосфорена.

Литература

1. Nat. Nanotechnol. / Y. Du [et al.]. 2015. Vol. 9. P. 372–377.
2. ACS Nano / H. Liu [et al.]. 2014. Vol. **8.** P. 4033–4041.
3. Nat.Commun / F. Xia [et al.]. 2014. 5, 4458.
4. Kresse G. VASP the guide: tutorial. Austria, University of Vienna, 2003. P. 94–104.

АУДИТ ЗАВИСИМОСТЕЙ RAILS ПРИЛОЖЕНИЙ НА ПРЕДМЕТ УЯЗВИМОСТЕЙ

М.В. Стержанов, М.А. Медунецкий, М.П. Хоронеко

Классификацией векторов атак и уязвимостей занимается международная некоммерческая организация OWASP (Open Web Application Security Project). В 2017 году OWASP опубликовал обновленный список из десяти самых опасных векторов атак на Web-приложения, получивший название OWASP TOP-10 [1]. Одним из важных направлений атак является использование компонентов с известными уязвимостями.

Современные Rails-приложения написаны с использованием специальных библиотек или гемов, которые поставляются сторонними компаниями. В большинстве случаев эти компоненты имеют открытый исходный код, что дает миллионам разработчиков по всему миру возможность изучения и анализа на предмет уязвимостей.

Крайне важно использовать последние версии компонентов и следить за появляющимися известными уязвимостями на сайтах типа securityfocus.com.

Ресурс Rubysec содержит текстовую базу данных уязвимостей Rails приложений, которая регулярно обновляется и поддерживается Rails сообществом. База представляет собой набор директорий, имена которых соответствуют именам руби гемов на сайте rubygems.org. Каждая директория содержит один или более справочный текстовый файл, имя которого включает в себя идентификатор CVE (Common Vulnerabilities and Exposures). Каждый справочный файл содержит описание уязвимости в формате YAML.

Для проверки зависимостей Rails проекта сообществом Rubysec предлагается бесплатная утилита bundler-audit, которая устанавливается в проект в виде гема и проверяет наличие потенциально уязвимых зависимостей при помощи анализа файла Gemfile.lock.

Литература

1. OWASP Top 10 – 2017 [Электронный ресурс]. – URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf. (дата обращения: 18.05.2018).

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ 3D-ПРИНТЕРОВ

В.А. Столер

Использование трехмерной печати для быстрого прототипирования изделий предполагает наличие 3D-принтеров с широкими функциональными возможностями. Большинство имеющихся на рынке принтеров имеют свои недостатки, что ограничивает их применение. В работе рассматриваются пути конструктивной и программной модернизации таких принтеров на примере принтера CubeX от 3D Systems (США).

CubeX – современный полупрофессиональный принтер, который по своим параметрам подходит для изготовления изделий небольшой фирмой. Вместе с тем использование принтера CubeX [1] выявило ряд недостатков, влияющих на его работоспособность, а именно: многочисленные изломы прутка пластика, из-за неоправданного длинного маршрута его прохождения к печатной головке (экструдеру); частые «срывы» изделия с рабочего стола-элеватора, из-за отсутствия его подогрева, что в свою очередь ограничивает количество пластиков (филаментов), используемых для печати; 3) невысокая скорость печати, из-за небольшого диапазона варьирования параметрами печати в прилагаемом к принтеру ПО.

Перечисленные проблемы были решены конструктивными изменениями 3D-принтера, а также обновлением его программного обеспечения. Так без больших переделок был значительно сокращен маршрут подачи филамента к экструдеру за счет применения специального крепления для катушек с пластиком, распечатанное самим принтером. Вторая конструктивная проблема решается путем замены элеватора 3D-принтера на поверхность с подогревом и возможностью регулирования температуры нагрева. Последняя доработка принтера коснулась замены фирменного программного обеспечения на программу-слайсер KISSlicer 1.6.2, скачанную с интернета и адаптированную к CubeX, что дало возможность влиять на такие параметры как скорость печати, температуру, форму и толщину слоя печати и подложки, а также позволило менять режимы обдува заготовки при печати, изменяя геометрию получающегося изделия.

Выполненные конструктивно-программные доработки позволяют создать 3D-принтер с расширенными функциональными возможностями, который в обновленном виде способен будет печатать с увеличенной скоростью многими видами пластика без потери качества печати.

Литература

1. Столер В.А. Особенности использования трехмерной печати при решении инженерно-технических задач // Технические средства защиты информации: тезисы докладов XIV Белорусско-российской науч.-техн. конф. Минск, 25–26 мая 2016 г. С. 70.

КИБЕРУГРОЗЫ И ОТКАЗОУСТОЙЧИВОСТЬ

Судани Хайдер Хуссейн Карим, М.Б. Абросимов

Киберугрозы – это возможность (вероятность) несанкционированного проникновения в распределенные информационные системы для копирования, модификации, уничтожения находящихся в них данных или для затруднения или приостановки функционирования программной или аппаратной части информационной системы. Киберугрозы, в основном, исторически будучи формой деятельности отдельных высококвалифицированных преступников, к настоящему времени превратились в форму политического и военного воздействия спецслужб государств и террористических групп, систематически ведущих активную борьбу за передел международных сфер влияния. Объектами вмешательства становятся информационные системы государственного, военного, экономического и социального управления, а также устройства с выходом в Интернет отдельных граждан от чиновников и предпринимателей высокого ранга, известных лиц до рядовых служащих и несовершеннолетних детей. При реализации киберугроз возможные отказы и затруднения в работе информационных устройств, сбои и ошибки при информационных запросах способны привести в масштабе страны к значительным экономическим, военным и социальным последствиям и к ощутимым материальным ущербам. В этой связи, обеспечение отказоустойчивости информационных систем, как способности сохранять свою работоспособность в условиях реализации киберугроз, является актуальной научно-технической задачей, имеющей важнейшее социально-политическое значение. Для решения данной задачи следует определить всю номенклатуру киберугроз для заданной распределенной информационной системы. Каждой киберугрозе необходимо поставить в соответствие ожидаемый информационный, экономический, социальный, военный или иной ущерб, который произойдет в случае ее реализации применительно к рассматриваемой информационной системе. Необходимо оценить способность информационной системы выполнять свои функции в условиях реализации отдельной угрозы или их совокупности. Далее, исходя из результатов оценки, следует определить диапазон мер информационной защиты, а также состав резервных элементов программного и аппаратного обеспечения, который заменит вышедшие из строя элементы системы. Эффективность защиты от киберугроз будет измерена на интервале времени как отношение предотвращенного ущерба от реализации данного вида угрозы к стоимости мер защиты от данного вида угрозы и стоимости резервных элементов программного и аппаратного обеспечения. Уровень отказоустойчивости информационной системы применительно к номенклатуре киберугроз будет определяться заданным уровнем эффективности, для которой защищенность системы вначале будет спроектирована разработчиком, а в процессе эксплуатации будет постоянно совершенствоваться в ответ на возникающие новые формы киберугроз.

МОДИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ИЗМЕНЕНИЯ МЕЖДУСТРОЧНОГО РАССТОЯНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА

А.А. Сущеня, Е.А. Блинова, П.П. Урбанович

Предлагается модификация стеганографического метода изменения смещения междустрочного расстояния электронного документа, так называемого line-shift coding. В его стандартной реализации предлагается скрывать сообщение в изменении междустрочных интервалов. Однако такой метод имеет несколько существенных недостатков: обладает малой

пропускной способностью и может быть выявлен как для электронного документа, так и для его напечатанной копии. Предлагается использовать в качестве стеганографического контейнера документ Microsoft Word и изменять смещение междустрочного интервала только неотображаемых символов. Анализ абзаца штатными средствами не показывает наличия смещения, изменение начертания или размера шрифта не выявляют наличия осажденных данных. Для контроля целостности осажденных данных предлагается также внести изменения в структуру электронного документа. Исходя из того, что файл документа Microsoft Word является архивом, содержащим набор XML файлов, можно использовать метод замены кавычек для размещения контрольной суммы осажденного сообщения.

Разработано программное средство, реализующее данную модификацию стеганографического метода изменения смещения междустрочного расстояния электронного документа с контролем целостности осаждаемого сообщения.

Литература

1. Блинова Е.А. Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа// Труды БГТУ. Сер. Физико-мат. науки и информатика № 6. С. 166–169.

2. Сущеня А.А. Стеганографическое преобразование текстов-контейнеров на основе языков разметки // 68-я научно-техническая конференция учащихся, студентов и магистрантов: сборник научных работ. Ч. 4. Минск, 17–22 апреля 2017 г. С. 145–149.

СИСТЕМА КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ С ВОЗМОЖНОСТЬЮ ПРОВЕРКИ ПОДЛИННОСТИ ИНФОРМАЦИИ И ЕЕ ИСТОЧНИКА

А.М. Тимофеев

В настоящее время одной из наиболее важных задач, решаемых при разработке высокоскоростных систем передачи и приема конфиденциальной информации, является обеспечение проверки подлинности передаваемой информации и ее источника [1]. Такая задача может быть решена путем использования механизмов аутентификации информации и ее источника посредством электронных цифровых подписей (ЭЦП) [1, 2]. При этом используемые алгоритмы ЭЦП, включающие процедуры постановки и проверки подписи, зачастую требуют достаточно больших вычислительных ресурсов и не позволяют обеспечить максимально возможную пропускную способность канала связи. Это объясняется необходимостью генерирования больших простых чисел, вычисления хэш-функций и инверсий в системе наименьших вычетов, а также передачи по каналу связи кроме электронного документа его ЭЦП. В связи с этим целью данной работы являлась разработка высокоскоростной системы передачи конфиденциальной информации, свободной от указанных выше недостатков существующих систем и позволяющей определять подлинность как передаваемой информации, так и ее источника. В работе предложена система конфиденциально связи, информационная безопасность которой основана на использовании процедуры поблочного смешивания данных, подлежащих передачи, с идентификационной информацией отправителя и режимов асинхронной передачи и приема информации при помощи оптических импульсов слабой мощности, которые содержат от одного до нескольких десятков фотонов. Разработанная система связи позволяет обнаруживать факт навязывания ложных данных, которые злоумышленник может пытаться выдавать за подлинные, транслируя в канал связи, а также в автоматическом режиме обнаруживать несанкционированный съем данных, передаваемых по волоконно-оптическому каналу связи.

Литература

1. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. М., НОУ «Интуит», 2016. 608 с.

2. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. СПб., БХВ-Петербург, 2015. 304 с.

СНИЖЕНИЕ УРОВНЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ВИДЕОТРАКТА ПЕРСОНАЛЬНОЙ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНОЙ МАШИНЫ С ИСПОЛЬЗОВАНИЕМ ПОДБОРА ЦВЕТА ТЕКСТА И ФОНА

Н.А.Титович, А.И. Майоров, Д.А. Высоцкий

Угроза утечки конфиденциальной информации, обрабатываемой на персональной электронно вычислительной машине (далее – ПЭВМ), по каналу побочных электромагнитных излучений (далее – ПЭМИ) известна достаточно давно. Особая опасность состоит в том, что даже в случае использования криптографических методов защиты на ПЭВМ угроза утечки по каналу ПЭМИ остается актуальной – злоумышленник может перехватить информацию от составных частей ПЭВМ, которые обрабатывают незашифрованную информацию. Видеотракт ПЭВМ, как правило, обладает наибольшим уровнем излучения ПЭМИ. В настоящее время существует два основных способа защиты информации от утечки по рассматриваемому каналу утечки: пассивный (экранирование ПЭВМ либо помещения, в котором размещена ПЭВМ) и активный (применение генераторов электромагнитного шума в непосредственной близости от ПЭВМ). Предлагаемый метод защиты видеотракта ПЭВМ применим для ПЭВМ, использующих интерфейс VGA. Информация в интерфейсе VGA передается в аналоговом виде по трем цветовым каналам и двум каналам синхронизации: строчному и кадровому. ПЭМИ видеотракта с интерфейсом VGA имеет схожую структуру с аналоговым телевизионным сигналом и представляет суперпозицию излучений трех цветовых сигналов и сигналов синхронизации. Цвет каждого пикселя задается уровнем каждого цветового сигнала. Соответственно, чтобы снизить уровень ПЭМИ необходимо выбирать максимально возможные темные цвета фона и текста, отображаемые на мониторе. Также необходимо максимально затруднить возможность различения злоумышленником текста и фона, этого можно достичь таким подбором цвета текста и фона, при котором сумма напряжений трех цветовых сигналов фона будет равна сумме напряжений цветовых каналов текста. Однако, необходимо сохранить удобство работы пользователя ПЭВМ. Человеческий глаз наиболее восприимчив к зеленому цвету. Проведенные исследования показали, что наиболее читаемым оказался зеленый текст на фоне с оттенками зеленого. Цвета удовлетворяют условию, описанному выше. Таким образом, с помощью представленного метода, можно значительно снизить уровень ПЭМИ, что уменьшит зону технической разведдоступности ПЭВМ и максимально усложнит задачу детектирования принятой злоумышленником информации.

Литература

1. Kuhn M.G. Electromagnetic eavesdropping risks of flat-panel displays [Electronic resource]. – URL: https://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf (date of access: 01.05.2018).

2. Филиппович А.Г. Побочные электромагнитные излучения видеотракта ПЭВМ // Управление защитой информации. 2008. Т. 12, № 1. С. 92–97.

МАЛОГАБАРИТНЫЙ ТЕСТОВЫЙ ГЕНЕРАТОР РАДИОПОМЕХ

А.В. Толмачев, В.М. Чертков

Малогабаритный тестовый генератор радиопомех разработан с целью испытаний радиолокационного оборудования в условиях широкого применения условным противником средств РЭБ с использованием различных тактических приемов. Для полноценной имитации тактической обстановки и формирования тактико-технических требований к генератору радиопомех выполнены: анализ характеристик перспективных отечественных радиолокационных станций [1], анализ применения активного элемента генератора, анализа возможных схем построения с выбранным активным элементом, анализ и выбор типа антенной системы [2]. Рассмотренные тактико-технические требования к имитатору помеховой обстановки позволили определить его общую структурную схему. Была выбрана и обоснована элементная база, выработано наиболее оптимальное схемное решение, которое обеспечивает требования по механической прочности, скрытности, транспортабельности, универсальности,

частотному диапазону, мощности и виду создаваемых помех, что позволило применять его в ходе испытаний радиолокационного обнародования и радиолокационных станций. Выполненное имитационное моделирование и проведенные натурные эксперименты позволили оценить эксплуатационную надежность малогабаритного тестового генератора радиопомех. Разработанный генератор радиопомех возможно использовать в качестве забрасываемого передатчика помех, который будет достаточно эффективным средством для усложнения работы радиолокационных средств противника, а также для тренировки работы операторов на радиолокационных станций, стоящих в настоящее время на вооружении.

Литература

1. Радиолокационная станция обнаружения маловысотных наземных объектов X-диапазона «Родник» [Электронный ресурс]. – URL: http://www.kbradar.by/products/radiolokatsiya/radiolokatsionnye-stantsii/519/ (дата обращения: 10.04.2018).

2. Охрименко А.Е. Основы радиолокации и радиоэлектронная борьба. Ч.1. Москва: Воениздат, 1983. 457 с.

КЛЮЧЕВЫЕ АСПЕКТЫ ПРОЦЕССА МОДЕЛИРОВАНИЯ РИСКОВ ДЛЯ ИНФОРМАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

А.В. Федорцов

Реализация эффективного управления информационной безопасностью (ИБ) в организации связана, в первую очередь, с формализацией координированных действий по руководству и управлению организацией в отношении рисков для материальных активов из состава информационной инфраструктуры. Менеджмент рисков [1], как правило, заключается (но не ограничивается) в последовательном выполнении следующих шагов: оценка рисков, обработка рисков, принятие рисков, обмен информацией о рисках. К ключевым аспектам процесса моделирования рисков для информационной сети организации следует относить вычисление значений вероятностей возникновения особого набора обстоятельств совершения атак на информационную инфраструктуру и ущерба (последствий) от таких событий ИБ для материальных активов [2], необходимых для выполнения количественной оценки рисков. Ввиду отсутствия универсального подхода к количественной оценке ущерба, позволяющего определить результат воздействия на программно-технические средства из состава информационной сети организации, решить задачу оценки последствий можно рассчитав прямой и косвенный ущерб соответствующим материальным активам. Прямой ущерб предлагается отражать как сумму отношений показателей функционирования программно-технических средств до и после совершения атаки либо отношений дополнительной стоимости затрат на восстановление оптимальных показателей функционирования к уже вложенным денежным средствам. Косвенный ущерб при этом будет характеризоваться суммой произведений определенных для организации весовых коэффициентов основных свойств обрабатываемой в информационной сети информации (конфиденциальность, целостность, сохранность и доступность) и количества атакованных материальных активов, обрабатывающих информацию.

Литература

1. СТБ ISO/IEC 27000-2012. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь.

2. Федорцов А.В., Кучинский П.В. Роль и место оценки ущерба от атак внутренних нарушителей в процессах управления информационной безопасностью организаций // Управление информационными ресурсами : материалы XIII Междунар. науч.-практ. конф. Минск, 9 декабря 2016 г. С. 205.

ПЛАЗМОННЫЕ ЭФФЕКТЫ В ГРАФЕНОВОЙ ПОЛЕВОЙ НАНОСТРУКТУРЕ

А.В. Фельшерук

Динамическая проводимость, определяемая концентрацией носителей заряда и химическим потенциалом, также зависит от потенциала полевого электрода, что, в конечном счете, ведет к изменению параметров взаимодействия электромагнитного излучения (ЭМИ) с графеновым слоем в полевой графеновой гетероструктуре. В данной работе представлены результаты расчетов коэффициентов распространения и поглощения ЭМИ в терагерцевом диапазоне (1–15 ТГц), а также длину волны плазмонных колебаний в зависимости от величины потенциала полевого электрода, температуры, и показателя преломления на границе среды и гетероструктуры. Уравнения, описывающие взаимодействие ЭМИ с графеном, выводятся из уравнений Максвелла, а дисперсионное соотношение, содержащее коэффициенты распространения и поглощения, из условия нетривиальности решений для этих уравнений. В свою очередь величина химического потенциала связана с величиной потенциала затвора и концентрацией носителей заряда уравнением электростатики гетероструктуры. Эти зависимости определяются с использованием интегрального уравнения для концентрации носителей заряда и электростатического уравнения для гетеростуктуры графен/диэлектрик/металл. Рассчитаны частотные зависимости динамической проводимости, коэффициентов распространения и поглощения при варьировании потенциала полевого электрода, толщины диэлектрика и плотности поверхностных состояний, температуры. Установлено, что в зависимости от сочетания параметров гетероструктуры наряду с монотонными возникают также и немонотонные частотные зависимости коэффициентов распространения и поглощения, а с ростом показателя преломления на границе среды и образца поглощение ЭМИ усиливается. Полученные частотные зависимости коэффициентов распространения и поглощения ЭМИ показали, что в рассмотренном диапазоне частот ЭМИ может не только распространяться, но также и усиливаться за счет плазмонных колебаний. Уменьшение длины волны плазмонных колебаний связано с сильной локализацией поверхностных плазмонов в графеновом слое.

ЭФФЕКТИВНЫЕ БИБЛИОТЕКИ МАШИННОГО ОБУЧЕНИЯ

И.И. Фролов

Современные информационные системы, в том числе и системы безопасности, видеонаблюдения, использующие последние достижения в области машинного обучения все больше используют в качестве первичных модулей для решения низкоуровневых задач готовые библиотеки или фреймворки от крупных компаний. Такой подход позволяет сэкономить время и средства на разработку, так и воспользоваться передовыми решениями от заслуживающих доверия разработчиков программного обеспечения.

Пользуется заслуженной популярностью библиотека глубокого обучения PyTorch [1] от Facebook, завоевавшая доверие и расположение исследователей по обработке естественного языка в силу своей гибкости, по сравнению со статическими фреймворками типа Tensorflow.

Однако Tensorflow также не теряет своих позиций. В 2017 году в феврале увидела свет версия Tensorflow 1.0 со стабильным API, поддерживающим и совместимым с более ранними версиями. Актуальная на сегодня версия – 1.4.1. Кроме базового фреймворка было разработано несколько дополнительных библиотек, таких как Tensorflow Fold для работы с динамическими графами, Tensorflow Transform для использования конвейеров данных и усовершенствованная библиотека Sonnet, разработанная копманией DeepMind. Также анонсирован новый режим Eager Execution, по принципу работы напоминающий PyTorch.

Однако появление большого количества фреймворков в области машинного обучения создает не только благоприятную среду для развития направления машинного обучения, но порождает некоторую разрозненность интерфейсов поставляемых продуктов. Для унификации обмена моделями между ними, Facebook и Microsoft разработали открытый формат ONNX.

Литература

1. Машинное обучение и искусственный интеллект: итоги за 2017 год [Электронный ресурс] – URL: https://dev.by/lenta/main/iskusstvennyy-intellekt-i-glubokoe-obuchenie-itogi-za-2017-god. (дата обращения: 17.05.2018).

МЕТОДЫ И МОДЕЛИ ДЛЯ СХЕМОТЕХНИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИБОРОВ СИЛОВОЙ ЭЛЕКТРОНИКИ

В.Т. Ханько, В.Р. Стемпицкий

Электрические модели полупроводниковых приборов силовой электроники являются важнейшим элементом для надежного и точного моделирования силовых электронных схем [1]. В течение последних 10 лет к самому перспективному поколению электрических моделей можно отнести модели семейства HiSIM, которые основаны на анализе поверхностного потенциала в качестве переменной состояния, что позволяет исключить региональный подход к построению моделей и использовать единое физически обоснованное выражение для подпороговой области вольт-амперной характеристики (ВАХ), а также области умеренной и сильной инверсии. Данный подход позволяет охватывать большое количество разнообразных структур устройств, таких как высоковольтный полевой МОП-транзистор или биполярный транзистор с изолированным затвором. Существует 5 электрических моделей, предназначенных для схемотехнического моделирования приборов силовой электроники: HiSIM-HV, HiSIM-UMOS, HiSIM-SJ, HiSIM-Diode, HiSIM-IGBT [2]. Данные электрические модели пользовались низким спросом до недавнего времени, поскольку поведение силовых цепей в основном определялось внешними емкостями и индуктивностями, а точность сигналов была несущественной из-за низких частот переключения, потери мощности были обусловлены статическим сопротивлением. Постепенно все изменилось, поскольку для современных силовых цепей с низкими потерями мощности, которые применимы в автомобильной электронике, мобильной связи, в интеллектуальных сетях с использованием возобновляемых источников энергии, очень важны более высокие частоты переключения.

От модели и области ее применения зависят методы. В зависимости от цели моделирования применяют стратегии экстракции параметров, отличающихся по числу используемых приборов (по группе транзисторов, по одному транзистору) и типу оптимизации параметров модели (с помощью глобальной оптимизации или локальной оптимизации).

В качестве примера была проведена экстракция параметров модели HiSIM-IGBT. Относительная погрешность схемотехнического моделирования с использованием экстрагированного набора параметров в сравнении с экспериментальными данными составила не более 7 %.

Литература

1. Денисенко В. Компактные модели МОП-транзисторов для SPICE в микро- и наноэлектронике. Москва : ФИЗМАТЛИТ, 2010. 408 с.

2. The HiSIM compact models of high-voltage/power semiconductor devices for circuit simulation / H.J. Mattausch [et al.] // IEEE 12th International Conference on Solid-State and Integrated Circuit Technology. 2014. P. 1415–1418.

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ BLOCKCHAIN

И.В. Хмурович, Ю.А. Скудняков

Одним из современных способов защиты информации является blockchain. Особый вид ведения реестра и учета при помощи криптографии имеет множество очевидных достоинств. Основные преимущества – это сложность фальсификации внесенных в систему blockchain данных и наличие информации у всех участников, подключенных к системе. Технология blockchain предлагает более безопасные транзакции, защиту от определенных хакерских атак и даже, в определенной степени, избавляет от необходимости паролей. Все данные blockchain хранятся на компьютерах пользователей blockchain-сети. Все пользователи сети равноправны и могут делать все, что угодно, в том числе безуспешно пытаться обмануть других

пользователей [1]. Запретить им никто не может, потому что все находятся в равных условиях, обладают равными правами и могут в равной степени исполнять и даже нарушать свои обязанности. Все пользователи blockchain образуют собой сеть компьютеров, на каждом из которых хранится копия данных blockchain. Обычно это полная копия всех блоков, но, в принципе, можно хранить лишь нужные на конкретном компьютере данные. Благодаря этому выключить или сломать blockchain практически невозможно, поскольку для этого надо выключить или сломать все компьютеры. Пока есть хоть один пользователь, blockchain существует [1]. Каждый новый пользователь расширяет и укрепляет эту сеть. Причем все компьютеры равноправны, там нет организаторов, модераторов, контролеров и менеджеров. Каждый отвечает за себя сам. Криптография – это основа blockchain, которая обеспечивает работу системы. Криптография в blockchain гарантирует безопасность, причем основанную на прозрачности и проверяемости всех операций. Различные криптографические техники гарантируют неизменность журнала транзакций blockchain, решают задачу аутентификации и контролируют доступ к сети и данным в blockchain в целом. Исходя из вышеизложенного, можно сделать вывод о том, что использование описанной технологии позволяет достаточно надежно осуществлять защиту информации. Рассмотренная технология достаточно успешно используется авторами работы.

Литература

1. Antonopoulos, A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014. 298 p.

МЕТОДЫ ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ

М.П. Хоронеко, М.А. Медунецкий, А.С. Летохо

SQL-инъекции были и остаются наиболее критичными уязвимостями приложений. Обычно атаки типа SQL-инъекций рассматривают относительно web-приложений, однако данной уязвимости подвержены любые клиент-серверные и сервис-ориентированные приложения, работающие с системами управления базами данных. SQL-инъекция – это атака, при которой злоумышленник производит вставку вредоносного кода в строки, передающиеся на сервер СУБД для синтаксического анализа и выполнения. Данная уязвимость состоит в том, что веб-приложение некорректно проверяет данные от пользователя, которые в дальнейшем используются для генерации SQL-запросов к базе данных.

SQL-инъекции можно классифицировать следующим образом:

1) по месту нахождения в запросе (инъекции в строковом параметре и в числовом параметре);

2) по способу внедрения инъекции (обычные и «слепые»).

Для успешного внедрения SQL-инъекций необходимо знать следующие параметры: способ передачи данных в веб-приложении, тип и версию СУБД, имя текущего пользователя, назначенные роли и системные привилегии.

В зависимости от назначенных текущему пользователю ролей и привилегий злоумышленник может попытаться извлечь хэши паролей пользователей СУБД, получить структуру БД и конфиденциальные данные или выполнить команды ОС, а также доступ к функциональным возможностям СУБД, а в некоторых случаях – к операционной системе сервера, на котором функционирует СУБД.

Приведем основные методы защиты веб-приложений:

– максимально возможная фильтрация данных;

– использовать при сравнении кавычки SELECT ...WHERE name='$name';

– фильтрация символов “%” и “_” при использовании SQL-функции LIKE.

– создание белого списка запросов на которые будет отвечать приложение.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ANGULAR ПРИЛОЖЕНИЙ

А.Л. Хотеев, А.С. Дроздов, Н.В. Харитонов, Е.И. Нехведович

Мир программного обеспечения эволюционирует с огромной скоростью. Всего пару лет назад настольные компьютеры и ноутбуки являлись основными устройствами, под которые

ориентировалась веб-разработка. Сегодня распределенные веб-приложения заменяют монолитные десктопные во многих сферах бизнеса. Поэтому крайне важно соблюдать нормы защиты веб-приложений. Фреймворк Angular.js поставляется с предварительно настроенными стратегиями по обеспечению безопасности от JSON уязвимостей и XSRF атак.

JSON уязвимости дают возможность веб-сайту третьих лиц подменить ваш URL для ресурса JSON, на запрос JSONP при определенных условиях. Для защиты от данного вида атаки сервер добавляет префикс ")]}',n" для всех ответов на запросы в формате JSON. Angular.js будет автоматически вырезать префикс перед обработкой ответа в формате JSON.

CSRF – вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Смысл атаки заключается в выполнении нежелательных действий на сайте ом имени аутентифицированного там пользователя. Angular.js предоставляет следующий механизм защиты от CSRF. При выполнении запросов XHR сервис $http считывает токен из файла cookie (по умолчанию XSRF-TOKEN) и задает его в качестве заголовка HTTP (по умолчанию X-XSRF-TOKEN). Поскольку только JavaScript, который работает на вашем домене, может читать cookie, ваш сервер может быть уверен, что XHR пришел из JavaScript, работающего на вашем домене. При первом GET запросе сервер возрващает в файле cookie токен с именем XSRF-TOKEN. Последующие XHR запросы сервер способен проверить, сравнивая значение coockie и присланного HTTP заголовка X-XSRF-TOKEN, чтобы удостовериться, что запрос не подделанный. Токен должен быть уникальным для каждого пользователя.

Литература

1. The Cross-Site Request Forgery (CSRF/XSRF) [Электронный ресурс]. – URL http://www.cgisecurity.com/csrf-faq.html (дата обращения: 16.05.2018).

2. Официальная документация по AngularJS [Электронный ресурс]. – URL: https://docs.angularjs.org/api/ng/service/$http (дата обращения: 16.05.2018).

ЭЛЕКТРОМИГРАЦИОННЫЕ ПРОЦЕССЫ В МЕЖСОЕДИНЕНИЯХ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

А.Г. Черных, В.В. Шульгов

Информационная безопасность требует совершенствования элементной базы микроэлектронных устройств защиты информации. По мере уменьшения размеров и совершенствования структуры микроэлектронных устройств возрастает роль многоуровневой системы межсоединений интегральных микросхем (ИМС) и основным ограничительным фактором в системе межсоединений является электромиграционная стойкость.

В работе представлены методы, которые позволяют провести оценку электромиграционной стойкости металлических межсоединений ИМС. Основные методы испытаний на стойкость к электромиграции условно можно разделить на испытания структур в составе корпуса (EM PLR) и испытания структур в составе пластины (EM WLR). При EM PLR испытания на электромиграцию проводятся в составе корпуса при постоянном токе и температуре К методам WLR–испытаний на отказ, вызванный электромиграцией, относят: изотермический тест (ISOT) и стандартный тест для ускорения электромиграции в структурах на пластине (SWET). Проведен анализ указанных методов, показано, что выбор метода зависит от задач, поставленных перед исследованиями.

Проведены исследования параметров электромиграции в межсоединениях ИМС на тестовых структурах с алюминиевой пленкой, а также сплавов Al+2%Cu и Al+1%Ho. После окончания электромиграционного теста структуры исследовали на оптическом и сканирующем электронном микроскопе, а микроструктуру пленок исследовали методом, основанном на дифракции обратно рассеянных электронов в электронном микроскопе. Проведенные исследования показали, что при наличии в алюминиевых пленках 2%Cu и 1%Ho приводит к малому порообразованию и следовательно к меньшему сопротивлению, чем в чистой алюминиевой пленке. Представлена корреляция полученных результатов для различных методов испытаний.

РЕШАЮЩЕЕ ПРАВИЛО ИДЕНТИФИКАЦИИ ЭЛЕМЕНТОВ С НЕЛИНЕЙНЫМИ ВОЛЬТАМПЕРНЫМИ ХАРАКТЕРИСТИКАМИ В НЕЛИНЕЙНОЙ РАДИОЛОКАЦИИ

В.М. Чертков, В.К. Железняк

Основным техническим средством защиты информации по поиску и обнаружению электронных закладных устройств является нелинейный радиолокатор. Проблема первичной идентификации сигналов от нелинейного радиолокатора с высокой вероятность правильного определения электронных закладных устройств стоит достаточно остро, а ее решение является актуальной задачей. Авторами предложен метод идентификации электронных закладных устройств, основанный на принятии решения по критерию скорректированного квадрата смешанной корреляции между значениями восстановленной вольтамперной характеристикой электронного закладного устройства, полученной путем расчета степенных коэффициентов аппроксимирующего ее полинома, согласно описанному способу в [1], со значениями эталонных вольтамперных характеристик для полупроводниковый компонентов и структур металл-оксид-металл. Показатели предложенного метода идентификации электронных закладных устройств имеет вероятность правильного их распознавания не ниже 0,9 и 0,8 для структур металл-оксид-металл [2].

Литература

1. Чертков В.М., Железняк В.К. Определение нелинейности вольтамперной характеристики объекта, исследуемого нелинейным радиолокатором // Доклады БГУИР. – 2017. № 8. С. 60–66.

2. Чертков, В.М., Железняк В.К. Оценка степени подобия идентификационного портрета радиоэлектронных средств с его эталоном // Современные средства связи: материалы XXI Междунар. науч.-техн. конф. Минск, 19–20 октября 2017 года. С. 308-309.

ПОДХОДЫ К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЮРИДИЧЕСКОЙ ОРГАНИЗАЦИИ

Г.Д. Чурчага

Элементами системы мер защиты информации являются меры правового, организационного и технического характера. Правовой элемент является обязательным для любого типа организации и для любой даже самой простой системы защиты информации. При его отсутствии организация не сможет должным образом защитить конфиденциальную информацию, а также привлечь к ответственности лиц, виновных в ее разглашении и утрате.

Правовой элемент, то есть меры юридического характера, направлен в основном на надлежащее оформление документов, а также на грамотную работу с персоналом организации, поскольку в основе системы защиты информации лежит человеческий фактор.

На данный момент во многих компаниях, будь то государственные предприятия, либо частные структуры, существует большой объем конфиденциальной информации. Разглашение конфиденциальной информации может нанести существенный экономический ущерб организации. Очевидно, что тайный сбор сведений, хищение документов, материалов, образцов, составляющих коммерческую или служебную тайну, организуется с целью завоевать рынок, сэкономить на приобретении ноу-хау и пр. По неофициальным данным, 80 % организаций несут убытки от «промышленного шпионажа».

Таким образом, стоит отметить, что в сфере защиты конфиденциальной информации организации важную роль играет ее персонал, который может стать как объектом, так и субъектом таких угроз. В связи с этим следует отметить, что при построении системы защиты информации организации необходимо налаживать работу юридического и кадрового отделов. Роль первого заключается в компетентном подборе персонала на этапе приема на работу либо государственную службу. Роль второго – в правовом оформлении ответственности за разглашение конфиденциальной информации, проведении информационно-профилактической работы, что, в общем, можно обозначить как превентивную функцию. Руководство организации на протяжении всего времени деятельности субъекта хозяйствования должно осуществлять контроль деятельности указанных подразделений.

КОНТРОЛЬ СОСТОЯНИЯ КОМПОНЕНТОВ ЛОКАЛЬНОЙ СЕТИ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ

В.Д. Шантарович, В.А. Ганжа

Протокол SNMP был разработан с целью управления сетевыми устройствами и допускает возможность внесения изменений в функционирование этих устройств. В наше время вопросы сетевой безопасности приобретают особое значение, особенно когда речь идет о протоколах передачи данных, в корпоративных сетях. После знакомства с SNMP становится понятно, что разработчики протокола думали об этом в последнюю очередь. К сожалению, в SNMP реализована очень простая система паролей, которую не следует считать безопасной. SNMP-запрос содержит групповое имя (community name), которое является разновидностью пароля. Создается впечатление что протокол рассчитан на работу в среде так называемых «доверенных хостов».

Управление сетью подразумевает установку на управляемые устройства специальных программных компонентов, называемых агентами управления; они могут отчитываться или отвечать на опросы объектов управления в системе управления сетью (NMS).

Несмотря на то, что большинство процессов, связанных с управлением сети, осуществляются средствами этой самой сети (что называется внутриполосным управлением), почти все системы управления сетями предусматривают различные методы внеполосного управления, обеспечивающие возможность обращения к управляемым устройствам даже тогда, когда сама сеть не функционирует.

Система управления сетью устроена на двух основных видах деятельности: способности управляемых устройств выдавать предупреждения об определенных событиях и способности объектов управления регулярно опрашивать управляемые устройства с целью сбора и группировки данных об этих устройствах, а также о сетях, их соединяющих.

БРАНДМАУЭР КАК ЭЛЕМЕНТ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Е.О. Шевчук, С.Г. Шульдова

Брандмауэр (межсетевой экран или файрвол) – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Основной задачей брандмауэра является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

Межсетевые экраны сейчас часто устанавливают не только на границе локальной сети и сети Интернет, но и между локальными сегментами сети для того, чтобы защитить и приходящий и локальный трафики. Программно-аппаратные элементы представлены в двух видах: в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства. Плюсы программно-аппаратных элементов защиты информации в том, что необходимо одно отдельное физическое устройство, как правило, с установленной ОС семейства *nix, которые настроены таким образом, чтобы выполнять только необходимые функции. Такие системы просто внедрять, управлять ими, они более производительны, так как из ОС исключены все неиспользуемые сервисы. Программно-аппаратные системы имеют высокую отказоустойчивость и доступность.

Основываясь на принципах работы аппаратных брандмауэров Cisco, в частности Cisco ASA 5500-X, в рамках магистерской диссертации планируется составить правила фильтрации, а также схему подключения брандмауэров в сети из нескольких серверов, что позволит обеспечить достаточный уровень безопасности любой сети.

Литература

1. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002. 306 с.

2. Ingham K., Forrest S. A History and Survey of Network Firewalls. University of New Mexico, 2002. 42 p.

3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ИНФРА-М, 2011. 416 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ И ТЕХНОЛОГИЯ eSIM

А.С. Шелков

Интернет вещей (IoT) – одно из самых развивающихся направлений в области информационных технологий и беспроводной связи. Одной из важных проблем в развитии данного направления является информационная безопасность (ИБ) инфраструктуры IoT. Инфраструктура IoT представляет собой совокупность устройств: датчиков, измерительных устройств, видеокамер, управляемых переключателей и т.д. Указанные компоненты, взаимодействуя между собой, или с внешней средой по определенным протоколам, образуют IoT. С момента создания концепции IoT отсутствовали жесткие ограничения и стандарты информационной безопасности устройств IoT, что делает небезопасным применение IoT для реальных задач. К основным слабым сторонам использования IoT относятся следующие пункты: питание датчиков, отсутствие единой стандартизации архитектуры и протоколов, отсутствие системы управления правами доступа, трудности обновления ПО, использование небезопасного ПО и др. Существенная часть этих недостатков может быть устранена применением технологии embedded SIM (eSIM) для устройств IoT. eSIM – технология, позволяющая виртуализировать модуль идентификации абонента (SIM): виртуальная SIM загружается через OTA-интерфейс на встроенный в мобильное устройство чип (eUICC). Идентификационные данные для виртуальной SIM предоставляются провайдером связи на узел SM-DP (Subscription Manager Data Preparation), который формирует профиль SIM-карты, впоследствии загружаемый и устанавливаемый в eUICC мобильного устройства. Применение этой технологии позволит реализовать следующие меры безопасности:

1) устройство становится частью сети сотового оператора, чем решается вопрос с аутентификацией;

2) провайдер услуг IoT может внедрить в профиль eSIM сканирующее ПО, которое может быть в дальнейшем использовано как часть IDS;

3) устройства с поддержкой eSIM должны проходить сертификацию GSMA;

4) появляется возможность обновления ПО устройства при помощи технологий OTA;

5) провайдер IoT может предоставлять специальных платформу для централизованного контроля и управления устройствами IoT для конкретных объектов.

Использование eSIM не решает всех вопросов ИБ, но позволит нивелировать самые критические уязвимости.

ПОДХОДЫ К БЕЗОПАСНОМУ КОНФИГУРИРОВАНИЮ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

А.С. Шилов, О.В. Бойправ

Операционные системы семейства Windows имеют ряд схожих характерных черт, в частности, защитные технологии, что облегчает обеспечение их безопасности и отчасти сводит его к правильной конфигурации параметров безопасности системы администратором. Данные параметры могут быть классифицированы в зависимости от механизмов операционной системы, с которыми они связаны: параметры контроля учетных записей, параметры устройств, параметры сетевого доступа, параметры завершения работы, параметры аудита, параметры входа в систему и т.д.

К критически важным параметрам безопасности относятся, в первую очередь те, которые связаны с учетными записями. В связи с неограниченным числом попыток неверного входа для данной записи, следует отключать параметр «состояние учетной записи «Администратор»» на рабочих машинах рядовых пользователей сети, что не позволит использовать данную запись при обычном входе, а также отключить автоматический вход администратора в консоль восстановления. Также необходимо ограничивать возможности пользователей по добавлению новых учетных записей настройкой параметра «блокировать учетные записи Майкрософт» и использование встроенной учетной записи «Гость», отключив параметр «состояние учетной записи «Гость»». Также следует контролировать установку

приложений и повышение прав, запрашивая пароль от администратора, активировав соответствующий параметр. Среди дополнительных настроек можно выделить следующие:

– отключение необязательных подсистем, т.к. используемая по умолчанию подсистема допускает запуск процесса одним пользователем, а последующее – работу с процессом другого пользователя, что способствует сокрытию фактов несанкционированного доступа;

– включение аудита использования привилегии на архивацию и восстановление, т. к. при резервном копировании создается копия файловой системы, чем может воспользоваться злоумышленником.

АЛЮМООКСИДНЫЕ ОСНОВАНИЯ С ПОКРЫТИЯМИ, МОДИФИЦИРОВАННЫМИ НЕОРГАНИЧЕСКИМИ ДИЭЛЕКТРИЧЕСКИМИ ПЛЕНКАМИ

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

В результате проведенных исследований отработаны технологические методы формирования дополнительных диэлектрических пленок на пористых алюмооксидных основаниях с целью получения модифицированных многослойных структур, обладающих закрытой пористостью и приводящих к улучшению теплофизических и электрофизических свойств конечных диэлектрических покрытий на алюминиевых основаниях [1].

Отработаны режимы вакуумного осаждения на пористые алюмооксидные поверхности неорганических диэлектрических пленок трех видов: 1) Al_2O_3 из мишени поликора (ВК100-1); 2) SiO_2 из мишени кварца (С5-1); 3) композита на основе Al_2O_3, SiO_2 и MnO из мишени корундовой керамики (22ХС). Осуществлено теоретическое моделирование послойного осаждения и установлено, что для модификации пористой структуры осажденными диэлектриками (с перекрытием и захлопыванием пор) необходимо проводить напыление пленок толщиной ~300-2000 нм в зависимости от толщины анодного Al_2O_3 и диаметра пор. Установлена зависимость коэффициента теплопроводности многослойной структурной системы «несущий Al + анодный Al_2O_3 + осажденный диэлектрик» от толщины Al-оснований из сплава АМг-2 (в диапазоне ~ 1–3 мм), толщины анодного Al_2O_3 (в диапазоне ~ 50–100 мкм) и толщины осажденных диэлектрических пленок (~1000 нм и ~2000 нм). Выяснено, что значения параметра теплопередачи многослойных модифицированных покрытий возрастают при уменьшении толщины такой составляющей, как анодный Al_2O_3, а уплотнение осажденными диэлектриками позволяет увеличить значения коэффициента теплопроводности. Так для толщины пористого Al_2O_3 ~50 мкм значения коэффициента теплопроводности возрастают с ~82 Вт/м·К до ~91 Вт/м·К соответственно при увеличении значений толщины осажденного (из мишени поликора (ВК100-1)) Al_2O_3 от ~1000 нм до ~ 2000 нм, в то время как параметр теплопередачи для немодифицированного пористого Al_2O_3 такой же толщины (~ 50 мкм) в общей системе с Al (~ 2 мм) составляет ~ 52 Вт/м·К. Объяснение этого факта заключается в том, что исходная пористая Al_2O_3-структура содержит газовую фазу с воздушным наполнением и составляющей адсорбированных на стенках пор водяных паров, коэффициенты теплопроводности которых низкие, составляют ~ 0,022 Вт/м·К (для воздуха) и ~ 0,6 Вт/м·К (для воды) и отрицательно влияют на теплопроводность твердофазной алюмооксидной структуры.

Литература

1. Шиманович Д.Л. Технологические режимы формирования дополнительных диэлектрических пленок на пористой поверхности алюмооксидных оснований и исследование электрофизических и теплофизических характеристик модифицированных покрытий // Фундаментальные проблемы радиоэлектронного приборостроения. 2017. Т. 17, № 2. С. 573–576.

МЕТОДЫ ФОРМИРОВАНИЯ ТОПОЛОГИЧЕСКИХ ЗОН ОТКРЫТОГО ВЫХОДА НА АЛЮМИНИЕВЫХ ОСНОВАНИЯХ В ТОЛСТОСЛОЙНЫХ Al_2O_3-ПОКРЫТИЯХ

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

Исследованы технологические методы толстослойного анодирования алюминия в локальных топологических областях при различных методах маскирования для

формирования открытых зон выхода на несущие алюминиевые основания с целью потенциальной возможности дальнейшего контактного монтажа мощных кристаллов непосредственно на металлизированные площадки (контакт «Al-основание – термоплощадка кристалла»), что позволяет исключить диэлектрическую составляющую на основе анодного оксида алюминия с низким параметром коэффициента теплопроводности в местах контакта и тем самым увеличить эффективность теплоотвода в матричных многокристальных системах.

Проведены экспериментальные исследования по определению коэффициента объемного роста толстослойных покрытий на основе пористого оксида алюминия и показано, что эти значения варьируются технологическими (электрохимическими, температурными) режимами оксидирования. Установлен линейный характер зависимостей коэффициента объемного роста от напряжения анодирования при формировании пленок Al_2O_3 в 10% H_2SO_4 и в 4% $H_2C_2O_4$ при различных температурах электролитов. Экспериментально выявлено, что при анодировании алюминиевого сплава АМг-2 в потенциостатическом режиме при U ~65 В в 4% $H_2C_2O_4$ при температуре Т ~20 ^oC, коэффициент объемного роста составляет ~1,5. Осуществлен сравнительный анализ методов маскирования (в присутствии фоторезистивной маски и маски из плотного анодного оксида) и с помощью методики поперечного микрошлифа изучены профили бокового ухода под маску на границе раздела «Al–Al_2O_3» при локальном глубоком анодировании Al [1]. Отработаны и оптимизированы 4 варианта технологических методов формирования открытых зон выхода на Al-основания в Al_2O_3-покрытиях: метод локального химического травления в предварительно сформированном сплошном Al_2O_3-слое; метод локального толстослойного анодирования в присутствии фоторезистивной маски; метод локального глубокого анодирования с защитным маскированием на основе плотного Al_2O_3; метод локального двухстадийного анодирования с промежуточным травлением Al_2O_3, сформированного на 1-ой стадии. Установлено что для исключения рельефности поверхности («колодцев») и для создания планарных топологических зон выхода на Al-основания (на линии поверхностной системы «Al–Al_2O_3») при условии коэффициента объемного роста ~1,5 при формировании конечных Al_2O_3-покрытий определенной толщины двухстадийным анодированием, необходимо на 1-ом этапе формировать Al_2O_3 толщиной в 2 раза меньше, чем на 2-ом этапе.

Литература

1. Шиманович Д.Л., Сокол В.А. Локальное толстослойное анодирование алюминия и анализ бокового ухода при различных методах маскирования // Фундаментальные проблемы радиоэлектронного приборостроения. 2014. Т. 14, № 3. С. 163–165.

РАСПРЕДЕЛЕНИЕ ЭЛЕКТРИЧЕСКОГО ПОЛЯ В СИСТЕМЕ ОСТРИЙНЫХ КАТОДОВ

И.А. Шинкевич

Приведены результаты математического моделирования распределения напряженности электрического поля в системе острийных катодов в зависимости от геометрии исследуемой структуры. Для моделирования использовался модуль «Electrostatics» программного пакета «Comsol Multiphysics». Для расчета напряженности поля в выбранной структуре использовалось решение уравнения Гаусса в диэлектрической среде. Исследуемая структура представляет собой массив углеродных нанотрубок, выполняющих роль катода, и плоского анода. Высота каждой нанотрубки – 174 нм, радиус – 24 нм. Производился расчет величины напряженности электрического поля на острие центральной нанотрубки при изменении расположения соседних нанотрубок относительно центральной. Расстояние изменялось от 100 нм до 250 нм с шагом в 10 нм. Величина напряжения между анодом и подложкой оставалась неизменной и составляла 1000 В. Полученная зависимость напряженности электрического поля на острие центрального катода от взаимного расположения нанотрубок носит сложный колебательный характер. Средний коэффициент усиления, определяемый отношением напряженности поля на вершине нанотрубки к среднему полю между нанотрубками составляет от 2 до 2.25. Полученные результаты отличаются от известных в литературе тем, что обычно наблюдается нелинейная зависимость от расстояния только с одним

максимумом. Наличие многопиковой зависимости говорит о том, что в трехмерном случае возникают дополнительные факторы, влияющие на распределение напряженности электрического поля в массиве нанотрубок. Эти факторы могут быть связаны с распределением заряда в нанотрубках и экранированием электрического поля отдельной нанотрубки полями соседних нанотрубок. Исследование этих факторов требует проведения дополнительных расчетов.

Литература

1. Трубецков Д.И., Рожнев А.Г., Соколов Д.В. Лекции по сверхвысокочастотной вакуумной микроэлектронике. Саратов: Изд-во ГосУНЦ «Колледж», 1996. 238 с.

2. Fuzinatto F. Field Emission Simulations of Carbon Nanotubes and Graphene with an Atomic Model // Journal of Nanomaterials and Molecular Nanotechnology. 2014. V. 3, Iss. 4.

АНАЛИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ И ЗАЩИТА ОТ НЕГО

И.Г. Юруть, С.И. Леонов

Обеспечение необходимого уровня защиты информации требует не просто осуществления некоторой совокупности научно-технических и организационных мероприятий, а создания целостной системы организационных мероприятий и применения специальных средств и методов защиты информации.

Если рассмотреть проблему защиты информации в сетях в целом, то можно выделить множество способов и методов доступа к информации в АСОИ. В противовес этим способам доступа существуют специальные средства защиты информации от несанкционированного доступа (НСД). Программные средства являются важнейшей и непременной частью механизма защиты современных АСОИ, что обусловлено такими их достоинствами, как универсальность, простота реализации, гибкость, практически неограниченные возможности изменения и развития. К недостаткам программных средств относится необходимость расходования ресурсов процессора на их функционирование и возможность несанкционированного изменения.

Ни одна система защиты данных не является неуязвимой. Защищая данные и создавая политику безопасности сети, необходимо задавать вопрос: является ли защищаемая информация более ценной для атакующего, чем стоимость атаки? Ответ необходимо знать, чтобы защитится от дешевых способов атаки и не беспокоиться о возможности более дорогой атаки. Это позволит со стороны материального обеспечения более рационально подойти к вопросу защиты информации. При организации работы на ЭВМ нужно разрабатывать комплексный план защиты от угроз НСД. Необходимым компонентом этого плана защиты ЭВМ являются программные средства. Кроме того, при обеспечении безопасности ЭВМ необходимо использовать и другие возможности. Должен быть организован контроль своевременной смены пароля. Должны быть продуманы и организованы физические средства контроля. Кроме того, для организации грамотной работы сети администратор должен хорошо представлять себе существующие угрозы НСД к информации. Все это вместе позволяет добиться требуемого уровня безопасности ЭВМ.

МЕЖДУНАРОДНЫЙ ПРОЕКТ РАЗРАБОТКИ СЕРИИ УЧЕБНЫХ ПОСОБИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А.И. Якимов, В.И. Аверченков, М.Ю. Рытов, Т.Л. Шебан

В университетах Российской Федерации накоплен значительный опыт подготовки специалистов по защите информации. В Республике Беларусь образовательным стандартом ОСВО 1-53 01 02-2013 [1] предусмотрена дисциплина «Основы защиты информации». Более того, вопросы защиты информации предусмотрены и в других дисциплинах специальности.

Совместно со специалистами Российской Федерации разрабатывается серия учебных пособий «Технологии защиты информации». Серия включает следующие учебные пособия:

Защита корпоративных данных в организации – рассмотрены общие вопросы обработки персональных данных в организации, нормативно-правовая база в области обработки и защиты персональных данных;

Основы компьютерной безопасности – общие вопросы обеспечения информационной безопасности компьютерных систем;

Организация защита информации – вопросы, связанные с организацией защиты информации на наиболее уязвимых направлениях деятельности предприятия, таких как работа с персоналом, проведение совещаний, переговоров и выставок, работа с конфиденциальными документами;

Защита информации в вычислительных сетях – представлены современные технологии защиты вычислительных сетей, отмечены методы воздействия внутренних нарушителей на корпоративную сеть;

Основы криптографической защиты информации – общие вопросы теории криптографии, принципы построения криптоалгоритмов и сетей засекреченной связи, а также основы криптоанализа и перспективные направления развития криптографии.

Литература

1. ОСВО 1-53 01 02-2013. Образовательный стандарт высшего образования. Специальность 1-53 01 02 Автоматизированные системы обработки информации. – Минск: М-во образования Респ. Беларусь, 2013. 26 с.

ОБУЧЕНИЕ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Яковлев, П.А. Хоревко, Ю.А. Скудняков

Современные организации активно используют информационные технологии, создают необходимые условия по развитию знаний и навыков сотрудников в области информационной безопасности, что на сегодняшний день является неотъемлемой частью совершенствования профессионального уровня персонала. Согласно исследованиям более 80 % инцидентов на предприятиях в сфере информационной безопасности, в которых виноваты сотрудники, происходит в результате неумышленных действий [1]. Возникает непростая задача: как добиться того, чтобы сотрудники более внимательно относились к информационной безопасности, выполняли необходимые правила и требования. Решение данной проблемы возможно несколькими путями, однако однозначно можно сказать, что без повышения квалификации сотрудников в этой области задачу защиты информации не решить. Процесс обучения в области информационной безопасности условно можно разделить на подготовку специалистов, отвечающих за защиту информации в организации, и рядовых сотрудников. Специфика обучения различных категорий пользователей состоит в глубине и масштабности отработки тех или иных вопросов [2]. Предлагается использовать метод компьютерной симуляции в обучении. Проводится анализ и обработка инцидентов, дается оценка в соответствии с политикой исследования рисков, принятой в организации. На основании результатов анализа составляется план обучения. Погружаясь в проблемную ситуацию, обучающийся пытается найти выход из нее с помощью уже имеющихся у него знаний, навыков и ресурсов. Когда становится очевидно, что их недостаточно, он начинает самостоятельно искать новые способы действий и запрашивать дополнительную информацию. Использование такого подхода позволяет прочувствовать ценность нового знания путем проб и ошибок, получить навыки правильного использования имеющихся средств защиты и ответственности за утечку информации. Независимо от результатов симуляции персонал приобретает необходимый опыт. Благодаря этому сотрудник на эмоциональном и подсознательном уровне запоминает учебный материал и понимает важность требований к информационной безопасности.

Литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2017. 324 с.

2. Бирюков, А.А. Информационная безопасность. Защита и нападение. М.: ДМК–Пресс, 2017. 434 с.

ШИФРОВАНИЕ ДАННЫХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

А.В. Яковлев, Ю.А. Скудняков, В.И. Пачинин

В настоящее время весьма актуальной проблемой является надежная защита информации. Одним из путей решения данной проблемы – использование существующих и разработка и применение новых, более эффективных, методов и средств шифрования данных с помощью искусственных нейронных сетей (ИНС). ИНС – совокупность нейронов, связанных между собой соответствующим образом. Нейрон включает модуль суммирования, определяющий взвешенную сумму всех входных сигналов и модуль функции активации. Соединения синапсов с аксонами образуют ИНС. Наиболее распространенными и хорошо изученными являются трехслойные ИНС. Шифрование данных осуществляется путем сохранения строки в открытом тексте ИНС. Процесс получения произвольного состояния сети из множества строк представляет собой задачу шифрования данных [1]. В предлагаемой системе шифрования нейронная сеть это узел, обученный заменять код символа на другой код, связанный с ним ассоциативно. Однако, в передаваемом сообщении, одни символы встречаются чаще, а другие реже. При частотном анализе полученного шифра текста легко обнаружить повторение в нем символов и расшифровать его. Поэтому следующим этапом является сглаживание частот повторения кодов. Например, зашифруем сообщение «Каждый охотник желает знать, где сидит фазан». Каждому символу алфавита соответствует случайное 48 битное неповторяющееся число. В сообщении есть повторяющиеся символы. Под каждый символ выделяется некая область числовых значений, любое значение из этой области будет соответствовать символу. Область числовых значений определяется координатами поверхности в пространстве, ограниченной по осям *X, Y, Z*. Функция построения поверхности является частично ключом, поэтому она не подлежит огласке. Обучение нейронной сети заключается в том, чтобы сеть правильно выбрала границы областей поверхности по площади. Это необходимо чтобы координаты точек, ассоциированных с символом, находились как можно дальше в границах области. Также задается специальная функция, определяющая изменения координаты точки для повторившегося символа.

Литература

1. Аксенов С.В., Новосельцев В.Б. Организация и использование нейронных сетей (методы и технологии) / Под общ. ред. В.Б. Новосельцева. Томск: Изд-во НТЛ, 2006. 128 с.

КОМПОЗИЦИОННЫЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ НА ОСНОВЕ ОКСИДОВ ЖЕЛЕЗА И ТИТАНА ДЛЯ ЗАЩИТЫ ОТ ВНЕШНИХ ПОЛЕЙ

И.С. Ярочкин, К.Н. Берёзкин, С.С. Алейник

Развитие современных технологий и производств технических средств различного назначения активные технические средства защиты информации быстро теряют свою актуальность. В сложившихся условиях представляется наиболее эффективным использование новых пассивных средств защиты информации от утечки по техническим каналам, а именно – создание систем экранирования технических средств обработки конфиденциальной информации и их компонентов.

Цель настоящей работы заключается в установлении взаимосвязи между составом силиконовых матриц с порошковыми наполнителями и их свойствами в радиочастотном диапазоне 8–12 ГГц.

Экраны ЭМИ формировали на основе порошка Fe_3O_4 с добавлением TiO_2. Затем указанные порошок смешивали с силиконом и тщательно перемешивали, добиваясь образования однородной массы. Полученную массу перемещали в рамку из органического стекла и равномерно распределяли материал по всему объёму рамки. Заполненную композитом рамку оставляли на сушку при комнатной температуре. Аналогичным методом были

изготовлены экраны, в состав которых входили TiO_2 и Fe_3O_4 в следующих соотношениях: 0,5×2,5; 1×2; 1,5×1,5; 2×1; 2,5×0,5.

Для исследования экранирующих характеристик в диапазоне 8-12 ГГц использовался панорамный измеритель ослабления и КСВН Я2Р-67 с ГКЧ-61 и волноводным трактом.

По результатам проведенных измерений было выяснено, что самый высокий коэффициент отражения показал образец на основе Fe_3O_4, а самое большое значение коэффициента передачи получилось у экрана на основе смеси $2{,}5(Fe_2O_4)+0{,}5(TiO_2)$. Использование в качестве наполнителей мелкодисперсных порошков оксидов металлов в силиконовой матрице позволило существенно улучшить характеристики экранов ЭМИ.

ДЛЯ ЗАМЕТОК

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XVI Белорусско-российской научно–технической конференции
(Минск, 5 июня 2018 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 30.05.2018. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 12,79. Уч.-изд. л. 11,3. Тираж 100 экз. Заказ 124.

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