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
XV Белорусско-российской научно–технической конференции
(Минск, 6 июня 2017 г.)

Минск БГУИР 2017

УДК 004.56 (043.2)
ББК 32.973.26–018.2

Технические средства защиты информации: Тезисы докладов XV Белорусско-российской научно-технической конференции, 6 июня 2017 г., Минск. Минск: БГУИР, 2017. – 116 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

СЕКЦИЯ 1 ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

СЕКЦИЯ 2 ОБНАРУЖЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

СЕКЦИЯ 3 ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

СЕКЦИЯ 4 ЭЛЕМЕНТЫ И КОМПОНЕНТЫ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

СЕКЦИЯ 5 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ

СЕКЦИЯ 6 ОБУЧЕНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СЕКЦИЯ 1
ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

DEVOLOPMENT OF THE VULNERABILITY MANAGEMENT PROGRAM IN BANKING

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]. Vulnerability management is the process in which vulnerabilities in are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization) [2].

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security. A vulnerability management process should be part of an organization’s effort to control information security risks. This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information [3].

Banks that do not maintain vulnerability management program could not comply with Payment Card Industry Data Security Standards but also place their customers and their data at risk. There are a number of techniques available to find and to eliminate vulnerabilities and offer increased level of protection of the private data. A successful and robust vulnerability management requires incorporation of various security components, the most critical of which are the risk, patch, asset, change and configuration management. Scanning a system will identify vulnerabilities and weaknesses that must then be addressed. The paper discusses the content of each component and integration of the vulnerability management program into the information security program.

NIST recommends that organizations create a group of individuals, called the patch and vulnerability group (PVG), who are specially tasked to implement the patch and vulnerability management program [4]. The paper also discusses paper the responsibilities of the PVG members.

References

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

2. Tom Palmaers. Implementing a vulnerability management process SANS Institute. 2013.

3. Williams, A and Nicollet, M: Improve IT Security With Vulnerability Management, Gartner ID Number: G00127481, May 2005.

4. Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies (July 2013). http://dx.doi.org/10.6028/NIST.SP.800-40r3.

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗРАБОТКИ, ФОРМИРОВАНИЯ И ПРИМЕНЕНИЯ ОРГАНИЗАЦИОННЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Безмен, О.А. Дугушкина

Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности (ИБ) с каждым годом становятся все более и более актуальными, и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и методы обеспечения ИБ. Организационно-правовое обеспечение ИБ представляет собой совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению ИБ, так и создание, и функционирование систем защиты информации (СЗИ) на конкретных объектах. Организационные методы обеспечения ИБ находят

практическое применение в деятельности руководства и персонала конкретного предприятия, на котором планируются и проводятся мероприятия по обеспечению ИБ объектов информационной инфраструктуры. Недостаточная подготовка персонала организации, слабое знание им нормативно-правовой базы по вопросам обеспечения безопасности может стать причиной уязвимостями эксплуатируемых информационных систем. Применение организационных методов обеспечения ИБ является обязательной составляющей обеспечения ИБ любой организации.

Организационно-правовая база обеспечения ИБ разрабатывается и описывается при проектировании и создании, а также последующей аттестации СЗИ информационной системы предприятия. Государственное предприятие «НИИ ТЗИ» является одной из ведущих организаций Республики Беларусь в области защиты информации. Вот уже более четверти века одним из направлений деятельности государственного предприятия «НИИ ТЗИ» является проектирование и создание СЗИ, предназначенных для решения задач защиты информации в самых разных информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено и не отнесенной к государственным секретам, а также аттестации таких систем в соответствии с действующим законодательством Республики Беларусь.

В докладе подробно представлены основные этапы разработки и формирования документации, регламентирующей организационные методы обеспечения ИБ и сопровождающей СЗИ информационной системы предприятия на всех этапах ее проектирования, создания и аттестации.

НАВЫКИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.Н. Беляцкая, В.С. Князькова

По оценкам специалистов, к 2019 г. в мире будет не заполнено от 1 до 2 миллионов вакансий в сфере информационной безопасности (ИБ). Например, в 2015 г. в США было свободно около 209000 вакансий в сфере ИБ. Такая нехватка специалистов может быть причиной сдерживания развития электронного общества, в частности, электронной экономики. Исследование, проведенное компанией Intel Security, показало, что 82% всех респондентов (страны: Австралия, Франция, Германия, Израиль, Япония, Мексика, Великобритания и США) указали на нехватку знаний в области ИБ. Это напрямую приводит к экономическим затратам у 71 % респондентов, главным образом из-за большей уязвимости организаций перед хакерскими атаками, а также в связи с необходимостью оплачивать труд специалистов в сфере ИБ более высоко. Так, в указанных выше странах заработная плата специалиста в области ИБ в 2,7 раза выше средней по отрасли.

Выделяют следующие основные навыки, которыми должен обладать специалист области ИБ. Во-первых, аналитические (способность к изучению компьютерных систем, оценке потенциального риска и способность предложить возможное решение). Во-вторых, коммуникационные (специалист в области ИБ должен обучать пользователей, объясняя им важность ИБ и способы защиты персональной и коммерческой информации). В-третьих, креативность (необходимо предугадывать действия компьютерных преступников, что требует нестандартного мышления). В-четвертых, внимательность к деталям (зачастую угрозы ИБ трудно распознать, поэтому специалист в области ИБ должен отслеживать даже незначительные изменения в информационной системе, предвидя любые, даже несущественные, потенциальные проблемы). В-пятых, знания в IT сфере (и угрозы, и методы их предотвращения постоянно меняются, поэтому необходимо постоянно совершенствовать свои знания по последним решениям, законодательству, практиками и методикам в области защиты информации). В качестве основных элементов образовательной системы в области ИБ рассматривается классическое академическое образование; при этом его интеграция с практической компонентой лучше подготовит будущего специалиста. Для оценки качества подготовки специалистов в сфере ИБ, Intel Security разработала интегрированный показатель, учитывающий расходы на образование; программы по науке, технологиям, инженерии и математике; наличие дисциплин по ИБ в вузах; использование передовых практик. Наилучшие результаты достигнуты такими странами, как США и Великобритания.

Литература

1. Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills [Electronic resource]. Mode of access: https://www.mcafee.com/ca/resources/reports/rp-hacking-skills-shortage.pdf. Date of access: 14.05.2017.
2. Sheridan, K. 7 Cyber-Security Skills In High Demand [Electronic resource]. Mode of access: http://www.informationweek.com/strategic-cio/security-and-risk-strategy/7-cyber-security-skills-in-high-demand-/d/d-id/1326494. Date of access: 14.05.2017.
3. Information Security Analyst Skills [Electronic resource]. Mode of access: https://www.thebalance.com/information-security-analyst-skills-2062409. Date of access: 14.05.2017.
4. Лыньков, Л.М. Методика оценки рисков информационной безопасности в системах электронной экономики / Л.М. Лыньков, Т.Н. Беляцкая, В. С. Князькова // Доклады БГУИР. – 2017. – № 2 (104). – С. 69–76.

ЗАЩИТА ИНФОРМАЦИИ В МОБИЛЬНОМ ПРИЛОЖЕНИИ «МЕНЕДЖЕР ПЕРИОДИЧЕСКИХ ПЛАТЕЖЕЙ»

А.В. Бердник, А.В. Матвеев

Объектом защиты информации в рассматриваемом докладе является мобильное приложение «Менеджер периодических платежей». В настоящее время все чаще необходимо использовать периодические платежи, такие как оплата телефона, учебы или услуг ЖКХ. Некоторые платежные системы в нашей стране позволяют настроить автоматические платежи на некоторые услуги, однако функционал регулирования частоты оплаты, как правило, отсутствует, и в целом данный способ не всегда уместен либо пугает некоторых пользователей из-за отсутствия личного контроля за платежами. Приложение подразумевает использование различных платежных систем, в том числе и использование системы расчета ЕРИП (Единое Расчетное и Информационное Пространство) [1]. Система ЕРИП имеет возможность выставления счета на некоторые услуги (оплата учебы, некоторых услуг ЖКХ и так далее), следовательно, зная идентификатор пользователя в данной услуге, приложение может само получить необходимую сумму к оплате. При создании событий пользователь может указать поведение программы в данном случае: предлагать полученную сумму, не оплачивать в случае если суммы нет или игнорировать данные ЕРИП и оплатить сумму, указанную пользователем.

Приложение работает с реальными деньгами пользователя, следовательно, каждое его одобрение оплаты должно быть подтверждено введением личного пароля. Пользователь может установить пароль при регистрации, которая запускается при первом запуске программы. Уникальным ключом каждого пользователя является номер мобильного телефона, изменить его можно в настройках программы. Пользователь может подключать к программе несколько платежных карт различных банков или платежных систем, либо другие способы оплаты (интернет-кошельки, оплата со счета мобильного) и в будущем, при создании событий, сможет выбрать с помощью какого способа оплаты оформить услугу. Также возможно выбирать способ оплаты перед каждым непосредственным платежом. Работа с платежными системами и системой расчета ЕРИП накладывает на приложение большую ответственность за информационную безопасность данных пользователя и всех проводимых операций. Опыт показывает, что простого пароля для авторизации в системе недостаточно, необходима шифровка данных при любых синхронизациях с сервером приложения и наличие безопасного соединения при отправке команд в систему расчета.

Литература

1. ЕРИП Расчет – Платежные агенты [Электронный ресурс]. – Режим доступа: http://raschet.by/bankam/platezhnye-agenty/. – Дата доступа: 19.05.2017.

ОСОБЕННОСТИ АНКЕТИРОВАНИЯ СОТРУДНИКОВ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ ПРИ ПРОВЕДЕНИИ АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Бойправ, Л.Л. Утин, В.В. Ковалёв

Предложен перечень вопросов для анкетирования сотрудников организаций электросвязи в зависимости от специфики деятельности последних: строительство

(организации категории 1), предоставление услуг электросвязи (организации категории 2), проектирование сетей электросвязи (организации категории 3), управление и регулирование деятельности организаций электросвязи (организации категории 4). Вопросы составлены с учетом требований к системе защиты информации, изложенных в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62, а также положений СТБ ISO/IEC 27001-2016.

Сотрудники, которых следует отнести к кругу лиц, подлежащих опросу в ходе аудита системы менеджмента защиты информации организаций электросвязи: руководитель и/или главный инженер; начальник службы безопасности; старшие производители работ или начальники строительных участков (в случае, если аудируемая организация относится к категории 1); начальники отделов, сотрудники которых работают с электронными документами и базами данных, в которых содержится информация ограниченного распространения (в случае, если аудируемая организация относится к категории 2, 3 или 4).

Из составленных авторами статьи анкетных вопросов для руководителей и/или главных инженеров организаций электросвязи категорий 1–4 можно выделить следующие основные:

1. Выполнена ли классификация КВОИ, доступ к которым имеют сотрудники Вашей организации? 2. Выполняется ли в Вашей организации классификация активов КВОИ, доступ к которым имеют сотрудники? 3. Внедрена и используется ли в Вашей организации политика информационной безопасности? 4. Назначено ли в Вашей организации лицо, на которое возложены обязанности по контролю за соблюдением положений политики информационной безопасности? 5. Осведомляются ли увольняемые сотрудники Вашей организации, которые имели доступ к информации ограниченного распространения, об ответственности, к которой они могут быть привлечены вследствие разглашения этой информации третьим лицам?

СИСТЕМА МОНИТОРИНГА И КОРРЕЛЯЦИЙ СОБЫТИЙ

Ю.О. Быханьков

Для построения эффективной системы защиты информации не только следует разобраться в требованиях законодательства, но и соизмерить их с финансовыми возможностями организации, а также определить механизм мониторинга и аудита информационной безопасности. На текущий момент в Республике Беларусь необходимость в системе мониторинга и корреляций событий следует из регулирующих приказов Оперативно-аналитического центра при Президенте Республики Беларусь и действующих, но местами неработающих и даже противоречащих законодательству стандартов серии 34.101. В виду того что требования к системе защиты информации закреплены, иногда возможно изменить класс объекта информатизации (информационной системы), чтобы уменьшить затраты на построение системы защиты информации, например сокращением средств на реализацию требований пп. 39, 40, 46 приказа № 62 ОАЦ, а в некоторых случаях на разработку и оценку задания по безопасности. Требования по сбору, просмотру и анализу событий безопасности являются обязательными в Республике Беларусь для систем защиты информации независимо от формы собственности. Уменьшение средств защиты может не только навредить безопасности, но и помочь, сфокусировав внимание специалиста. В списке сертифицированных средств уже существуют продукты для адекватного исполнения требований по анализу событий, в то же время существуют варианты формального выполнения пунктов требований регулятора, которые не могут сравниться с системами корреляций событий. В том же приказе прописывается анализ событий уполномоченными субъектами, однако как показывают исследования, квалифицированные субъекты без специальных средств не могут выполнять анализ на должном уровне в режиме реального времени, особенно анализ логов с различных элементов инфраструктуры, что является критически важным для обеспечения защиты информации.

Литература

1. Закон Республики Беларусь Об информации, информатизации и защите информации от 10 ноября 2008 г. № 455-З.

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62.

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

А.Н. Горбач, С.Н. Касанин

В Указе Президента Республики Беларусь от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере.

В Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» четко определено в каких целях организуются и проводятся Научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации:

Приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93 утверждена государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации и специальных технических средств (ГНТП «Защита информации – 3»), на 2016 – 2020 годы.

Эти документы в области технической защиты информации гармонично дополняют и другие соответствующие НПА.

Анализ состояния дел в сфере технической защиты информации показывает:

1. Сложились вполне сформировавшаяся концепция и структура, основу которой составляют:

2. Эффективность и соразмерность мер по защите информации от утечек по техническим каналам в Республике Беларусь позволяет обеспечить защиту информации в соответствии с требованиями действующих нормативно-методических документов и технических нормативных правовых актов.

Исследования в данной области свидетельствуют, что для борьбы с этой тенденцией нельзя ограничиваться отдельными и разовыми мероприятиями, необходим системный подход. Это непрерывный процесс, немаловажное и первостепенное значение в котором отводится развитию и совершенствованию научно-методологических аспектов в области технической защиты информации.

Первое: необходима проработка и конкретизация приоритетных научные исследования в области технической защиты информации.

Второе: значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

Третье: совершенствование кадровой политики в сфере ТЗИ.

АНАЛИЗ СОСТОЯНИЯ И МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

М.М. Дроздов, А.М. Прудник

В настоящее время идет процесс бурного развития информационных технологий, которые стали неотъемлемой частью нашей жизни. Вместе с этим, возрастает и количество угроз информационной безопасности. По данным МВД Республики Беларусь за прошедший год, количество угроз информационной безопасности в Республике Беларусь увеличилось на 63,6 % [1]. Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9 %. В связи с этим, необходима разработка эффективных методов и средств защиты информации. Главной целью, при разработке методов и средств информационной безопасности, является определение критериев защищенности информационных систем, формулировка требований к их уровню защищенности, а также формирование системного подхода к проблеме анализа и синтеза технических и программных средств защиты информации от несанкционированного доступа.

Одним из способов решения данной проблемы является комплексное использование аппаратных и программных средств защиты, которые должны быть ориентированы на комплексное обеспечение эффективного решения функциональных задач информационной системы. Методологически решение этих задач следует осуществлять как проектирование сложной, достаточно автономной программно-аппаратной системы во и взаимодействии с окружающими ее

функциональными задачами информационных систем. Для эффективного решения проблем информационной безопасности необходима комбинированная реализация программных и аппаратных средств, которые поддерживают современные криптографические алгоритмы, обеспечивающие решение подавляющего большинства проблем безопасности, таких как аутентификация, шифрование данных, контроль целостности, электронная цифровая подпись; и должны поддерживать гибкость применения и высокую масштабируемость решений.

Литература

1. Статистические данные за 2016 год // МВД Республики Беларусь. URL: http://mvd.gov.by/main.aspx?guid=3311 (дата доступа: 17.05.2017).

ИЗМЕНЕНИЕ В СТАНДАРТ СТБ 34.101.8-2006 ПРОВЕДЕНИЕ ИСПЫТАНИЙ

Д.И. Жукова, Д.В. Шуляк

Одним из основных изменений в СТБ 34.101.8-2006 является расширение классификации ПСЗВВП и АПС. В новой редакции стандарта добавляются следующие типы ПСЗВВП и АПС:

ПСЗВВП и АПС четвертого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку пакетов сетевого трафика и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС пятого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС шестого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку элементов объекта ИТ на наличие ВП, выявление вредоносного воздействия и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС седьмого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по сети, и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС восьмого типа после запуска по запросу пользователя должны обеспечивать проверку элементов объекта ИТ на наличие ВП и обезвреживание обнаруженных пассивных и активных ВП.

Ко всем типам ПСЗВВП и АПС стандарт устанавливает детальные требования. Уточненная классификация позволит улучшить качество СЗИ допускаемых к распространению на рынке Республики Беларусь.

Литература

1. СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY».

3. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

ОЦЕНКА НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ СОЗДАНИЯ РЕСПУБЛИКАНСКОЙ СИСТЕМЫ МОНИТОРИНГА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Ю.А. Ковалевич, И.В. Елсаков, А.В. Шкробот

При проектировании и построении республиканской системы мониторинга общественной безопасности (РСМОБ) для конкретных целевых групп объектов в рамках профильного сегмента обеспечения общественного порядка существует ряд противоречий в нормативно-правовых, организационно-технических и технических вопросах,

регламентирующих построение и функционирование систем видеонаблюдения:

– различия в терминологии;

– однозначно не регламентированы требования к защите информации / видеоинформации, включая ее защиту от модификации;

– не указаны категории объектов на которых допускается скрытая установка систем видеонаблюдения;

– имеется двойственность требований в обеспечении резервного электропитания;

– различие требований к составу охранной телевизионной системы / системы видеонаблюдения;

– несоответствие наименований и детализированного описания (параметр/показатель) уровней различения;

– отсутствуют единые требования к сертификации / подтверждению соответствия составных элементов системы видеонаблюдения;

– отсутствуют требования к молниезащите систем видеонаблюдения;

– не описаны вопросы организации передачи видеоинформации при создании и применении систем видеонаблюдения с использованием радиоканальной направляющей среды.

На основании изложенного выше можно сделать вывод, что создание нормативно-правовой базы, регламентирующей вопросы нормативно-правового, организационно-технического и технического обеспечения построения и функционирования РСМОБ является сложной задачей и потребует приведения в соответствие значительного числа действующих НПА/ТНПА Республики Беларусь в отрасли систем видеонаблюдения.

О ПРОЕКТАХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ СОЮЗНОГО ГОСУДАРСТВА

Э.П. Крюкова, А.А. Ковалевский

Целью работы, выполненной в рамках Союзной программы ((шифр «Норма»), было исследование особенностей, разработка организационно-правовых основ формирования систем и механизмов обеспечения информационной безопасности субъектов и критически важных объектов Союзного государства, защиты информации, не составляющей государственные секреты, об этих субъектах и объектах. Анализ законодательства Республики Беларусь и Российской Федерации в области обработки, использования и защиты сведений, составляющих служебную информацию ограниченного распространения, персональную информацию, коммерческую тайну, информацию на критически важных объектах показал, что при наличии согласующихся положений правовых актов имеются и существенные разночтения, и пробелы в механизмах защиты прав владельцев (собственников) такой информации и систем ее обработки. Разработаны проекты пяти нормативных правовых актов Союзного государства: «О порядке обработки, использования и защиты персональных данных», «О порядке использования и защиты сведений, составляющих коммерческую тайну», «О служебной информации ограниченного распространения в Союзном государстве», «О порядке использования и защиты служебной информации ограниченного распространения Российской Федерации и Республики Беларусь», «Концепция информационной безопасности критически важных объектов Союзного государства». При разработке этих документов использован современный мировой, в частности, европейский опыт правового регулирования отношений в рассматриваемых областях. Разработанные документы содержат положения, устанавливающие механизмы правового регулирования взаимоотношений государств-участников Союзного государства в области защиты критически важной информации, а также правоотношений субъектов государств-участников Союзного государства, и могут быть использованы для совершенствования национального законодательства.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ВАЖНЫХ ОБЪЕКТОВ

Э.П. Крюкова, В.А. Филипович

В законодательстве государств-участников Союзного государства нашли отражение основные задачи обеспечения информационной безопасности критически важных объектов

(КВО) отраслевых инфраструктур, включающие:

– обеспечение безопасности функционирования КВО и жизнедеятельности населения, в том числе, в условиях чрезвычайных ситуаций;

– предупреждение и локализация угроз техногенного характера, совершенствование систем мониторинга и прогнозирования чрезвычайных ситуаций техногенного характера;

– создание эффективных систем защиты КВО;

– недопущение организации и активизации террористической деятельности в отношении КВО инфраструктуры страны; разработка и реализация правовых и экономических средств защиты КВО.

Законодательство государств-участников Союзного государства устанавливает основные направления защиты информации на КВО:

– обеспечение конфиденциальности информации о критических активах, являющихся главными объектами диверсий и саботажа, информации, хранящейся в архивах и автоматизированных информационных системах организационного управления.

– обеспечение целостности и доступности информации (данных), циркулирующей в системах контроля и управления, созданных на базе вычислительной техники (компьютерных систем), важных для безопасности КВО.

Анализ национальных нормативных и нормативных технических актов государств-участников Союзного государства выявил подходы в области защиты информации и обеспечения информационной безопасности КВО, их согласованность и различия, что потребовало разработки соответствующего документа в рамках Союзного государства – Концепции обеспечения информационной безопасности КВО.

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ «ИНТЕРНЕТА ВЕЩЕЙ» (INTERNET OF THINGS)

В.Ф. Кулиш, Т.В. Борботько

Широкое распространение сетевых технологий и облачных вычислений, а также внедрение протокола IPv6 привело к появлению большого числа устройств Интернета вещей, подключенных к сети Интернет. Интернет вещей - концепция вычислительной сети физических устройств, оснащенных встроенными технологиями для взаимодействия друг с другом посредством сети Интернет. Осенью 2016 года стало известно о появлении ботнета Mirai, который на тот момент включал в себя 400 тыс. устройств Интернета вещей. Создатель ботнета предоставил в открытом доступе исходный код, использовавшийся для внедрения вредоносных программ. Это позволило исследователям изучить его архитектуру и выявить основные векторы атак.

1. Применение стандартных имен пользователей и паролей для аутентификации в панелях управления устройств. В коде модуля для заражения устройств был обнаружен список с именами пользователей и паролями. Для заражения ботнет использовал сетевой протокол telnet, который позволяет удаленно выполнять команды на устройстве.

2. Использование уязвимостей в веб-приложениях для управления параметрами устройства. Для атаки использовалась уязвимость в обработке данных, полученных по протоколу CWMP, который применяется поставщиками услуг подключения к сети Интернет для удаленного управления абонентским оборудованием.

Основными проблемами обеспечения безопасности являются небезопасная базовая конфигурация устройств, а также не реализованный механизм обновления этих устройств. Данные по распространенности устройств свидетельствуют о том, что устройств Интернета вещей с каждым днем будет становиться все больше. Поэтому проблема их безопасности является весьма актуальной.

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ СКАНЕРОВ В МОБИЛЬНЫХ УСТРОЙСТВАХ

И.И. Лабаревич

На данный момент самое распространенное применения биометрии в мобильных устройствах – это сканер отпечатка пальцев. На телефонах под управлением ОС IOS это Touch

ID, а на телефонах под управлением ОС Android это Fingerprint.

Алгоритмы реализации данной технологии в этих системах разные. Заранее скажу, что сканер отпечатков пальца на IOS на порядок лучше и гораздо труднее поддается взлому, чем аналогичная технология на Android-телефонах. Физически, эти сканеры реализованы по-разному, а также имеют разные способы шифрования самих сканов.

В телефонах компании Apple сканированный отпечаток пропускается через хеш-функцию и сохраняется в Secure Enclave – защищенном от доступа извне микрокомпьютере.

В телефонах под ОС Android до 6 версии операционной системы были даже такие казусы, как хранение сканов в памяти телефона, в незашифрованном виде, в общедоступной папке. С выходом Android 6.0 в Google не только разработали собственный API для аутентификации по отпечаткам пальцев, но и обновили Compatibility Definition Document, которому обязаны следовать все производители, желающие сертифицировать свои устройства для установки сервисов Google (это очень важный момент, о нем чуть позже).Было выпущено сразу два референсных устройства: Nexus 5X и Nexus 6P. В них – и неотключаемое шифрование раздела данных, и правильная реализация датчиков отпечатков, получившая название Nexus Imprint.

Сравнить безопасность Touch ID с ситуацией в мире Android не получится: если у Apple устройств единицы, то смартфонов на Android, наоборот, слишком много. В них могут использоваться самые разные датчики, основанные на разнообразных технологиях (от емкостных и оптических до ультразвуковых). Для разных датчиков подбирают разные технологии обхода. К примеру, для Samsung Galaxy S6 вполне срабатывает финт с разблокированием телефона моделью пальца, напечатанной на 3D-принтере из самого обычного пластика (с Apple Touch ID такой простой трюк не пройдет; для печати нужно будет использовать материал, обладающий особыми свойствами). Некоторые другие устройства легко обманываются распечатанными с высоким разрешением картинками. А вот сравнение с Nexus Imprint вполне имеет смысл. В Nexus 5X и 6P Google использовал образцово-показательный подход к безопасности. Это и неотключаемое шифрование раздела данных, и грамотная интеграция датчиков отпечатков, да и сами датчики выбраны не абы как. В устройствах сторонних производителей могут использоваться недостаточно безопасные датчики, могут зиять откровенные дыры в безопасности (несмотря на формальное соответствие требованиям Android Compatibility Definition). Дактилоскопическая аутентификация – не панацея. Ее основное предназначение не в том, чтобы сделать более безопасным конкретно твое устройство, а в том, чтобы снизить неудобства, связанные с безопасной блокировкой телефона, и таким образом убедить основную массу пользователей все-таки блокировать свои устройства.

АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОННОГО БИЗНЕСА

Л.М. Лыньков, В.С. Князькова

Организация электронного бизнеса (ОЭБ) с точки зрения технического обеспечения представляет собой единое информационное пространство, интегрирующее в себя функциональные области маркетинга, производства, финансов, кадров и т.п. Комплексная оценка информационной инфраструктуры ОЭБ, в частности ее информационной безопасности (ИБ) организуется через аудит системы ИБ. К основным особенностям проведения аудита ИБ ОЭБ можно отнести следующие. Во-первых, ОЭБ представляет собой сложную и многоуровневую систему, включающую множество подсистем (функциональные области, например, финансы и маркетинг) и надсистем (например, контролирующие органы). Во-вторых, средой функционирования ОЭБ является сеть Интернет, использование которой привносит дополнительные риски для организации в силу ее общедоступности. В-третьих, в ОЭБ на первый план выходит обучение всех без исключения сотрудников как минимум основам ИБ. Согласно исследованию, проведенному в 2014 г. компанией Ernst & Young, 33% респондентов назвали именно персонал одним из основных источников угроз ИБ.

Обычно ОЭБ осуществляет свою деятельность через интернет-сайт. В таком случае при аудите системы ИБ необходимо оценить такие аспекты, как соответствие контента и

назначения веб-сайта заявленным в уставе организации вилам деятельности, сам веб-сайт (его дизайн, контент, СЕО-продвижение), поведение посетителей сайта, а также уязвимость по отношению к внешним и внутренним угрозам ИБ. Аудитору необходимо также оценить ИБ ОЭБ с точки зрения ИБ при идентификации и аутентификации клиентов и контрагентов, обеспечения целостности, доступности и конфиденциальности информации о бизнес-трансакциях, получения или осуществления переводов денежных средств и пр. В данном контексте аудит системы ИБ ОЭБ осуществляется с целью: оценки рисков, связанных с возможностью реализации угроз ИБ ОЭБ; оценки текущего уровня защищенности информационной системы ОЭБ; выявления «узких мест» в системе защиты ИБ; оценки соответствия информационной системы требованиям стандартом по ИБ; разработки рекомендаций по внедрению новых и совершенствованию существующих механизмов ИБ ОЭБ.

Литература

1. Overcoming compliance fatigue. Reinforcing the commitment to ethical growth. 13th Global Fraud Survey [Electronic resource]. – Mode of access: http://www.ey.com/Publication/vwLUAssets/EY-13th-Global-Fraud-Survey/$FILE/EY-13th-Global-Fraud-Survey.pdf. – Date of access: 10.05.2017.

2. Ситнов А.А. Особенности аудита электронного бизнеса / А.А. Ситнов // Аудитор. 2013. № 7.

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ОЦЕНКИ КОЛИЧЕСТВА ПРОСМОТРОВ ИНТЕРНЕТ-ПУБЛИКАЦИЙ

Т.Н. Михайлова, Д.В. Щегрикович

Продвижение публикаций в сети Интернет – сложная динамически развивающаяся отрасль. Авторам интернет-статей необходимо понимать возможности популяризации материала и быть уверенным в сохранности авторского права. Разработанное программное решение позволит журналистам и редакторам оптимизировать текст публикаций и сохранить уникальность своего материала, рекламодателям уменьшить затраты на рекламный бюджет, а содержателям новостных ресурсов расширить их функционал. Принцип работы описываемого подхода заключается в извлечении 120 признаков из текста публикации методами обработки естественного языка [1], описывающих ее морфологические, графематические, синтаксические, семантические и пунктуационные свойства [2]. Разработанная система представляет собой веб-ресурс, который на основе текста статьи предсказывает популярность публикации. Прогнозирование популярности представляет собой бинарную классификацию: отнесение потенциальной публикации к классу «Популярная публикация» – набранное количество просмотров за неделю – от 0 до 2500 просмотров, или «Не популярная публикация» – от 2500 просмотров за неделю [3, 4]. Достигнутая точность работы модели – 67 % правильно классифицированных объектов из тестовой выборки. Выделены значимые и не значимые признаки для популяризации новостной интернет-публикации на данном ресурсе [5]. Характеристики, которыми описывается текст с целью построения прогноза популярности можно использовать для сравнения публикаций на предмет похожести: высокое значение корреляции признаков двух статей свидетельствует о возможном незаконном использовании материалов. Такой способ позволит защитить авторское право, избежать плагиата, и, самое главное, – избежать использование видоизмененного текста, так как в отличие от систем антиплагиата, которые производят стандартное сравнение текстов, он позволяет произвести глубокую оценку их структуры: тональности, сложности, запутанности и мн. др.

Литература

1. Natural Language Processing and Text Mining / Edited by Anne Kao and Stephen R. Poteet. 272 p.

2. Stefan, T.H. Quantitative corpus linguistics with R.

3. Flah, P. Machine Learning: The Art and Science of Algorithms That Make Sense of Data / P. Flah. – 2015. – 400 p.

4. Duda, R.O. Pattern Classification / R.O. Duda, P.E. Hart, D.G. Stork. – NY.: John Wiley Sons, 2001. – 639 p.

5. Breiman, L. Out-Of-Bag estimation. Technical report, Statistics Department University of California / L. Breiman. – Berkeley, 1996.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ НЕБОЛЬШОГО ПРЕДПРИЯТИЯ

Я.Л. Могилёвчик

Обсуждаются результаты аудита информационной безопасности в компьютерной сети небольшого предприятия. Сеть включает 84 компьютера, 7 принтеров, 3 МФУ и 3 физических сервера. Структура сети представляет собой 2 соединенных 10-портовых коммутаторов D-Link DSG-1210-10P и порядка 9 подключенных к ним и друг к другу различных неуправляемых коммутаторов.

В ходе аудита были определены области правильного функционирования сети, исследованы уязвимости и риски, обследованы возможности защиты периметра, защиты сегментов сети, содержащих общедоступные сервисы и отделяющие их от частных (демилитаризованых зон сети) и другие работы. Особое внимание было уделено инспекции пакетов с хранением состояния (Stateful Packet Inspection), что позволило дополнительно защититься от атак, выполняя проверку проходящего трафика на корректность.

В докладе показано, что проведенный аудит дал возможность полностью окупить затраты на свое проведение (как материальных, так и человеческих ресурсов) за счет сокращения инцидентов информационной безопасности в сети по окончании аудита (сократились затраты на ликвидацию инцидентов).

О ФОРМИРОВАНИИ ЦЕНТРАЛИЗОВАННОГО АУДИТА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОСТАВЕ ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ РЕСПУБЛИКИ БЕЛАРУСЬ

А.О. Молчан, О.Э. Сязанцев

В силу быстро растущей информатизации общества количество хранимой, обрабатываемой и передаваемой в электронном виде информации растет в геометрической прогрессии. Возникает острая необходимость в контроле и ограничении доступа к обрабатываемой информации, а также в своевременной информированности ответственных за информационную безопасность (далее – ИБ) лиц об инцидентах ИБ. Помимо общедоступности информации уязвимость информационных систем (ИС) возрастает также за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения (ПО). Для мониторинга ИС на предмет корректного функционирования всех ее процессов, активов и ресурсов, а также сохранности информации, доступ к которой ограничен, в составе системы защиты информации (СЗИ) ИС организуется подсистема аудита событий ИБ.

Системы аудита событий ИБ используются для мониторинга ИС на предмет корректного функционирования и сохранности информации, доступ к которой ограничен. На данный момент существует множество средств аудита событий ИБ, как встроенных в общесистемное ПО, так и специально разработанных программных и программно-аппаратные комплексов. Однако, в государственных ИС согласно законодательству Республики Беларусь в области защиты информации (ЗИ) допустимо использование только тех средств ЗИ, которые прошли сертификацию по требованиям безопасности информации и получили сертификат соответствия либо экспертное заключение на соответствие требованиям технических нормативных правовых актов в области технического нормирования и стандартизации.

Многие средства ЗИ ведут журналы аудита автономно, и интеграция их производится вручную ответственными за ИБ лицами. Главная проблема формирования централизованного аудита ИБ в составе СЗИ ИС на данный момент является дороговизна иностранных продуктов (в частности, систем SIEM) и ограниченное представление систем аудита ИБ белорусского производства на рынке средств ЗИ, которые также позволяли бы снизить угрозы ИБ.

Для решения данного вопроса были выявлены требования к подсистеме аудита ИБ на основании законодательной базы Республики Беларусь, обеспечивающие максимальную безопасность в современных условиях, проведен анализ средств аудита ИБ представленных в реестре средств ЗИ, утвержденном Оперативно-аналитическим центром при Президенте Республики Беларусь, сформулированы рекомендации по формированию централизованного аудита ИБ.

ДИАГНОСТИКА ПСИХОФИЗИОЛОГИЧЕСКИХ ПОКАЗАТЕЛЕЙ ОПЕРАТОРОВ ИЕРАРХИЧЕСКИХ СИСТЕМ ВЫСОКОЙ ОТВЕТСТВЕННОСТИ В ЭКСТРЕМАЛЬНЫХ СИТУАЦИЯХ

Н.В. Пушкарева, В.А. Гущо

Диагностика должна позволять на ранних стадиях отслеживать отклонение психофизиологического состояния операторов расчетов сложных систем управления от нормы. Современное оборудование достоверно определяет даже малейшие сдвиги в анатомии и физиологии различных тканей организма. Однако обследование такими методами как ультразвуковое исследование, компьютерная томография, позитронно-эмиссионная томография и т.д. часто бывает дорогостоящим, громоздким и требует работы квалифицированных специалистов с медицинским образованием. При работе с лицами экстремальных видов деятельности требуется внедрение в практику работы новых методов и устройств для диагностики психофизиологического состояния (ПФС) человека в ходе выполнения поставленных задач. Необходимо применение других высокоточных, доступных для широкого использования и простых в эксплуатации технологий. При всем разнообразии аналитических методов, применяемых в современной медицине, все чаще ставится задача проведения превентивной диагностики [1]. Измерения в «боевых» условиях и в учебно-тренировочной работе требуют кратковременной, нетрудоемкой и информационной процедуры обследований. Всякая групповая деятельность, особенно операторская, протекает в условиях обратных связей. В этой взаимосвязанной деятельности любая акция одного члена группы вызывает «возмущение» в деятельности других, вынужденных сообразовываться с ней.

Системы группового слежения высокой ответственности включают в свой состав операторов, работающих не только на одном уровне иерархии. Повышение точности сопровождения в них основано на идее одновременной параллельной работы двух, а в общем случае и большего числа операторов. Такие системы представляют собой иерархические системы группового слежения (ИСГС) – это многоуровневые системы, включающие в свой состав нескольких операторов слежения. В ИСГС каждый оператор нижнего уровня включен в контур управления оператора верхнего уровня (более высокого). Под управлением понимается комплектование групп операторов и эргономическое обеспечение качества их работы. Для комплектования групп необходимо произвести подбор операторов, предрасположенных по своим психофизиологическим параметрам к групповой деятельности. В качестве диагностического устройства для подбора операторов предлагается дополнительно с гомеостатической системой использовать также иерархическую систему группового слежения. В качестве диагностического устройства на основе ИСГС могут применяться схемы Г. Татевосяна и А. Мелешева.

Литература

1. Бояркин М.А., Шапцев В.А. Об одном из подходов к решению проблемы «Человеческого фактора» на объектах нефтегазового комплекса [Электронный ресурс]. – Режим доступа: http://www.ipdn.ru/rics/doc0/DB/b3/3-boya.html. – Дата доступа: 19.05.2017.

ИНФОРМАТИЗАЦИЯ ОБЩЕСТВА И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ

Е.А. Свирский

Внедрение информационных технологий во все сферы деятельности общества стало нормой. И, очевидно, что обратного пути нет. Темпы развития и внедрения информационных технологий очень высоки. С одной стороны это радует, поскольку высокие темпы свидетельствуют об устойчивом движении общества к развитию и самосовершенствования, а со второй создает проблемы, связанные с освоением и пользованием инновационных технологий. Инновационные технологии далеко не всегда доведены до совершенства и могут стать источниками угроз безопасности для пользователей, как в плане несанкционированного предоставления доступа к ресурсам пользователей, так и личной безопасности пользователей.

Если реклама по новым продуктам информационных технологий активно распространяется самими производителями этих продуктов, то освещения вопросов безопасного их использования, особенно в сочетании с другими информационными

продуктами почти не ведется или эти вопросы обсуждаются только в профессиональной среде. До рядового пользователя существующие угрозы в популярных продуктах информационных технологий и возможные последствия их использования не доходят. Вообще говоря, даже лица в обязанности, которым вменено обеспечивать информационную безопасность, далеко не всегда осведомлены с существующими проблемами в сфере защиты информационных ресурсов и тем более защиты личности.

В настоящее время перед обществом встает серьезная проблема ликбеза в сфере защиты личности и информационных ресурсов, как общества в целом, так и отдельных пользователей. На государственном уровне этой проблеме достаточного внимания не уделяется. Необходимо выработать концептуальные основы повышения осведомленности общества в проблемах информационной безопасностью, и самым серьезным образом подойти к проблемам информационного зомбирования. Промедление в решении этих вопросов может серьезно повлиять на мотивационное поведение масс, защищенность государства от внешнего вмешательства в управление и устойчивое экономическое и политическое развитие государства.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОСНОВА ДЛЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

М.В. Сороко, А.М. Прудник

Рассматриваются практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2013 [1]. СМИБ – это часть общей системы управления организации, которая основана на оценке рисков, и которая предназначена для реализации, эксплуатации, мониторинга и совершенствования ИБ.

Перед разработкой СМИБ должно быть получено одобрение руководства для организации; должен быть разработан план проекта, который, в частности, предполагает определение области применения; определены требования, которым должна соответствовать СМИБ, должны быть определены информационные активы организации и получены данные по текущему состоянию ИБ в рамках области применения СМИБ; должна быть определена методология оценки рисков, сама оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими.

Собственно разработка СМИБ предполагает разработку конечной структуры организации с описанием ролей и сфер ответственности; разработку политик ИБ; разработку процедур обеспечения ИБ; разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления; разработку средств управления; план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, включая аспекты аудита, мониторинга и измерения; разработку программы обучения, образования и информирования персонала организации в области ИБ, в т.ч. материалы для обучения в области ИБ, само обучение в области ИБ, включая разъяснение функций и ответственности, планы обучения и записи результатов обучения, образования и информирования в области ИБ и разработку конечного плана проекта СМИБ.

После разработки и внедрения СМИБ организации надлежит выполнить процедуры мониторинга и анализа, провести внутренний и внешний аудиты, произвести измерение результативности средств управления с целью определения их соответствия требованиям безопасности, а также выполнить оценки рисков.

Заключительными действиями являются разработка процедур по корректирующим и предупреждающим действиям, произвести проверку полного соответствия СМИБ по контрольной таблице стандарта ISO/IEC 27003 [2] и, при необходимости сертификации по национальному стандарту [3], провести внешний аудит.

Литература

1. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements // International Organization for Standardization. URL: https://www.iso.org/standard/54534.html (дата доступа: 17.05.2017).

2. ISO/IEC 27003:2017 Information technology – Security techniques – Information security

management systems – Guidance. // International Organization for Standardization. URL: https://www.iso.org/standard/63417.html (дата доступа: 17.05.2017).

3. СТБ ISO/IEC 27001:2016. Системы менеджмента информационной безопасности. Требования. Введ. 2016-01-10. Минск: БелГИСС, 2016. 28 с.

ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД АНАЛИЗА ДЕФЕКТОВ ПРИ КОНТРОЛЕ ПЛАНАРНЫХ СТРУКТУР

Е.А. Титко

В работе представлены быстродействующие алгоритмы эффективного обнаружения дефектов планарных структур, возникающих при изготовлении из СБИС. Они основаны на объектно-ориентированном подходе анализа дефектов с помощью сегментированных алгоритмов с минимальной логической сложностью [1]. При этом достигается расширении структурных информационных данных о топологии при некотором изменении аппаратной операции оборудовании автоматического контроля разных модификаций одного семейства. Это достигается за счет большого запаса по производительности, в результате которого появляется возможность иметь оригинальные, но унифицированные с точки зрения исполняемого кода, алгоритмы для различных типов топологии и, соответственно, различных топологических слоев, а также для различных типов дефектов. При этом настройка на конкретный тип топологии или дефекта осуществляется за счет смены базы данных алгоритма, а сам алгоритм может оставаться, практически, неизменным.

В результате применения разработанных алгоритмов обнаружения дефектов достигается высокая производительность автоматического оборудования, повышение субпиксельного разрешения, возможность специализации алгоритмов по типам обрабатываемой топологии и группам дефектов, упрощение аппаратной реализации путем распараллеливания и совмещения во времени операций, выполняемых за один такт.

Самостоятельное значение имеет возможность определения фотолитографической значимости дефектов в режиме реального времени. В некоторых случаях возможность определения фотолитографической значимости дефектов в режиме реального времени позволяет также автоматически принимать решение о критичности дефекта и, соответственно, выполнять пакетную обработку шаблонов в автоматическом режиме.

Литература

1. Титко, Е.А. Универсальная система получения субпиксельного разрешения / Е.А. Титко, С.А. Манин, Г.А. Зубов // Информационные технологии и системы 2016 : материалы Междунар. науч. конф., Минск, Респ. Беларусь, 26 окт. 2016 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2016. – С. 88–89.

МЕТОД КОМПЕНСАЦИИ ПОГРЕШНОСТЕЙ РАССОВМЕЩЕНИЯ РЕАЛЬНОГО И ЭТАЛОННОГО ОБЪЕКТОВ

Д.С. Титко

В работе рассматривается метод автоматизированного контроля топологии планарных структур, который основан на системе динамического автосовмещения реального и эталонного изображений [1]. Метод основан на алгоритмической минимизации количества ложных дефектов.

Разработанный метод предназначен для системы маскирования ложных дефектов, которая работает на основании информации, получаемой от устройства распознавания края элемента, которое на каждом шаге работы детектора дефектов вырабатывает признак края элемента, который принимает значение «1» при компарировании края элемента и значение «0» – в противном случае. Эта система, при вводе соответствующего признака оператором-технологом, позволяет маскировать несовпадения реального и искусственного изображений в диапазоне ±1 или ±2 пикселя относительно положения края элемента искусственного изображения. В результате появляется возможность снизить чувствительность установки на краях элементов, что позволяет контролировать топологию изделий для которых допускается

более высокая неровность края элементов и не регистрировать большое количество ложных дефектов на краях элементов топологии. Метод компенсации погрешностей рассовмещения реального и эталонного объектов предназначен для оснащения оборудования автоматического контроля топологии, включая: систему привязки координатной системы установки к эталонной координатной системе, систему динамического автосовмещения реального и эталонного изображений, систему маскирования несовпадений на краях элементов топологии. Предложенная алгоритмизация и аппаратно-программная реализация на ее основе была использована при разработке программного обеспечения компенсации погрешностей рассовмещения реального и эталонного объектов установок ЭМ-6029Б и ЭМ-6329 автоматического контроля топологии планарных структур.

Литература

1. Аваков, С.М. Автоматический контроль топологии планарных структур / С.М. Аваков. – Минск : ФУАинформ, 2007. – 168 с.

МЕТОДЫ ЭВРИСТИЧЕСКОГО АНАЛИЗА ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ВЕБ-ПРИЛОЖЕНИЯХ

А.С. Цалко, П.В. Кучинский

В большинстве случаев сетевых атак злоумышленниками на веб-приложения результатом являются загруженные файлы – вредоносное программное обеспечение. Самым старым и популярным методом обеспечения защиты приложений является сигнатурный анализ. Связано это с тем, что атаки на веб-приложения в большинстве случаев производятся на основе уже известных уязвимостей с использованием готовых инструментальных средств [1].

С каждым днем исходные коды вредоносного ПО стараются замаскировать и сделать как можно более изменчивым, «полиморфным» или наоборот, сделать максимально простым и похожим на обычный скрипт. Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт. Не редки случаи размещения исходного кода в базах данных веб-сайтов, а также в изображениях [2].

При применении злоумышленником нового метода обфускации или места размещения исходных кодов сигнатурный автоматический анализ не даст результатов. В этом случае на помощь приходят методы эвристического анализа – совокупность функций, нацеленных на обнаружение неизвестных сигнатурным базам вредоносного ПО.

Метод эвристического анализа определяет по косвенным признакам, является ли объект вредоносным. Причем в отличие от сигнатурного метода эвристик может детектировать как известные, так и неизвестные угрозы безопасности. Для того, чтобы применить методы эврестического анализа для веб-приложений (веб-сайтов), необходимо рассматривать их в качестве «черного ящика». Система, которую представляют как «черный ящик», изучается как имеющая некий «вход» для ввода информации и «выход» для отображения результатов работы, при этом происходящие в ходе работы системы процессы наблюдателю неизвестны.

Для определения набора паттернов поведения вредоносное ПО необходимо классифицировать и группировать по методам использования. В результате исследования поведения найденных с помощью сигнатурного сканирования образцов вредоносного ПО удалось выделить многие паттерны поведения и методы их детектирования.

Использование методов сигнатурного анализа позволило выявить за месяц наблюдений 8 новых произведенных атак на PHP-сайты, подконтрольные ЦИИР БГУИР. Использование данных методов наблюдения за поведением серверов и внешними изменениями вкупе с сигнатурным анализом является неотъемлемой частью обеспечения информационной безопасности веб-сайтов.

Литература

1. Anti-Malware.ru, Коробочная безопасность веб-приложений. Внутренности Web Application Firewall [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Web_Application_Firewall. – Дата доступа: 17.02.2017.

2. Sucuri.net, Malware Hidden Inside JPG EXIF Headers [Электронный ресурс]. – Режим доступа: https://blog.sucuri.net/2013/07/malware-hidden-inside-jpg-exif-headers.html. – Дата доступа: 17.02.2017.

МЕРА СХОЖЕСТИ НЕЛИНЕЙНОСТЕЙ ВОЛЬТАМПЕРНЫХ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ ЗАКЛАДНЫХ УСТРОЙСТВ СЪЕМА ИНФОРМАЦИИ

В.М. Чертков, В.К. Железняк

Мера сходства играет ключевую роль при формировании классификации изучаемого множества параметров объекта и при распознавании принадлежности объектов к тому или иному классу. Специфика этих задач состоит в том, что мера сходства здесь является величиной относительной, она зависит не только от сходства объекта с определенным классом, но и от его сходства с другими классами [1]. Актуальность темы обусловлено решением проблемы определения меры схожести нелинейностей вольтамперных характеристик (ВАХ) радиоэлектронных закладных устройств съема информации, полученных на основе разработанного авторами способа распознания типа нелинейности [2]. В качестве критерия определения меры сходства известной и расчетной ВАХ, т.е. распознания типа ВАХ, выбрано средние значение среднеквадратических отклонений каждого расчетного коэффициента аппроксимирующего полинома третьей степени. В ходе проведения экспериментов определен оптимальный порог критерия меры сходства для принятия решения о соответствии задаваемой и расчетной ВАХ.

Литература

1. Количественная мера компактности и сходства в конкурентном пространстве / Н.Г. Загоруйко [и др.] // Сибирский Журнал Индустриальной Математики. – 2010. – Т. XIII. – № 1. – С. 59–71.

2. Чертков, В.М. Идентификационный портрет как основной параметр идентификации РЭС / В.М. Чертков, В.К. Железняк // Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. Минск, 31 марта 2016 г. – С. 237–241.

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

Д.В. Шандяло

В отличие от всех других сред передачи информации, формирование каналов несанкционированного съема на участках волоконно-оптического тракта, требует прямого доступа к оптоволокну и специальных мер отвода части излучения из оптоволокна. Извлечение информации при регистрации выведенного из волокна излучения зависит от вероятности ошибочного приема одного двоичного символа передаваемой информации и вероятности искажения кодовых комбинаций. Эти показатели зависят от вида используемых сигналов, от способов обработки сигналов, а также от длительности используемых кодовых комбинаций. В данной работе приведены вычислильная работа и концепция в виде физического эксперимента, при использовании подключения посредством метода импульсной рефлектометрии. Дается определение, описание, а также способ формирования технического канала утечки информации в волоконно-оптических технологий. Основой системы фиксации несанкционированного доступа (НД) является система диагностики состояния (СДС) оптического тракта, которая построена с анализом отраженного сигнала. На основании проведенного анализа и дальнейших исследований, предполагается обосновать соответствующие способы защиты информации в ВОЛС, а также разработать алгоритм и методику оценки защищенности ВОЛС. Методика оценки защищенности информации от несанкционированного доступа в ВОЛС описывает основные принципы, средства и методы обеспечения ИБ и может использоваться для оценки рисков нарушения ИБ

На основании исследования сделаны выводы по возможности улучшения контроля и повышения защищенности передаваемой информации по ВОЛС. В качестве возможных мер, позволяющих достичь этого, рассматривается использование постоянной и эффективной

защиты информационных ресурсов, в состав которой входит методика оценки защищенности информации от несанкционированного доступа в ВОЛС. Разработанная методика помогает уточнить величину информационных потерь при заданных вероятностях обнаружения и ложного срабатывания. Показано, что необходимость практического внедрения и эффективного использования защищенных ВОЛС в сетях связи является задачей сегодняшнего дня.

Литература

1. Гришачев, В.В. Анализ каналов утечки информации в оптиковолоконных системах связи / В.В. Гришачев, В.Н. Кабашкин, А.Д. Фролов // Вопросы защиты информации. – 2003. – № 1 (44).

2. Спирин, А.А. Введение в технику оптоволоконных сетей / А.А. Спирин. – М.: Наука, 1998. – 428 с.

СЕКЦИЯ 2
ОБНАРУЖЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

STUDY OF THE RELATIONSHIP OF SIGNAL / NOISE RATIO AND SPEECH INTELLIGIBILITY IN POSSIBLE POINTS OF INFORMATION LEAKAGE

Amakiri Minafuro, Ojuka Samuel, Khomo Khoaba Bigde, O.B. Zelmanski

Currently, various technical devices are used to intercept speech information: directional and laser microphones, dictaphones, etc. The main channels of the leakage are direct acoustic and vibration [1]. The work is devoted to the estimation of the effect of the type of interference signal and the signal-to-noise ratio on the security of speech information. The expert methods were selected as evaluation methods. During the experiment, speech intelligibility was assessed when various types of noise signals were exposed to it at different signal-to-noise ratios. Such interferences as white noise, a voice chorus (the voices of several speakers), as well as a speech-like signal formed directly from the speaker's speech were investigated. For the experiment, the following equipment was used: the Edifier R1900 T3 speaker system for playing test and interference signals, the sound spectrum analyzer MANOM-4/2, the Behringer C-1 microphone, two laptops with the Cool Edit Pro2 software installed for playing test signals and recording sound. The test signals were recorded in an acoustically muffled room. The vibration channel was studied by recording and listening to a mixture of useful and interference signals passing through the elements of enclosing structures (double-glazed windows, doors). As the sources of vibration interference, acoustic transducers included in the delivery of the device for protecting voice information "Priboi" were used. The direct acoustic channel was studied by recording and listening to a mixture of useful and interference signals at various points in the space of the room. The choice of such points is due, first, to the proximity to the elements of building structures with minimal values of their own sound insulation, and secondly, to the geometry of the room. Standing waves create a series of peaks and dips in the room, while in certain areas, the volume levels can be higher than those reproduced by the source. Accordingly, points were selected near the walls, in zones of dihedral angles (wall / ceiling joints, wall / floor, etc.), and in triangular angles (wall / wall / ceiling joints). The acoustic noise analyzer was used for the initial estimation of signal levels and noise. The phonograms containing noisy test signals were listened to by 10 auditors (5 women and 5 men) at signal-to-noise ratios of 10, 0, –5 and –10 dB. The conclusions drawn on the basis of these results indicate that the speech-like interference formed directly from the masking speech seems to be the most effective for protecting speech information, since it makes it possible to provide the required speech intelligibility value at a noise level by 5–10 dB lower than in the case of white noise application.

Literature

1. Active and passive methods and means of information protection against leakage via technical channels: monograph. / Ed. L.M. Lynkov. – Minsk: Bestprint, 2011. – 275 p.

ПРИМЕНЕНИЕ КОМПЛЕКСНОГО ВЕЙВЛЕТА МОРЛЕ ДЛЯ ОЧИСТКИ РЕЧЕВОГО СИГНАЛА ОТ ШУМОВ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ

И.Б. Бурачёнок, В.К. Железняк

В настоящее время развитие информационных технологий позволяет реализовывать сложные алгоритмы обработки сигналов с использованием цифровых методов и средств. Существенную роль среди таких алгоритмов играют линейные интегральные преобразования, которые являются особенно эффективными для обработки полезных сигналов, в нашем случае принятых измерительных сигналов (ИС) на выходе технического канала утечки информации (КУИ) в условиях наличия шумов и помех. Одним из таких преобразований является вейвлет-преобразование, позволяющее путем трансформации выходного ИС провести его детальный частотно-временной анализ. Значительный вклад в теорию вейвлет-преобразования, в частности, вейвлет-фильтрации, внесли зарубежные ученые: И. Добеши, Д. Донохо, С. Малла, И. Мейер, а также российские, украинские и белорусские ученые, среди которых следует отметить работы Н. М. Астафьевой, А. П. Петухова, О. В. Рыбальского.

По сравнению с другими методами вейвлет-очистка ИС от шумов имеет ряд преимуществ, заключающихся в первую очередь в оптимальной частотно-временной локализации, что позволяет обнаружить компоненты шума вблизи некоторой точки и, не искажая при этом самого сигнала, удалить их, тем самым очистив полезный сигнал от шума. Математическое обоснование метода очистки речевого сигнала от шумов с использованием комплексного вейвлета Морле (КВМ) и сравнение его с другими методами нами было рассмотрено в работе [0]. Применение КВМ для анализа тонкой структуры ИС, принятого на выходе КУИ, позволило выявить наличие разномасштабной периодичности, содержащейся в анализируемых зависимостях, а также выявить появившиеся частотные составляющие, не соответствующие его собственным частотам. Это открыло реальную возможность осуществить дополнительную очистку ИС от шумов и, тем самым, существенно повысило точность оценки защищенности речевой информации в КУИ.

Исследования показали, что вейвлет-анализ целесообразно проводить при определенно заданных отношениях мощности ИС к мощности шума.

Литература

1. Бурачёнок, И. Б. Анализ вейвлет-преобразованием тонкой структуры гласных звуков речевого сигнала / И. Б. Бурачёнок, В. К. Железняк // Теоретические и прикладные аспекты информационной безопасности : материалы междунар. науч.-практ. конф., Минск, 19 июня 2014 г. / УО «Акад. М-ва внутр. дел Респ. Беларусь»; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2015. – С. 124–128.

ОПРЕДЕЛЕНИЕ ТОНАЛЬНОСТИ ТЕКСТА МЕТОДОМ ОБУЧЕНИЯ БЕЗ УЧИТЕЛЯ

А.И. Гербик, М.В. Аксамит, Е.А. Макович

Для определения тональности текста в настоящее время активно применяются методы машинного обучения с учителем, однако для их применения необходимо наличие обучающей выборки. Сбор данных для обучающей выборки может быть либо невозможен, либо неоправданно затратен. В таких случаях целесообразно применять методы обучения без учителя.

Данный метод определения тональности состоит из трех шагов. На первом шаге из текста выделяются фразы, которые могут выражать мнение автора. Для этого для всех слов текста определяются их часть речи, затем в тексте осуществляется поиск фраз, которые соответствуют одному из синтаксических шаблонов, часто используемых для выражения мнения (например, существительное + прилагательное либо глагол + наречие). На втором шаге определяется тональность фраз, выделенных на первом шаге. Для этого из поточечной взаимной информации фразы и слова «хороший» вычитается поточечная взаимная информация этой же фразы и слова «плохой». Поточечная взаимная информация – логарифм отношения вероятности появления двух терминов вместе к вероятности появления этих терминов независимо друг от друга. В качестве оценки вероятности используется количество результатов поисковой системы на соответствующий запрос. В результате для каждой фразы будет получено значение тональности: положительное число будет означать положительную тональность, отрицательное – негативную. На третьем шаге определяется тональность текста путем нахождения среднего значения тональностей фраз, входящих в данных текст.

Подходы, основанные на обучении без учителя, хоть и показывают меньшую точность в работе, но получаемые модели являются доменно-независимыми и верно определяют тональность отдельных слов, значение которых зависит от контекста.

Литература

1. Bing Liu. Sentiment Analysis and Opinion Mining, Morgan & Claypool Publishers, May 2012.

2. Bo Pang, Lillian Lee, Shivakumar Vaithyanathan. Thumbs up? Sentiment classification using machine learning techniques // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). 2002. P. 79–86.

ОПРЕДЕЛЕНИЕ ТОНАЛЬНОСТИ ТЕКСТА МЕТОДОМ ОБУЧЕНИЯ С УЧИТЕЛЕМ

А.И. Гербик, Е.А. Макович, М.В. Аксамит

Целью анализа тональности является нахождение мнений в тексте и определение позиции автора относительно упомянутой темы. При наличии выборки размеченных данных данную задачу можно рассматривать как задачу классификации, эффективными методами решения которой являются методы машинного обучения с учителем.

Для того, чтобы методы решения задач классификации можно было применить для анализа тональности текста, необходимо текст представить в виде математического вектора. В настоящее время одной из самых распространенных в различных областях лингвистических исследований является векторная модель «мешок слов». Текст в данной векторной модели рассматривается как неупорядоченное множество слов. Вектор, являющийся модельным представлением текста в векторном пространстве, образуется упорядочением весов всех слов (включая те, которых нет в конкретном тексте). Размерность этого вектора равна количеству различных слов во всей коллекции, и является одинаковой для всех текстов коллекции.

Полученную задачу классификации можно решить различными методами машинного обучения: наивный байесовский классификатор, логистическая регрессия, метод опорных векторов, методы нейронных сетей и т.д. Сравнив их временную сложность, качество полученных моделей, масштабируемость можно выбрать наиболее подходящий для конкретных данных и конкретной задачи.

Литература

1. Bo Pang, Lillian Lee, Shivakumar Vaithyanathan. Thumbs up? Sentiment classification using machine learning techniques // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). 2002. P. 79–86.

2. Kushal Dave, Steve Lawrence, and David M. Pennock. Mining the peanut gallery: Opinion extraction and semantic classification of product reviews. In Proceedings of WWW, pages 519–528, 2003.

ИССЛЕДОВАНИЕ РАЗБОРЧИВОСТИ РЕЧИ С ИСПОЛЬЗОВАНИЕМ СВЯЗНЫХ ТЕКСТОВ НА АРАБСКОМ ЯЗЫКЕ

С.М. Горошко, С.Н. Петров

Исследования разборчивости речи (Н.Б. Покровский, Ю.С. Быков, М.А. Сапожков) начались в середине прошлого века в связи с возникшей необходимостью оценки качества средств связи. Факторов, ухудшающих передачу речи, может быть несколько: фоновый шум, длинные поздние отражения и эхо. В результате были получены базовые зависимости между различными видами разборчивости: слоговой, словесной, фразовой. Методы измерения разборчивости речи можно разделить на: субъективные (чисто субъективный метод; объективизированный; тональный); объективные (формантные, AI (индекс артикуляции), SII (индекс разборчивости речи); модуляционные: (STI (Speech transmission index – индекс передачи речи), RASTI (быстрый STI), STIPA (STI для систем звукоусиления), STITEL (STI для телекоммуникационных систем). Однако в реальности мы имеем дело только со связными текстами. Существующая методика оценки защищенности речевой информации от утечки по техническим (акустическим) каналам нуждается в корректировке с учетом специфики задач защиты информации и, прежде всего, в определении методических и косвенных погрешностей.

Целью работы является усовершенствование и общепринятой инструментальной методики оценки разборчивости речи на основе модернизации зависимостей коэффициентов восприятия и словесной разборчивости от формантной.

Испытания проводились с использованием связных текстов в произношении дикторов, свободно владеющих арабским языком. Необходимо установить различия методов при оценке разборчивости связной речи и отдельных фраз, слов, а также выявить факторы, существенно усложняющие разборчивость речи на арабском языке. Целесообразно сформировать речеподобный и формантный шум для оценки эффективности защищенности речевой информации.

Литература

1. Покровский, Н.Б.Расчет и измерение разборчивости речи / Н.Б. Покровский. – М.: Связьиздат, 1962. – 392 с.

2. Михайлов, В.Г. Измерение параметров речи / В.Г. Михайлов. – М.: Радио и связь, 1987. – 168 с.

ОПЕРАТИВНЫЙ КОНТРОЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОБРАБОТКИ ДАННЫХ НАТУРНОГО ЭКСПЕРИМЕНТА С ИСПОЛЬЗОВАНИЕМ ГРАФОВ И ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

В.К. Железняк, Д.С. Рябенко, С.В. Лавров, С.Н. Абраменко

Оперативный контроль защищенности объектов информатизации (ОИ) обеспечивают параметрическим методом, основанным на измерительном контроле [1]. Планирование контроля основано на установленном требовании к показателям точности. Достоверность контроля должна отображать степень объективности результатов контроля [2]. Для сложных объектов, каким является ОИ, устанавливают требования к показателям защищенности $П \in [Пн, Пв]$, где Пн и Пв – нижние и верхнее поле допусков показателей защищенности.

В современных ОИ используют устройства автоматизированного встроенного контроля параметров средств активной защиты. Для оперативного контроля оценки защищенности информационных объектов используют систему измерительную автоматизированную (СИА) К6-6 Россия и комплекс измерительный программно-аппаратный КИПА (Республика Беларусь), К6-6 и КИПА формируют стимулирующие сигналы с нормируемыми метрологическими характеристиками. Точностные параметры определяются первичными измерительными преобразователями в соответствии с требования измерительного контроля, точностные свойства которых устанавливаются показателями достоверности по ГОСТ 19919-74. В К6-6 и КИПА предусмотрен самоконтроль, поэтому они не влияют на результаты контроля параметров ОИ.

Достоверность диагностического контроля систем ОИ оцениваются функциональным методом поиска и локализации состояния параметров [3]. Вероятностный анализ состояния систем ОИ проводят с использованием графов переходов из состояния *i* в состояние *j* с интенсивностями *ij* попарно несовместных состояний, что образует полную сумму вероятностей, равной единице [4]. Ориентированный граф охарактеризовывают матрицей инциденций, строки которой соответствуют вершинам графа, а ее столбцов – ориентированным ребрам [5]. Методика расчета систем с обратными связями и их цепей при помощи графов, составляемых по схемам, предложены в работе [6].

Литература

1. Железняк В.К. Защита информации от утечки по техническим каналам. – СПб, 2006. – 188 с.

2. Кузнецов В.А., Исаев Л.К., Шайко И.А. Метрология. М-ФГУП «Стандартинформ», 2005. – 300 с.

3. Шабанов Г.П. Контроль функционирования больших систем. – М.: Машиностроение. 1977. – 204 с

4. Крещук В.В. Метрологическое обеспечение эксплуатации сложных изделий. – М.: Изд-во стандартов, 1989 – 200 с.

5. Карни Ш. Теория цепей. Анализ и синтез: Пер с англ. В.Г. Раутиана / Под ред. С.Е. Лондона – М.: Связь, 1973. – 368 с.

6. Гуревич И.В. Основы расчетов радиотехнических цепей (линейные цепи при гармонических воздействиях). – М.: Связь, 1975. –368 с.

ВЫСОКОЧАСТОТНОЕ НАВЯЗЫВАНИЕ. ПРИНЦИП РЕАЛИЗАЦИИ И МЕТОДЫ ЗАЩИТЫ

Д.Ю. Колесник, А.И. Майоров

Под высокочастотным навязыванием (ВЧ-навязыванием) понимают способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства. Он заключается в модуляции электромагнитного зондирующего сигнала речевым в результате их одновременного воздействия на элементы

обстановки или специально внедренные устройства.

Метод ВЧ-навязывания, несмотря на свою теоретическую привлекательность, на практике сложно осуществим. Подключение ВЧ генератора к проводам, линиям связи и т. п. очень сложен, а, зачастую, невозможен по причине того, что данные линии не выходят за пределы контролируемой зоны. Также недостатками являются малая дальность действия и высокие уровни облучающих сигналов, наносящие вред здоровью людей. Данные обстоятельства существенно снижают ценность ВЧ-навязывания. Однако, в истории известны факты использования данного метода советскими спец. службами, что дает основание утверждать, что угроза утечки информации по данному каналу реальна и для обеспечения сохранности конфиденциальной информации необходимо производить комплексную защиту от ВЧ-навязывания. Некоторые из методов защиты от ВЧ-навязывания приведены ниже.

Осуществление сканирования радиодиапазона на предмет излучения ВЧ-генератора и инструментального контроля излучений на предмет выявления зондирующих ВЧ-сигналов в линиях связи; установка средств активной защиты информации; установка пассивных схем защиты – фильтрация; защита информации от ВЧ-зондирования также может быть реализована за счет создания защищенных объектов методом экранирования помещений.

Таким образом, методы защиты информации от ВЧ-навязывания во многом схожи с методами защиты от утечки информации по другим каналам утечки информации.

Литература

1. Технические средства и методы защиты информации: Учебник для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

2. Лыньков, Л.М. Основы защиты информации и управления интеллектуальной собственностью / Л.М. Лыньков, В. Ф. Голиков, Т. В. Борботько. Минск: БГУИР, 2013. – 243 с.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ ОТ СИГНАЛОВ РЕВЕРБЕРАЦИИ В ПАССИВНОМ ГИДРОЛОКАТОРЕ ПРИ КОГЕРЕНТНОМ НАКОПЛЕНИИ СПЕКТРАЛЬНЫХ СОСТАВЛЯЮЩИХ

Д.Н. Нгуен

С выхода акустоэлектрического преобразователя приемной антенны пассивного гидролокатора в тракт обработки поступает принятый сигнал, включающий полезный сигнал, сигналы реверберации и помехи от различных источников биологического и другого происхождения. Полезным в пассивном гидролокаторе является слабый периодический сигнал, создаваемый гребным винтом морского объекта, а помехи и сигналы реверберации часто являются основными факторами, ограничивающими эффективность работы гидролокатора [1]. Поэтому задача обнаружения и выделения полезного сигнала на фоне помех и сигналов реверберации стала актуальной для пеленгаций, распознавания и пр.

Выделение полезного сигнала на фоне помех может осуществляться по спектру при известной частоте его повторения, которая может быть определена способом когерентного накопления спектральных составляющих [2]. Частота повторения сигналов реверберации совпадает с частотой повторения полезного сигнала, поэтому их спектры похожи. Выделение полезного сигнала на фоне реверберациий может осуществляться во временной области по разнице времени задержки. Полезный сигнал обычно имеет наименьшее время задержки по сравнению с сигналом реверберации. Определение времени задержки затрудняется из-за того, что при распространении в воде полезный сигнал маскирует интенсивными помехами. Однако определение времени задержки полезного сигнала можно более качественно осуществлять при реализации способа когерентного накопления спектральных составляющих.

Литература

1. Ольшевский, В.В. Статистические свойства морской реверберации / В.В. Ольшевский. – М.: Наука, 1966. – 205 с.

2. Гейстер, С.Р. Способ когерентного накопления спектральных составляющих принятого сигнала в пассивном гидролокаторе / С.Р. Гейстер, Д.Н. Нгуен // Наука и военная безопасность. – 2016. – № 3. – С. 36–38.

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ПОЛЬЗОВАТЕЛЬСКИХ СКРИПТОВ ПРИ РАБОТЕ С ВЕБ-САЙТАМИ

М.А. Николенко, И.А. Адуцкевич

Пользовательские скрипты представляют собой написанный на языке JavaScript исполняемый код, подключаемый браузером на страницы веб-сайтов, предназначенный для расширения стандартного функционала браузера. Примечательной особенностью пользовательских скриптов является возможность работать на разных сайтах, несмотря на правило ограничения домена, что способствует возможности нежелательной утечки и распространению информации. В данной работе была исследована безопасность использования пользовательских скриптов на примере разработанного модуля голосового управления веб-сайтами. Модуль представляет собой пользовательский скрипт, позволяющий управлять веб-сайтом при помощи голосовых команд. Его работа заключается в считывании и анализе данных с веб-сайта, определении основных функциональных элемнтов для работы с веб-сайтом, и организацию голосового управления. Для реализации голосового интерфейса были использованы Web Speech API и JavaScript библиотека Pocketsphinx.js.

В ходе исследования работы модуля было обнаружено, что при анализе данных с некоторых веб-сайтов могут возникать утечки информации и личных данных, считывание вредоносного кода и его распространение. Исследование показало, что этот факт находится в прямой взаимосвязи с низким уровнем защиты ряда веб-сайтов в сети Интернет. Чтобы предотвратить утечку и распространние информации был реализован комплекс мер по исправлению критических уязвимостей в пользовательских скриптах, которые включают в себя: валидацию и анализ полученных данных на предмет вредоносного кода, защиту от XSS и CSRF атак. Последующий анализ показал, что шанс утечки пользовательских данных при работе со скриптами существенно снизился.

Литература

1. Microsoft, Developer Network: [Электронный ресурс]. Режим доступа: https://msdn.microsoft.com/ru-ru/library/zdh19h94(v=vs.100).aspx. – Дата доступа: 15.05.2017.

2. Molily.de [Электронный ресурс]. Режим доступа: https://molily.de/xss/. – Дата доступа: 17.05.2017.

КОМПЬЮТЕРНО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ДЛЯ ИЗМЕРЕНИЯ ПАРАМЕТРОВ АФАР

В.Т. Ревин, Н.М. Наумович, А.А. Гавриченко

Исследование амплитудно-фазового распределения активных фазированных антенных решеток (АФАР) представляет собой достаточно трудоемкую задачу, решить которую без автоматизации процессов выделения, сбора, обработки и регистрации измерительной информации практически невозможно. Современные средства измерений – компьютерно-измерительные системы – позволяют решить данную задачу путем реализации голографического метода, который считается одним из наиболее перспективных направлений для исследования характеристик антенн. Суть данного метода заключается в исследовании амплитудно-фазового распределения (АФР) электромагнитного поля вблизи раскрыва тестируемой антенны посредством прецизионного сканирующего зонда.

Механическая часть разработанной компьютерно-измерительной системы представляет собой двух координатное сканирующее устройство в азимутальной (ось X) и угломестной (ось Y) плоскостях. Диапазон сканирования в азимутальной плоскости до 1200 мм, а в углометной – до 700 мм, Погрешность определения координат по осям не превышает 0,1 мм. Скорость сканирования регулируется программно-временным способом и может достигать 50 мм/с.

Измерение амплитудных и фазовых параметров СВЧ сигнала, задаваемого компьютерно-управляемым синтезатором частоты, обеспечивается векторным анализатором цепей в диапазоне частот от 8 до 12 ГГц, динамическом диапазоне от 0 до 70 дБ и диапазоне изменения фазовых сдвигов от 0 до 360° (±180°). При тщательной настройке средств измерений и хорошем качестве радиопоглощающего покрытия погрешность измерения коэффициента усиления амплитудных параметров ±0,2…0,5 дБ; фазовых параметров ± 2°.

Литература

1. Сверхширокополосные измерительные системы [Электронный ресурс]. – Режим доступа: www.trimcom.ru. –Дата доступа: 19.05.2017.

2. Синани А.И. Антенный полигон для измерения.

ПОМЕХОЗАЩИТА РАДИОЛИНИЙ

В.В. Симончик

Основная цель системы радиоэлектронного подавления РЭС - при имеющейся мощности станции помех как можно больше увеличить вероятность ошибки за счет снижения отношения энергии бита к суммарной спектральной плотности мощности помех и собственных шумов. С другой стороны система РЭС старается обеспечить энергетическую и пространственную скрытность работы за счет применения широкополосных сигналов и антенн с малым уровнем боковых лепестков диаграммы направленности антенны. Если известно местоположение станции помех и ее эффективная изотропно излучаемая мощность (ЭИИМ), то для обеспечения помехозащиты РЭС надо воспользоваться уравнением помехозащиты, которое выводится при следующих предположениях [1, 2].

Уравнение помехозащиты в логарифмическом виде будет иметь следующий вид [3]: $P_{c\,\text{пд}} \cdot G_{c\,\text{пд}} = P_{\text{п}\,\text{пд}} \cdot G_{\text{п}\,\text{пд}} + h^2_{\text{пор}} - B + \left(\frac{r_c}{r_a}\right)^2 + \frac{G(\Theta)_{\text{пм}}}{G_{c\,\text{пм}}}$, дБВт, где N_0 – спектральная плотность шумов в нашей системе связи; $G(\Theta)_{\text{пм}}$ – коэффициент усиления антенны приемника СРС в направлении на станцию помех; B – база сигнала; $P_n/P_\text{с}$ – отношение мощности помехи к мощности сигнала; $h^2_{\text{пор}}$ – пороговое значение, при котором обеспечивается работа радиолинии с заданным качеством; $\frac{G(\Theta)_{\text{пм}}}{G_{c\,\text{пм}}}$ – уровень бокового лепестка диаграммы направленности антенны нашей приемной станции; $\left(\frac{r_r}{r_a}\right)^2$ – расстояние между приемником и передатчиком нашей системы связи.

Из уравнения помехозащиты следует, чтобы было легче противостоять помехе надо увеличивать базу сигнала и уменьшать уровень бокового лепестка диаграммы направленности антенны нашей приемной станции ,уменьшать расстояние между приемником и передатчиком нашей системы связи$\left(\frac{r_r}{r_a}\right)^2$, а также за счет применения помехоустойчивого кодирования уменьшать.

Уменьшение расстояния между станциями систем связи приводит к уменьшению мощности передатчика и тем самым понижает перехватывающую мощность разведывательного приемника. Основной стратегией постановщика помех положено как при имеющейся мощности передатчика помех вызвать, или увеличивать вероятность ошибки на бит в нашей системе связи.

Литература

1. Помехозащищенность систем радиосвязи / В.И. Борисов [и др.]. – Москва : Радио и связь, 2003. – 640 с.

2. Помехозащищенность с расширением спектра сигналов методом ППРЧ / В.И. Борисов [и др.]. – Москва: Радио и связь, 2000. – 384 с.

3. Тепляков, И.М. Телекоммуникационные системы / И.М. Тепляков. – Москва: ИП РадиоСофт, 2008.

СПОСОБ ВЫСОКОСКОРОСТНОГО КВАНТОВО-КРИПТОГРАФИЧЕСКОГО ОБМЕНА ИНФОРМАЦИЕЙ С КОНТРОЛЕМ ЕЕ НЕСАНКЦИОНИРОВАННОГО РАСКРЫТИЯ И ЦЕЛОСТНОСТИ

А.М. Тимофеев

При реализации систем криптографической защиты информации одним из наиболее важных этапов является экспорт и импорт критических объектов, в качестве которых могут выступать криптографические ключи, параметры криптографических алгоритмов и пр. Экспорт и импорт таких объектов с использованием телекоммуникационных каналов связи требует защиты объектов для предотвращения их несанкционированного раскрытия и/или модификации, что обеспечивается преимущественно квантово-криптографическими способами, которые, в сравнении с прочими (криптографическими, аппаратными, алгоритмическими и др.), обеспечивают абсолютную защищенность критических объектов [1]. Однако известные квантово-криптографические способы имеют достаточно сложную процедуру согласования базисов, в которых передаются и принимаются символы, что не позволяет выполнять высокоскоростной экспорт и импорт критических объектов по телекоммуникационным каналам связи [1]. В связи с этим целью данной работы являлась разработка высокоскоростного квантово-криптографического способа экспорта и импорта критических объектов по волоконно-оптическим каналам связи. В работе получены выражения для оценки пропускной способности волоконно-оптического канала связи, вероятности ошибки и длительности времени регистрации передаваемых символов. Предложен способ экспорта и импорта критических объектов по волоконно-оптическому каналу связи, позволяющий уменьшить ошибку передачи данных, связанную с деполяризацией оптического излучения, упростить процедуру согласования базисов, в которых переданы и приняты символы, и повысить за счет этого скорость передачи и приема критических объектов.

Литература

1. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]. – Минск, 2007.

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ: ПРОБЛЕМЫ И РЕШЕНИЯ

В.А. Трушин, А.В. Иванов

При оценке защищенности речевой информации от утечки по техническим каналам в качестве показателя защищённости принято использовать коэффициент словесной разборчивости W. Используемая в настоящее время методика определения W [1] основана на формантном методе Покровского Н.Б., который был в свое время разработан прежде всего для оценки качества каналов связи [2], что и обусловило ряд некорректностей в существующем методе, а именно:

– проводимые Покровским Н.Б. артикуляционные испытания с использованием некоррелированных таблиц не отражает реалии задач защиты речевой информации, где присутствуют связные, содержательные тексты;

– не учтена возможность записи переговоров с последующим их многократным прослушиванием;

– разбиение частотного диапазона на октавные полосы не отражают специфику слухового аппарата человека, где анализ речевого сигнала осуществляется по критическим полосам;

– в существующей методике (по сути методике косвенных измерений) совершенно не рассматриваются вопросы погрешности W, что противоречит ФЗ РФ «Об обеспечении единства измерений».

В докладе приводятся результаты исследований, посвященных решению вышеуказанных проблем.

Литература

1. Железняк, В.К. Некоторые методические подходы к оценке эффективности защиты речевой информации / Ю.К. Макаров, А.А. Хорев // Специальная техника. – 2000. – № 4. – С. 39–45.

2. Покровский, Н.Б. Расчет и измерения разборчивости речи / Н.Б. Покровский. – М.: Связьиздат, 1962. –390 с.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ БЕСПРОВОДНОЙ СВЯЗИ МАЛОГО РАДИУСА ДЕЙСТВИЯ

Л.Л. Утин, М.А. Сабериан

В последние годы наблюдается устойчивая тенденция развития технологий беспроводной связи малого радиуса действия (NFC). Технологии ближней бесконтактной связи являются одним из альтернативных решений передачи данных с мобильного телефона к приемному устройству. NFC – технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092.

Достоинствами данной технологии является низкое время установления связи (менее 0,1 с. (для сравнения в технологии Bluetooth данный параметр равен 6 с)), сложность перехвата электромагнитного излучения злоумышленником из-за малого радиуса действия (менее 20 см), простота реализации и ряд других.

Следует отметить, что несмотря на достоинства данной технологии, ей присущи определенные недостатки, которые предлагаются к обсуждению на конференции. Однако, не смотря на достоинства рассматриваемой в докладе технологии ей присущи определенные недостатки, приводящие к следующим угрозам информационной безопасности:

– до настоящего времени существует потенциальная опасность заражения банковской системы вирусами, которая может осуществиться при использовании мобильного телефона в качестве средства по оплате платежей;

– использование средств постановки помех в диапазоне 13,56 МГц приводит к срыву сеансов связи с использованием технологии NFC;

потенциальная возможность утечки персональных данных при осуществлении связи.

Особенности применения средств защиты информации для нейтрализации (уменьшения последствий от реализации угроз) предлагаются к обсуждению в докладе.

СЕКЦИЯ 3
ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

CORPORATE NETWORK SECURITY SIEM-SYSTEM IMPLEMENTED ON ZABBIX SOFTWARE

Al-Baiati Ali Emad, A.S. Shelkov, N.V. Nasonova

Security incidents and events monitoring systems (SIEM) play an important role in enterprise information systems. SIEM systems have one or more log servers that perform log analysis, and one or more database servers that store logs. Regardless of how the SIEM server receives log data (either agentless or agent-based), the server analyzes data from all sources, correlates events among log entries, identifies and prioritizes meaningful events, and initiates response to events, if necessary.

SIEM solutions usually make it possible to protect privacy, integrity, and availability of these logs. For example, communications between agents and SIEM servers usually pass through a reliable TCP protocol in encrypted form. In addition, agents and SIEM servers can use authentication before they can transfer the data (for example, sending data from the agent to the server, making server-side changes in the agent settings).

Zabbix software was studied to implement a SIEM-system for a corporate network. Among many well-known monitoring systems Zabbix monitoring system was chosen for the implementation of SIEM. The capabilities of this system make it possible to use it as a system for collecting information, for its further processing and detecting IS events and logs analyzing in various operating systems, for making a decision on the occurrence of an IS incident, for notification of staff members responsible for the IS system, and for response to the known threats in a preventive manner.

On the basis of the examined information on the Zabbix system and the capabilities of hardware virtualization, a laboratory model was created, on which the network attack and the Zabbix system response to it can be demonstrated. Depending on the hardware resources, the model can be expanded, which makes it a useful tool for the investigation of network attacks, the information system response to network attacks, and the SIEM-system testing on the basis of the Zabbix software.

MODIFIED RLE ALGORITHM FOR SATTILITE IMAGE COMPRESSION

H.K. Albahadily, V.Yu. Tsviatkou

New suggested RLE compression algorithm to compress satellite grayscale images and reduce the size of the encoded data by reducing the bits needed to represent the coded date with bitplane technique. The proposed methods achieved very good compression ratio with satellite large space images of earth. The modified RLE algorithm ISN using the same idea of RLE which counts repeated runs but – instead of reserving fixed size of bytes to save the repeat and runs as pairs – we will send the repeated runs with a value representing how many bits need to save that repeat [1].

So *I* representing the pixel value,*S* representing the variant size of how many bits needed to represent it and *N* is the repeated times. The results were very good as we can see in the table below.

Table of compression ratio for test images layers 8–5

Layer	Img1	Img2	Img3
L8	1.3641	1.5950	1.0902
L7	1.2788	1.3636	0.8284
L6	0.9224	1.0950	0.5899
L5	0.6123	0.6591	0.4933

The results showing that the modified algorithm ISN provides compression ratio up to 1.595 times for MSB layer according to the nature of the image and its bitplanes.

References

1. New modified RLE algorithms to compress grayscale images with lossy and lossless compression / H. Albahadily [et al.] // International Journal of Advanced Computer Science and Applications. – 2016. – Vol. 7, № 7.

SOFTWARE SOLUTION FOR VULNERABILITY DETECTION

Qahtan Hussein, Momoh Angelo, A.I. Bukshtynova

Web Application Architecture can be of various types. Web applications have been developed on the basis of improvement and complication of web-node functions. Web application extends functions of a web-node by making it possible for its clients to use business logic and hence to modify the data on the server. This definition of web applications specifies that it consists of at least three important architectural components: a client browser, a web server, and an applications server.

Often a web application also uses a database server. A more rigorous definition of a web application can be as follows: a client/server software system, comprising of at least the following architectural components: HTML/XML browser on one or more client computers, communicating with the web server through the HTTP protocol, and the applications server which manages the business logic.

To detect vulnerabilities in web applications, there are many methods, such as the penetration testing method, the source code analysis of the application. The penetration testing method is the most accessible, since it only requires access to the web application. And such access is available to all users, if the application is accessible from the Internet.

These methods include the following steps: passive information gathering; definition of the web environment and platform; port scanning / collection of service banners; automatic scanning; definition of «weak points» of the resource; manual analysis; collection and analysis of information received; analysis of attack vectors; confirmation of received vectors; compilation of a report.

To implement the software solution, the Python programming language was chosen. This choice is conditioned by the fact that all operating systems support this language and there are a great number of libraries to use. The software solution involves the library for the work with networks and sub networks of IPv4 (netaddr) protocol, the library for the processing of HTML-markup which helps to extract data (bs4), and the library for asynchronous processing of web-services (gevent), which helps to speed up the software performance through the concurrent execution of commands not sequential.

The program complex functions on following algorithm. On a program input the information on a target network moves. These data can be presented in the form of the domain of the second level, a network of IPv4 addresses, the list of domains of the third level, the list of IPv4 addresses. Depending on the data submitted on an input the file networkscanner forms the list of not repeating addresses. The list is transferred to a file portscanner.py which on an exit returns data about open ports and the office information on network sites and transfers these given to a file report.py. The file report.py processes the received results and deduces to their user.

СИМБИОЗ SIEM И DLP

Т.А. Андриянова, С.Б. Саломатин

В настоящее время одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных от несанкционированных действий сотрудников. Согласно исследованиям за прошлый год, в более чем 80 % случаев утечка информации в компаниях происходила по вине (или неосторожности) именно внутреннего нарушителя. Таким образом, DLP технологии становятся неотъемлемой и обязательной частью корпоративных систем информационной безопасности, существенно повышая уровень защиты конфиденциальных данных. Это обусловлено еще и тем, что большая часть традиционных средств защиты, таких как антивирусы, межсетевые экраны и системы аутентификации не способны обеспечить эффективную защиту от внутренних нарушителей.

Одним из наиболее перспективных вариантов расширения функционала DLP систем является интеграция с SIEM технологией. В симбиозе системы взаимно дополняют друг друга. Компоненты DLP-системы осуществляют поиск и классификацию защищаемой информации по установленным критериям. А SIEM формирует «единое окно» для администратора безопасности, в котором сводятся данные о выявленных файлах, подлежащих защите, попытках доступа к ним, а также коррелируется технологическая информация, поступающая от ОС, СУБД, сетевого оборудования и других источников, формируя полную картину состояния информационной безопасности в организации.

Симбиоз SIEM и DLP многократно повышает уровень информационной защиты организации и упрощает работу службе безопасности.

Литература

1. Исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] – Режим доступа: https://www.infowatch.ru/analytics. – Дата доступа: 19.05.2017.

АНАЛИЗ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОГРАММНЫХ ПРОДУКТАХ ДЛЯ ПОЛИКЛИНИК

Е.Д. Антонов, И.С. Гречко, Ю.Ю. Григорьева

Развитие компьютеризации здравоохранения [1] в Беларуси в последние годы может заметить каждый белорус, и в первую очередь, в своей поликлинике. Программные продукты (ПП) для белорусских поликлиник (ПП для поликлиник, ППдМ) разрабатывают в основном 3 минских организации: частное ЗАО «Мапсофт» [1], Белорусский центр медицинских технологий и информатизации (БелЦМТ) [3] и Объединенный институт проблем информатики (ОИПИ) [4] АН РБ. При этом доля минских поликлиник, компьютеризированных каждой организацией, имеет примерно следующий вид: «Мапсофт» – 35 %, БелЦМТ – 25 %, ОИПИ и другие – 40 %. Все ППдМ имеют примерно одинаковую структуру и решают примерно одинаковый круг задач – автоматизация деятельности врача, автоматизация структурных подразделений поликлиники (бухгалтерия, снабжение, статистика и др.).

Однако защита персональных данных пациентов в ППдМ всех разработчиков находится на уровне разграничения прав доступа к данным и контроля за доступом путем анализа логов. В условиях наличия в каждой минской поликлинике неавтоматизированной регистратуры, где хранятся бумажные амбулаторные карты пациентов, вышеописанная защита теряет смысл: зачем злоумышленнику преодолевать сложности доступа к электронным данным, когда проще получить эти данные у низкооплачиваемого работника регистратуры поликлиники. В этих условиях надежная защита персональных данных пациентов в ППдМ будет реализована только после внедрения организационных мероприятий по компьютеризации существующих в поликлиниках регистратур с бумажными амбулаторными картами пациентов.

Литература

1. Демидов, А.В. Информатизация организаций здравоохранения Республики Беларусь // Вопросы организации и информатизации здравоохранения / А.В. Демидов. – 2014. – № 3. – С. 20–25.

2. «МАПСОФТ» – разработка, внедрение и обслуживание ПО [Электронный ресурс]. – Режим доступа: www.mapsoft.by/of AWG-based WDM-PON Architecture with Multicast Capability. – Дата доступа: 19.05.2017.

3. БелЦМТ [Электронный ресурс]. – Режим доступа: www.belcmt.by/. – Дата доступа: 19.05.2017.

4. Объединенный институт проблем информатики[Электронный ресурс]. – Режим доступа: uiip.bas-net.by/. – Дата доступа: 19.05.2017.

МЕТОДИКА КАТЕГОРИЗАЦИИ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БД НА ОСНОВЕ АЛГОРИТМА КЛАСТЕРНОГО АНАЛИЗА SOM

Э.В. Артемьев

Понимание характера уязвимостей информационной безопасности имеет решающее значение для анализа угроз, которые они представляют. В значительной мере это касается таких информационных систем, как базы данных (БД), которые имеют ряд характерных особенностей, свойственных хранилищам данных: двойственная природа систем управления базами данных (СУБД), зависимость уязвимостей и механизмов управления от данных и описывающей их организацию модели, угрозы логического вывода, различная значимость сочетаний данных. Все это определяет специфический характер уязвимостей информационной безопасности БД. Поэтому для повышения эффективности защиты при выборе методов

обеспечения безопасности БД необходимо учитывать указанные особенности.

В настоящий момент существует необходимость в адекватной категоризации уязвимостей БД, принимая во внимание их своеобразие. Применение международного стандарта классификации уязвимостей CVE (Common Vulnerabilities and Exposures) [1], обеспечивает средства для однозначного именования общеизвестных уязвимостей, но при этом не стандартизируются категории уязвимостей, связанных с БД.

Выбор методики кластеризации данных для интеллектуального классифицирования уязвимостей БД обусловлен тем, что кластеризация данных – это способ, применяемый для формирования кластеров объектов, которые имеют похожие признаки. Для таких объектов внутриклассовое подобие максимально, а межклассовое сходство сводится к минимуму, что идеально подходит для категорий уязвимостей. Еще одно преимущество использования кластеризации данных по категориям уязвимостей заключается в том, что требуются минимальные предшествующие знания и предположения. Поэтому целесообразным представляется применение алгоритма кластеризации SOM (Self-organizing map) [2] для категоризации уязвимостей БД. Преимуществом использования SOM в данной методике является возможность получать скрытые сведения из входного набора данных, а также в наглядной визуализации и интерпретации результатов. Категоризация уязвимостей БД с помощью SOM позволит более качественно ранжировать угрозы безопасности БД с целью своевременного реагирования на наиболее критичные из них.

Литература

1. Common Vulnerabilities and Exposures (CVE) [Электронный ресурс]. – Режим доступа http://cve.mitre.org/. Дата доступа 05.02.2017.

2. Kohonen, T.**,** Self-Organizing Maps, Second Edition, Berlin: Springer-Verlag, 1997.

ПРИМЕНЕНИЕ РОЕВЫХ АЛГОРИТМОВ К РЕШЕНИЮ ЗАДАЧ КРИПТОЛОГИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

А.И. Бобров

В настоящее время известны применения генетических алгоритмов для оптимизации широкого круга задач, в том числе задач криптоанализа. Различными авторами рассматривались методы организации криптографических атак на традиционные симметричные криптосистемы, использующие шифры перестановки и замены, а также на блочные криптосистемы с использованием методов эволюционной оптимизации и генетического поиска. Недостатком генетических алгоритмов является наличие слепого поиска. В общем случае это приводит к генерации решений с нарушениями и тем самым увеличивает время поиска и требует дополнительного контроля, генерации большого количества одинаковых решений, генерации большого количества плохо приспособленных решений, что может привести к попаданию в локальный оптимум. Поэтому представляют интерес эвристические методы, инспирированные природными системами, в которых осуществляется поэтапное построение решения задачи (то есть добавление нового оптимального частичного решения к уже построенному частичному оптимальному решению).

К таким методам относят и муравьиные алгоритмы, моделирующие поведение колонии муравьев, связанное с их способностью быстро находить кратчайший путь от муравейника к источнику пищи. Колония муравьев рассматривается как многоагентная система, в которой каждый муравей-агент действует автономно на основе простых правил.

Задача поиска алгоритма муравьиных колоний в общем случае заключается в определении позиций для символов из алфавита ключа таким образом, что целевая функция, определяющая оптимальность шифртекста (при заданном открытом тексте) при реализации алгоритма шифрования или оптимальность открытого текста (при заданном шифртексте) при реализации алгоритма криптоанализа, достигает экстремума. Данная задача – частный случай квадратичной задачи о назначениях, традиционно являющейся тестовой задачей для оценки эффективности методов поиска. Метод, построенный на муравьином алгоритме, подходит для расшировки малых и средних текстов, а также может применятся при комплексных методах криптоанализа, в качестве предварительной прогонки перед основных ходом метода.

МОДУЛЬ ВНЕДРЕНИЯ ИНФОРМАЦИИ В ЗВУКОВЫЕ ФАЙЛЫ В ФОРМАТЕ MP3 НА ОСНОВЕ МЕТОДА ФАЗОВОГО КОДИРОВАНИЯ

Е.В. Бондарчук, И.А. Мурашко

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Существуют два основных направления в компьютерной стеганографии. Первое направление основано на цифровой обработке сигналов. Второе использует иные принципы.

Метод фазового кодирования, предлагающий использовать слабую чувствительность системы слуха человека к незначительным изменениям фазы сигнала, был предложен В. Бендером, Н. Моримото и др. Основная идея метода – фаза начального сегмента аудиосигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз. Это объясняется тем, что к разности фаз человеческое ухо более чувствительно. Фазовое кодирование, когда оно может быть применено, является одним из наиболее эффективных способов кодирования по критерию отношения сигнал-шум [1].

Фазовое кодирование включает в себя следующие шаги:

– разделяется оригинальный звуковой сигнал на более мелкие сегменты таким образом, чтобы их общая длина была равна длине сообщения;

– с помощью дискретного преобразования Фурье создается матрица фаз;

– вычисляется разность фаз между соседними сегментами;

– секретное сообщение встраивается только в фазу первого сегмента;

– с учетом разности фаз создается новая матрица фаз, используя новую фазу первого сегмента;

– звуковой сигнал восстанавливается путем применения обратного дискретного преобразования Фурье с использованием новой матрицы и исходной матрицы величин, после чего звуковые сегменты сцепляются.

Чтобы извлечь секретное сообщение из звукового файла получатель должен знать длину сегмента. После чего получатель с помощью дискретного преобразования Фурье может извлечь секретную информацию [2].

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М.: СОЛОН-ПРЕСС, 2009. – 265 с.

2. Нигматулин, Э.В. Обзор методов цифровой аудиостеганографии / Нигматуллин Э.В., Ковырзина К.С. // Электронный сборник статей по материалам XLII студенческой международной научно-практической конференции. Новосибирск, 31 мая 2016 г.: изд. АНС «СибАК». – 2016. – № 5 (41). – Новосибирск, 2016. – С. 118–124.

СТЕГАНОГРАФИЧЕСКОЕ ВСТРАИВАНИЕ СЛУЖЕБНОЙ ИНФОРМАЦИИ В КАРТОГРАФИЧЕСКИЕ ИЗОБРАЖЕНИЯ

Ю.В. Борохова

Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации. Задачу встраивания и выделения сообщений из другой информации выполняет стеганографическая система. Основными объектами стеганографии являются: контейнер – любая информация, предназначенная для сокрытия тайных сообщений; сообщение – это термин, используемый для общего названия передаваемой скрытой информации; стеганографический канал – канал передачи стегоконтейнера; ключ – секретный ключ, необходимый для сокрытия информации.

Картография – наука об исследовании, моделировании и отображении пространственного расположения, сочетания и взаимосвязи объектов, явлений природы и общества. В настоящее время картографическое производство опирается на материалы космических снимков.

Спутниковые изображения находят применение во многих отраслях деятельности – сельском хозяйстве, геологических и гидрологических исследованиях, лесоводстве, охране

окружающей среды, планировке территорий, образовательных, разведывательных и военных целях. На спутниковых снимках отсутствуют знаки и обозначения объектов, поэтому есть необходимость в размещении на них служебной информации.

Использование стеганографических возможностей встраивания информации в картографические изображения позволит упростить работу с данными об определенном объекте исследования. Данные об объекте можно хранить непосредственно в самом изображении. При встраивании, исходное изображение можно разделить на слои и в каждый слой встроить определенную информацию. В этом случае, при извлечении некоторой информации, необходимости извлекать все, не будет.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: СОЛОН-Пресс, 2002.

2. Как карты передают географическую информацию [Электронный ресурс]/ArcGIS Recourses – 2010. – Режим доступа: http://resources.arcgis.com/ru/help/getting-started/articles/026n0000000q000000.htm.

УГРОЗЫ ТЕХНОЛОГИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

С.Ю. Вашкевич, А.Е. Мишустина, Е.Е. Гачко, Т.С. Аубакирова

Особенностью развития современной сферы разработки мобильных и встроенных приложений становится использование наиболее перспективных технологий, из которых особо можно выделить технологию дополненной реальности (AR, augmented reality). Анализ рынка показал, что приложения, использующие AR-технологии, становятся популярны не только в сфере развлечений, но и получают множество вариантов практического применения.

При оценке рисков дополненной реальности в первую очередь обращают внимание на отвлекающие факторы. К примеру, слишком большое количество информации, находящейся в поле зрения водителя, может привести к фатальным последствиям. Менее вероятна угроза проникновения в системы дополненной реальности хакеров с последующим вторжением в частную жизнь, похищением цифровых данных и рисками физической безопасности. Можно подменить выходную информацию AR-систем, заставляя пользователя поверить, что сгенерированные компьютером объекты (например, поддельные дорожные знаки) реальны. Противоположный сценарий: так как приложениям дополненной реальности нужен доступ к реальным данным, собранным при помощи различных датчиков, вредоносные приложения могут похищать информацию о наблюдаемых объектах и местоположении пользователя.

В отчете 2016 Emerging Technology Domains Risk Survey [1] дополненная реальность названа одной из десяти технологических областей, которые в случае взлома могут привести к серьезным сбоям (в сфере безопасности, конфиденциальности, финансовой или операционной). Классические методы и средства повышения безопасности (например, шифрование данных, передаваемых по беспроводным каналам) позволяют защитить входные и выходные данные приложений. Но для этого необходимо иметь четкое представление об интеграции средств безопасности в сферу дополненной реальности.

Литература

1. 2016 Emerging Technology Domains Risk Survey [Электронный ресурс] / Software Engineering Institute. Carnegie Mellon Institute. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf. – Дата доступа: 18.05.2017.

ИСПОЛЬЗОВАНИЕ ВЕКТОРНОЙ ГРАФИКИ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ WEB-СИСТЕМ

О.Н. Виничук

Цифровое изображение – графическая форма представления данных, предназначенная для зрительного восприятия. Будучи закодированным с помощью особого алгоритма и записанным на носитель, этот массив данных становится файлом, который зачастую имеет достаточно большой размер. В современном процессе полиграфического производства все

иллюстрации и элементы оформления представлены цифровыми изображениями различных типов. Основной гипотезой, положенной в основу данной статьи, является возможность преобразования изображения в svg формат для возможности масштабирования изображения до любого размера без потери качества, возможность сокращения размера файла путем сжатия и обработки изображения. SVG-изображение – это набор графических операторов, описывающих формирование простых графических элементов, таких, как векторы, многоугольники, окружности, дуги. При выводе на матричные устройства векторная графика предварительно преобразуется в растровую графику, преобразование производится программными или аппаратными средствами современных видеокарт.Важным моментом является тот факт, что в браузере SVG-графика отрисовывается с помощью растровых механизмов. Поддержка полупрозрачностей в каждом слое, градиенты линейные, градиенты радиальные, визуальные эффекты (тени, отмывки, блестящие поверхности, текстуры, паттерны любой конструкции, символы любой сложности).

Избыточность данных является центральным понятием цифрового сжатия данных. Плюсом векторных изображений SVG является сравнительно небольшой размер файлов, их содержащих. Это делает удобной передачу векторных изображений по электронным каналам связи. Особое распространение векторные изображения получили в рекламной продукции благодаря возможности качественного полиграфического воспроизведения четких линий, ярких цветов, ровных заливок и геометрически правильных контуров. Использование SVG значительно упрощает реализацию деловой графики и делает вывод любой графической информации строгим и структурированным.

Литература

1. Электронный научный журнал «Медиаскоп» [Электронный ресурс] / Электронный научный журнал «Медиаскоп» – Режим доступа - http://www.mediascope.ru. – Дата доступа: 28.02.2017.

ВОПРОСЫ ПРИМЕНЕНИЯ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ

Г.А. Власова, Н.А. Козырев

Стремительное развитие Интернета и внедрение интернет-технологий во все сферы жизнедеятельности человека привело к появлению так называемого Интернета Вещей (Internet of Things, IoT). В настоящее время более 99% всех изготовленных микропроцессоров используется во встроенных системах и менее 1% - в традиционных компьютерах. IoT рассматривается комиссиями Европарламента и Совета Европы как основной путь развития информационных и интернет-технологий [1]. Подключение к сети Интернет десятков миллиардов новых устройств, которые ранее не рассматривались в качестве информационных, формирует новые требования к информационной безопасности, в том числе к криптографическим методам защиты.

Массовый характер применения и небольшие потоки передаваемых данных привели к необходимости использования алгоритмов малоресурсной или «легковесной криптографии» (lightweight cryptography, LWC) для реализации в устройствах, имеющих ограниченные вычислительные возможности. Как правило, к реализации малоресурсной криптографии предъявляются следующие требования: низкая потребляемая энергия; малые размеры микросхемы; обработка небольших потоков информации с приемлемым быстродействием; дешевизна устройств. При этом в отличие от объемов требуемых ресурсов, криптостойкость должна снижаться незначительно. Однако легко реализовать любые две из трех целей разработки: безопасность и экономичность, безопасность и производительность или стоимость и производительность, но очень трудно оптимизировать все три цели такой разработки одновременно [1]. Так, безопасность и высокое быстродействие можно реализовать параллельными методами вычислений, но при этом увеличивается стоимость устройства. Увеличение времени обработки позволяет, обеспечив требуемую криптостойкость, уменьшить размеры микросхемы, снижая соответственно производительность устройства. Увеличение криптостойкости за счет увеличения длины ключа приводит к уменьшению экономичности и быстродействия устройства. Таким образом, разработка устройств, реализующих алгоритмы

малоресурсной криптографии для каждого приложения с учетом заданных требований, представляет собой сложную многопараметрическую задачу.

Задачей для исследований является также допустимый уровень снижения безопасности при реализации «легковесной криптографии». Так в [1, 2] предлагается использовать симметричные алгоритмы с длиной ключа 80 и 128 бит. Однако без смены ключа сегодня данные алгоритмы уже не могут считаться криптостойкими.

Литература

1. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. Вып. № 1 (9), С. 26–43.

2. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. Вып. № 2 (10). С. 2–10.

СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЦЕНТРАЛИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМАХ

П.Л. Волынец

В последние годы бурное развитие информационных технологий, появление новых способов передачи информации, увеличение объемов и скорости передаваемой информации привело к необходимости смены действующих децентрализованных банковских систем на более современные централизованные комплексы. Централизация системы позволяет быстрее производить расчеты, выполнять клиентские операции и вести мониторинг своего бизнеса, сокращая издержки на сопровождение и развитие многих систем одновременно.

Система на основе решений от компании SAP позволяет решать огромный спектр задач с ведение единой базы, с возможностью интеграции с другими система по различным каналам, имеет гибкую систему настроек и возможность самостоятельного создания необходимых программ для конкретной организации.

Однако при расширении функциональности собственными разработками внутри системы появляются проблемы с мониторингом работы пользователей в системе стандартными средствами для выявления ошибок и противоправных действий. Также появляются проблемы с ограничениями прав доступа к собственным разработкам стандартными средствами. Появляется также необходимость внедрения собственных расширений в стандартные программы для изменения работы базовых программ для определенных бизнес процессов.

Для решения данных проблем были разработаны методы ведения журналов и информирования пользователей, реализованы методы проверки полномочий в собственных разработках и расширениях стандартных программ, реализуются и совершенствуются методы анализа программного кода на возможные уязвимости и ошибки, анализ противоречий в ролях доступа у пользователей, анализ тривиальности паролей у системных пользователей.

Переход к централизованным решениям благоприятно сказывается на скорости работы системе, едином ведении всей необходимой отчетности и позволяет контролировать все процессы в системе в любое время в реальном времени.

Литература

1. Андерсон Дж. Лучшие практики внедрения SAP. 2011

2. Danielle Larocca Signoril. SAP Query Reporting

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЦИФРОВЫХ СИСТЕМ СЛЕЖЕНИЯ ЗА ЗАДЕРЖКОЙ ПСЕВДОСЛУЧАЙНОГО СИГНАЛА С ИНВЕРСНОЙ МОДУЛЯЦИЕЙ

С.А. Ганкевич

Среди систем слежения за задержкой псевдослучайного сигнала с инверсной модуляцией наиболее известны системы со снятием модуляции на входе путем суммирования по модулю два входной последовательности с ее копией, задержанной на длительность элементарной посылки, и системы с обратной связью по решению.

Снятие модуляции приводит к удвоению одиночных ошибок и искажению одной элементарной посылки при инвертировании, что снижает показатели качества за счет уменьшения коэффициента усиления в контуре и увеличения флюктуационной составляющей.

Использование обратной связи по решению требует задержки последовательности на входе системы на длительность символа, что, как правило, не приемлемо при большой длительности символа. Однако задержку можно исключить при использовании текущей оценки решения, которая на начальном этапе при низком отношении сигнал/шум имеет значительную вероятность ошибки, существенно снижаемую с течением времени приема символа.

Результаты имитационного моделирования схемы [1], дополненной сумматором по модулю два и элементом задержки, и схемы [1], дополненной обратной связью по решению в виде коррелятора с пороговым устройством, реализующих вышеописанные методы, представлены в виде переходных характеристик и временных зависимостей ошибок слежения для различных отношений сигнал/ шум и первоначальных частотных расстроек. Так, при эталонном сигнале с базой 127 на входе, модулированным сигналом типа «меандр», и отношением сигнал /шум 0 дБ система с обратной связью по решению имеет более высокие показатели по быстродействию и динамической ошибке в 1,4 раза; по величине флюктуационной ошибки системы равноценны.

Литература

1. Ганкевич, С.А. Имитационное моделирование цифровой системы слежения за задержкой псевдослучайного сигнала / С.А. Ганкевич // Современные средства связи : материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск. – С.78–80.

ИНЪЕКЦИИ ВРЕДОНОСНОГО КОДА В ВЕБ-ПРИЛОЖЕНИИ ДЛЯ УДАЛЕННОГО РЕЗЕРВИРОВАНИЯ РАБОЧИХ МЕСТ И ПОМЕЩЕНИЙ

Д.О. Гейман

Рассматривается информационная безопасность нового программного продукта – веб-приложения, которое позволяет управлять местами для совместной работы, такие как конференц-залы, залы для видеоконференций и проектные помещения. Оно позволит сотрудникам офисных компаний управлять общими помещениями используемых для проведения собраний и совещаний: осуществлять мгновенный поиск свободных мест и оборудования; просмотр календаря занятости помещений и сотрудников; резервирование мест проведений, оборудования, питания и добавление участников совещания. Помимо этого, приложение позволит организовать рабочие места для сотрудников, которые находятся в офисе не каждый день. Они смогут резервировать рабочие места только на то время, на которое им необходимо, что позволяет значительно сократить количество рабочих мест. Веб-приложение используется множеством различных организаций, распределенных по всему миру. Организации получают доступ к приложению через один общедоступный портал в интернете. Данные разных организаций должны быть отделены друг от друга, поэтому безопасность информации стоит в приоритете.

Проведенная опытная эксплуатация веб-приложения показала, что одной из уязвимостей его являются инъекции вредоносного кода в программу. В течение опытной эксплуатации были отмечены инциденты, вызванные уязвимостями вида межсайтовый скриптинг – XSS (атака на пользователя, направленная на выполнение в его браузере произвольного сценария, т. е. внедрение вредоносного JavaScript-кода на страницу атакуемого веб-приложения. Инцидентов, вызванных другими уязвимостями, присущими веб-приложениям, (например, выявляемых при ведении CRLF-атак на приложение (техник модификации HTTP-заголовков запроса, атак HTTP Response Splitting, XXE (XMLexternalEntity) атак, CSRF (Cross Site Request Forgery), межсайтовой подделки запросов) обнаружено не было. В докладе рассматриваются новые фрагменты программного кода веб-приложения, разработанные для отражения XSS атак.

ВЫБОР ПОЛЬЗОВАТЕЛЕМ БИОМЕТРИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ ДОСТУПА

А.А. Гивойно, Ю.Ю. Григорьева, И.А. Сеглюк, М.Ю. Ситник, Е.Ю. Нарижный

В настоящее время защита данных проводится в основном с помощью разрешения на доступ к ним, в том числе и по биометрическим параметрам. Общепринято считать, что разрешение доступа к данным по биометрическим параметрам может осуществляться на основе распознавания а) отпечатков пальцев; б) радужной оболочки глаза (РОГ); в) лица; г) геометрии руки; д) голоса; е) сетчатки глаза; ж) ряда дополнительных биометрических параметров (по ДНК, по термограммам, по запаху тела и т. д.) [1]. Из-за множества вариантов средств доступа перед собственником данных возникает задача их выбора.

Для решения этой задачи в докладе предлагается следующая последовательность шагов.

1. Определить несколько вариантов предпочтительных средств доступа (авторизационных систем, АС).
2. Выбрать набор технико-экономических показателей сравниваемых друг с другом АС.
3. Каждый выбранный показатель представить в виде балльной шкалы (чем предпочтительнее АС, тем выше балл), например, для показателя «цена АС»: 25 000 $ – 7 баллов, 26 000 $ – 5 баллов, 27 000 $ – 3 балла.
4. Выбрать весовые коэффициенты каждого показателя так, чтобы сумма их равнялась единице.
5. Рассчитать критерий выбора АС как скалярное произведение вектора выбранных показателей и вектора весовых коэффициентов (чем предпочтительнее АС, тем выше критерий).

Предлагаемая последовательность шагов иллюстрируется двумя примерами: сравнением друг с другом и последующим выбором двух средств контроля доступа по РОГ и двух средств контроля доступа по отпечатку пальца.

Литература

1. Прудник, А.М. Биометрические методы защиты информации / А.М. Прудник, Г.А. Власова, Я.В. Рощупкин. Минск: БГУИР, 2014. – 150 с.

СИСТЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ДЛЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ

И.В. Голубович

На сегодняшний день, благодаря бурному развитию технологий электронной обработки данных, биометрические технологии находят применение не только в криминалистике, но и в иных областях. К таким областям можно отнести информационную безопасность, защиту в банковских технологиях, системы управления доступом, системы учета рабочего времени и регистрации посетителей и др.

Основной целью удостоверения личности с целью аутентификации пользователя для учета рабочего времени является уникальная идентификация личности. Биометрические системы, базирующиеся на физиологических параметрах, значительно надежнее систем, основывающихся на характерных чертах поведения. В биометрии используются признаки присущие каждому человеку, такие как: папиллярный узор пальца, форма кисти руки, узор радужной оболочки глаза, параметры голоса, черты лица, термограмма лица, схема кровеносных сосудов, форма и способ подписи, фрагменты генетического кода и др.

Биометрическая идентификация это также и дополнительный уровень защиты, так как биометрические данные сложно подделать. Одним из достоинств подобных данных является то, что биометрические данные неизменны и уникальны для каждого человека. Основным преимуществом биометрической аутентификации является то, что подобные данные невозможно забыть, потерять, передать другому человеку, украсть или воспроизвести в полном объеме.

Для реализации подобных биометрических систем часто используется такая биометрическая характеристика как отпечаток пальца, так как она обладает наиболее высокими экспертными оценками свойств среди биометрических характеристик человека. Самым

быстродействующим и простым в реализации методом аутентификации по отпечатку пальца является сравнение по особым точкам. Существуют проверенные временем алгоритмы, реализующие данную процедуру аутентификации, однако, необходимость в разработке и реализации новых алгоритмов с лучшими характеристиками не отпадает и на сегодняшний день.

Литература

1. Stan Z. Li Anil K. Jain, Encyclopedia of Biometrics. Second edition, Springer, 2009.

2. Maltoni D., Maio D., Jain A.K., Prabhakar S., Handbook of Fingerprint Recognition, Springer, 2003.

ИССЛЕДОВАНИЕ И ПРИМЕНЕНИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Выбрана конструкция функция безопасности для MVC 5, которая основана на средствах Owin − промежуточного программного обеспечения аутентификации. В процессе исследований аутентификации использовалась система мобильных приложений для банка Последовательность для входа в систему приложений следующая: 1. Пользователь регистрировался в системе ibank24.ir. 2. После регистрации по электронной почте он получает экаунт активизации, в котором содержался ключ активизации мобильных приложений. 3. Пользователь загружает сайт Android app. 4. Для работы используется: имя, пароль и ключ активизации. 5. Ключ запрашивается системой для входа в облачную среду. 6. Меню и ключ вводится пользователем.

Представлена структура программной системы аутентификации в ИКИС для работы сотрудников с мобильными приложениями в реальной системе защиты информации банка. Проведены исследования модели и алгоритмов аутентификации пользователей мобильных приложений в облачной среде, результаты которых показали их эффективность при работе в системе защиты информации банка.

Разработанные модели и средства аутентификации пользователей мобильных приложений использованы в учебном процессе кафедры ИТ Минского инновационного университета для улучшения изучения дисциплины «Основы защиты информации» студентами специальности ПОИТ, а также при выполнении НИР «Модели и средства информационного управления и электронного маркетинга предприятия».

КОМПОНЕНТЫ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Активное развитие мобильных технологий ставит перед организациями вопрос аутентификации в корпоративной сети с облачными вычислениями. Простой и достаточно надежный метод аутентификации – это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться специальными программами, дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).

Усиленная аутентификация, в том числе с использованием дополнительных факторов, должна происходить на компьютере и мобильном устройстве, иначе мобильность будет слабым звеном в контуре безопасности организации. При этом меры обеспечения ИБ не должны создавать неудобства для пользователей. Одной из современных тенденций в области аутентификации является использование SSO (Single Sign-On). Идея этой технологии

заключается в обеспечении единой аутентификации для всех информационных систем организации, которые с точки зрения доступа являются разнородными и никак не интегрированы между. Вместо ввода логина и пароля для каждого приложения достаточно один раз пройти аутентификацию, например, при входе в домен. В докладе раскрывается особенности к реализации SSO-технологии.

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ RFID

Р.А. Жерносеков, В.Т. Першин

Основная цель использования технологии радиочастотной идентификации (Radio Frequency Identification, RFID) заключается в обеспечении в режиме реального времени бесконтактного и точного сбора и обработки данных по учету расположения и перемещения товарных изделий в складских условиях, реализуемых в компьютерных и телекоммуникационных сетях. Сегодня RFID-технология пока не получила широкого распространения в Республике Беларусь. Основной причиной, тормозящей ее развитие, является стоимость программно-аппаратного оборудования. Цена необходимого для реализации RFID технологии сопоставима со стоимостью оборудования, применяемого в обычной системе управления складом (Warehouse Management System, WMS). Однако, стоимость расходных материалов, а именно RFID-меток, остается несравнимо выше. Например, стоимость этикеток штрих-кода для одной метки колеблется в пределах 0,5–10 долл. Исследованию подвергалась технология RFID с маркировкой всех товаров, а также ячеек стеллажей и зон склада. Сигналы меток считывались автоматически или в ручном режиме дистанционно. Физический контакт метки и считывающего устройства при этом не требовался. RFID – это технология автоматического ввода данных, состоящая из компактных радиометок, использующихся в качестве носителей информации и стационарных или мобильных считывателей. Метки прикрепляются к идентифицируемым объектам или встраиваются в них. Считыватели могут устанавливаться в местах, где производится ввод данных, или применяться в качестве мобильных устройств. Технология RFID используется для маркировки, идентификации и отслеживания товаров в процессе их движения от производителя по цепочке поставок в руки покупателя или потребителя. Технология радиочастотной идентификации в Республике Беларусь только формируется, но она имеет хороший потенциал, поскольку экономика нашей страны интегрируется с экономикой России, а в России уже работают, по крайней мере, два завода по производству RFID идентификаторов.

ИССЛЕДОВАНИЕ УСТРОЙСТВА СЧИТЫВАНИЯ ИНФОРМАЦИИ В RFID СТАНДАРТА EM-MARINE

Р.А. Жерносеков, В.Т. Першин

Сообщаются результаты теоретического и экспериментального исследования устройства считывания бесконтактным способом уникального кода, записанного в RFID карты, другие метки стандарта EM-Marine. Показано, что данный считыватель может применяться во всех программных приложениях, используемых в компьютерных и телекоммуникационных сетях, требующих ввода пароля для проверки полномочий или проверки права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними. Это могут быть дисконтные системы в сфере продаж товаров и услуг, системы учета, контроля доступа, контроля рабочего времени, как в локальных, так и в более развитых компьютерных и телекоммуникационных сетях. Анализируемое устройство может использоваться при парольной защите всего компьютера, например, устанавливаемой в BIOS. Уникальный код, прочитанный из RFID-метки стандарта EM-Marine, представляет собой 40 бит двоичной информации. Для передачи в компьютер эта информация преобразуется в последовательность символов. Единого стандарта для такого преобразования не существует. Поэтому, в различных программах формат посылки кода, ожидаемый от считывателя, может отличаться. Эмулируя ввод на клавиатуре компьютера в виде цифровых символов, этот набор передается в компьютер в виде сигнала на рабочей частоте 125 кГц с использованием амплитудной манипуляции. Все настраиваемые параметры считывателя запоминаются в его энергонезависимой памяти, т.е. сохраняются при выключении питания и при подключении

считывателя к другому компьютеру. Это позволяет произвести настройку или конфигурирование считывателя на одном компьютере, а эксплуатировать – на другом компьютере. Используемое программно-аппаратное оборудование соответствовало основному действующему стандарту ISO/IEC 18000-2:2009. Дистанция регистрации обычно составляла 10 ~ 50 мм. Оборудование близкого чтения недорого, но сами метки являются относительно дорогими и без перспектив удешевления из-за конструктивных особенностей их изготовления.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНЫХ СТРУКТУР ПРИ РАБОТЕ С БОЛЬШИМИ ОБЪЕМАМИ ДАННЫХ

И.Е. Закревский

Операции над большими массивами данных являются неотъемлемой частью ежедневной работы. Растут базы данных, что сказывается на скорости работы средств защиты информации, таких как средства аутентификации, DLP системы, анализаторы трафика и т.д. Одним из путей решения проблем скорости доступа является использование вероятностных структур данных, в частности – фильтр Блума.

Фильтр Блума – это вероятностная структура данных, позволяющая хранить и проверять принадлежность элемента к множеству [1]. В фильтре Блума возможны ложноположительные срабатывания. Фильтр Блума представляет собой битовый массив из m бит, которые по умолчанию обнулены. Далее, пользователю необходимо определить k независимых хеш-функций, которые будут преобразовывать массив входных данных произвольной длины в битовую строку фиксированной длины m достаточно равномерным способом. Процент ложноположительных может быть уменьшен увеличением размера массива m и/или числа хеш-функций k [2].

В данной работе был реализован фильтр Блума ($k = 3$, $m = 109$) и использован для определения необходимости вызова удаленной БД. Использование фильтра Блума в качестве структуры данных для хранения информации о наличии элемента в БД позволило сократить на 77 % используемую память по сравнению с хеш-таблицами, также незначительно уменьшило время на добавление состояния новых элементов в множество (> 5 %).

Литература

1. Bloom, B.H. Space/time trade-offs in hash coding with allowable errors.
2. Dillinger, P.C. Fast and Accurate Bitstate Verification for SPIN.

РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ БЕЗОПАСНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ГОМОМОРФНОЙ КРИПТОГРАФИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

М.А. Кадан

С внедрением повсеместного использования облачных технологий остро встает вопрос сохранности данных и их безопасной обработки в облачных хранилищах. Разумным решением проблемы обеспечения конфиденциальности данных может служить шифрование всех приватных данных перед передачей в облако и обеспечение выполнения операций над зашифрованными данными, без их предварительного дешифрования, известное как гомоморфное шифрование [1].

Предметом доклада является применение гомоморфного шифрования в реализации безопасных мобильных приложений для облачных вычислений. Рассматривается задача определения требований к безопасности использования облачных хранилищ данных и подходов к проведению безопасных вычислений над данными облачного хранилища с использованием методов гомоморфного шифрования [2].

На основе теоретических принципов гомоморфного шифрования обоснован, спроектирован и реализован модуль для обеспечения возможности безопасного хранения и обработки данных в облачных структурах, не имеющий аналогов для решения задач данного рода на платформе iOS. Исследована эффективность использования метода гомоморфного шифрования в зависимости от максимальной длины операндов и ключа шифрования, а также исследована производительность модуля с использованием приложения на языке Swift.

Литература

1. Craig Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing (STOC). – 2009. – P. 169–178.

2. Кадан, М.А. Безопасные вычисления с использованием гомоморфной криптографии для облачных хранилищ данных / М.А. Кадан, М.А. Макарычев // Современные информационные технологии и ИТ-образование. 2016. – Т. 12, № 3. – С.43–49.

ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЦИФРОВЫХ ФОТОГРАФИЙ НА ОСНОВЕ РАЗЛИЧИЙ JPEG-ФОРМАТОВ

А.М. Кадан, П.С. Каспер, А.И. Лазарь, Н.А. Радевич, Е.А. Шишкин

Современные цифровые фотокамеры и фотографии, полученные с их помощью, являются носителями информации, значимой для компьютерной технической экспертизы.

Целью данной работы является исследование особенностей формата JPEG, связанных с особенностями программно-технической реализации цифровых фотокамер различных производителей, и формирование наборов признаков для применения методов машинного обучения в задачах классификации цифровых фотокамер (брэнд / модель) на примере задачи определения подлинности цифровых изображений в JPEG-формате.

Согласно требованиям стандарта ISO/IEC 10918-1, JPEG-файл содержит последовательность маркеров, каждый из которых начинается с байта 0xFF.. В то же время в структуре JPEG-формата у различных производителей отличается типы используемых маркеров, количество вхождений маркеров одного типа в структуру файла, длина блока кода, связанного с такими маркерами, порядок появления маркеров в JPEG-файле и другие характеристики, также связанные с маркерами. Различия в использовании маркеров наблюдаются не только в файлах различных производителей фотоаппаратуры, но и для различных моделей одного и того же производителя, а также и для одних и тех же моделей при выборе различных режимов фотосъемки. Использование графического редактора также изменяет структуру исходного JPEG-файла, что позволит идентифицировать программное средство, с помощью которого была нарушена подлинность исходного изображения.

Сказанное выше позволяет выдвинуть гипотезу, что анализ структуры JPEG-формата цифрового изображения позволит получить ответы на вопросы: является ли данное цифровое изображение оригинальным, не подвергалось ли оно редактированию в графическом редакторе; определить бренд-модель цифровой фотокамеры, которой сделано данное изображение.

В ходе выполнения работы была сформирована база, включающая более 1500 различных комбинаций бренд-модель и более 25000 оригинальных цифровых фотографий, ставшая основой для наборов признаков, использованных в методах машинного обучения, положенных в основу приложения для проверки подлинности цифровых изображений.

СЕРВИС ДЛЯ ПРОВЕРКИ ПОДЛИННОСТИ ЦИФРОВЫХ ФОТОГРАФИЙ

А.М. Кадан, П.С. Каспер, А.И. Лазарь, Н.А. Радевич, Д.Ю. Сенько, Е.А. Шишкин

Цифровые фотографии стали неотъемлемой частью информационного обеспечения различных процессов, но широкая доступность инструментов для редактирования изображений зачастую ставит под сомнение их подлинность. Современные цифровые фотокамеры и фотографии, полученные с их помощью, являются носителями криминалистически значимой информации, а количество различных способов мошенничества в сфере ИТ постоянно растет, будучи измененными, такие фотографии уже не будут нести достоверную информацию. Поэтому актуальной, и не только для специалистов в области компьютерной технической экспертизы, является задача обеспечения возможности подтверждения подлинности цифровых изображений. Подобные задачи актуальны, к примеру, в финансовых сферах, страховом деле, информационной безопасности, защите информации и криминалистике.

Под «подтверждением подлинности» будем понимать возможность определения бренда цифровой камеры и ее модели. Либо определение класса программного средства, с помощью которого было изменено оригинальное цифровое изображение.

Целью данной работы является представление клиент-серверной системы, учитывающей особенности реализации формата JPEG, связанные с программно-технической реализацией цифровых фотокамер различных брендов и моделей, работа которой основана на применении методов машинного обучения для решения задачи определения цифровой фотокамеры (брэнд / модель), которой было сделано подлинное изображение, или определения графического редактора, которым были внесены изменения.

Сервис проверки подлинности цифровых изображений разработан и функционирует как локальное клиент-серверное приложение, так как передавать в локальную сеть, а тем более в сеть Интернет, криминалистически значимую информацию недопустимо. Сервис позволяет определять лишь подлинность изображений JPEG-формата, а сам процесс определения подлинности основан на алгоритмах классификации: построения дерева принятий решений и методе k ближайших соседей. В настоящее время база сервиса содержит информацию о 48 брендах (производителях цифровых фотокамер) и более чем 650 моделях.

СИСТЕМА SSO В ИНТЕГРИРОВАННОЙ СЕТИ

А.О. Качанова

Современная тенденция в области аутентификации является использование технологии единого входа (англ. Single Sign-On). Это удачный компромисс между безопасностью доступа к приложениям и удобством работы пользователя. Идея этой технологии заключается в обеспечении единой аутентификации для всех информационных систем организации, которые с точки зрения доступа являются разнородными и никак не интегрированы между собой или с общей службой каталогов. Кроме того, подобное решение повышает уровень информационной безопасности в части парольной политики. Областью практического применения данного исследования являются компании, которые имеют многочисленные внутренние подсистемы.

В докладе рассматривается система, использующая API технологию с использованием языка JSON, что позволяет обеспечить надежную политику безопасности, повышенную безопасность всех ресурсов предприятия, снизить вероятность возникновения критических ошибок, упростить процесс аутентификации пользователя в интегрированной сети. Система использует дополнительную биометрическую процедуру аутентификации.

Литература

1. Bashir, K., Asif, S. Important Considerations for Single Sign-On Solution. International Journal of Multidisciplinary Sciences and Engineering, 2010.

2. Bishop, M. Introduction to Computer Security. Boston: Pearson Education, 2005

АНАЛИЗ РЕЧЕВОЙ ИНФОРМАЦИИ КАК ЭТАП МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СЕТИ ИНТЕРНЕТ

Е.В. Кисель, А.В. Курочкин

В настоящее время значительное внимание уделяется задаче идентификации и аутентификации личности на основании одного или нескольких биометрических признаков. Одним из перспективных направлений в биометрической идентификации и аутентификации является распознавание речевой информации. Существенным преимуществом использования голоса в качестве одного из факторов аутентификации является отсутствие необходимости в сложном специализированном оборудовании – для записи образца голоса можно использовать обычный микрофон. Распознавание речевой информации может использоваться в качестве одного из факторов при проведении многофакторной аутентификации. В значительной степени многофакторная аутентификация может применяться для обеспечения безопасности при доступе на различные интернет-ресурсы. В данном контексте большой значимостью обладает задача автоматизированного распознавания речи в реальном времени в рамках проведения многофакторной аутентификации на веб-сайт. Пользователю предлагается, в качестве одного из этапов аутентификации для входа на защищенную зону веб-сайта, произнести заранее записанный пароль, который в дальнейшем сверяется с эталоном во внутренней базе данных; на основании результата сверки принимается решение о подтверждении или отклонении

аутентификации. Для реализации описанной функциональности может использоваться библиотека pocketsphinx.js. Библиотека разработана с использованием языка javascript и позволяет осуществлять распознавание речи в реальном времени прямо в браузере конечного пользователя. Принцип работы распознавания основан на использовании скрытых марковских моделей. Основные преимущества такого подхода – высокая скорость и точность распознавания. Для хранения эталонных образцов может осуществляться генерация словарей, на основании которых можно осуществлять аутентификацию пользователя по голосу.

Литература

1. Speech Silicon: An FPGA Architecture for Real-Time Hidden Markov-Model-Based Speech Recognition / J. Schuster [et al.] // J. Embedded Systems. 2006.

2. On Preprocessing of Speech Signals / A. Keerio [et al.] // International Journal of Signal Processing. 2009. № 5.

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕДИЦИНСКИХ СИСТЕМАХ

А.В. Курочкин, Е.А. Головатая

Внедрение информационных технологий в медицине обуславливает необходимость уделять значительное внимание вопросам информационной безопасности в различных видах систем медицинского учета. Конфиденциальность личных данных и защита информации, представляющей врачебную тайну, является важнейшей составляющей медицинских систем. Таким образом, при их проектировании необходима разработка комплексного решения по обеспечению конфиденциальности, целостности и доступности обрабатываемых данных.

Обеспечение конфиденциальности в медицинских системах осуществляется при помощи жесткого разграничения доступа к информации, представляющей врачебную тайну – электронным медицинским картам, историям болезни и т.п. Введение политики аудита обрабатываемых данных позволяет отследить возможные источники утечки информации. Использование процедур многофакторной аутентификации и введение политики смены парольной информации для персонала позволяет снизить риск несанкционированного доступа. При ограничении доступа необходимо учитывать, что конфиденциальными являются не только единичные записи, но и различные виды отчетной, сводной и статистической информации.

Для предотвращения угроз доступности информации необходимо исключить возможность доступа ко всей базе данных медицинских записей целиком, а также ограничить доступность внутренней сети медицинского учреждения извне. Кроме того, для предотвращения возможных последствий, можно использовать процедуру планового резервного копирования информации с физическим ограничением доступа к резервным копиям. Угрозы доступности данных в медицинских системах обычно стоят не так остро, как в системах с массовым доступом. Тем не менее, для снижения рисков ограничения доступности по непредвиденным обстоятельствам можно использовать репликацию или шардинг информации.

Литература

1. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с.

2. Prater V.S. Confidentiality, privacy and security of health information: Balancing interests / V.S. Prater // University of Illinois, Chicago: Biomedical and Health Information Sciences, December 8, 2014.

АЛГОРИТМ ОБЕСПЕЧЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ ИНФОРМАЦИОННОГО ПОТОКА НА ОСНОВЕ ШИРОКОПОЛОСНОГО СИГНАЛА

М.А. Лебедевич

В настоящее время к системам передачи информации предъявляются высокие требования к безопасности передаваемой по открытым каналам связи информации. Одним из основных путей обеспечения этих требований является использование сигналов с расширением

спектра, или шумоподобных сигналов (ШПС). Применение подобного сигнала подразумевает использование специального кода (в нашем случае, псевдослучайной последовательности) на приемной и передающей стороне. Через использование в системе метода расширения спектра достигается энергетическая эффективность и помехозащищенность сигнально-кодовой конструкции, защита от сосредоточенных помех и сокрытие сигнала под шумами.

Основной задачей проводимых исследований является синтезирование алгоритма, обеспечивающего указанные выше характеристики, если в качестве расширяющей спектр последовательности будет использоваться случайно-подобный бинарный или многоуровневый сигнал, генерируемый системами с нелинейными обратными связями. По результатам проведенного исследования предполагается синтезировать квазиоптимальный алгоритм обработки сигнала на фоне помех и выявить параметры нелинейной системы, при которых обеспечивается приемлемый коэффициент взаимной корреляции сигналов.

Результаты данной работы могут оказать большую помощь в разработке и оптимизации схем и алгоритмов расширения спектра и внести большой вклад в улучшения качества связи.

Литература

1. Чердынцев, В.А. Системы передачи информации с расширением спектра сигналов / В.А. Чердынцев, В.В. Дубровский. – Минск, 2009. – 131 с.

2. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

ОБЪЕДИНЕНИЕ РЕШЕНИЙ О КЛАССЕ ЦЕЛИ В ИНФОРМАЦИОННОЙ ПОДСИСТЕМЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ЗЕНИТНОЙ РАКЕТНОЙ БРИГАДЫ

А.Ю. Липлянин, Е.И. Хижняк

В основе эффективного управления боевыми средствами системы войск противовоздушной обороны лежит качественное управление огневыми средствами, решаемое в управляемой подсистеме комплексов средств автоматизации. Одним из факторов успешного функционирования управляющей подсистемы является эффективное решение задачи целераспределения. При этом критерием качества процесса целераспределения определим значение предотвращенного ущерба объекту обороны [1], в котором немаловажный фактор при расчете данного показателя учитывается важность цели, которая в настоящий момент задается оператором вручную. Однако, не вызывает сомнения тот факт, что важность цели неразрывно связана с ее классом и задачей выполняемой в налете [2]. Но в связи с тем, что на средства автоматизации приходят данные о классе цели от различных источников, решения о принадлежности классов источников разнится как качественно, так и количественно. По этой причине возникает задача объединения решений о классе цели.

В современной зарубежной литературе задачи, методы и алгоритмы коллективного распознавания встречаются в различных работах под разными названиями:

– объединение множества классификаторов (combination of multiple classifiers);
– объединение классификаторов (classifier fusion);
– объединение экспертов (mixture of experts);
– комитеты (committees);
– согласованная агрегация (consensus aggregation);
– голосующее объединение классификаторов (voting pool of classifiers);
– динамический выбор классификатора (dynamic classifier selection);
– комбинированные системы классификаторов (composite classifier system);
– комбинирование решений (decision combining);
– классификаторы типа «разделяй и властвуй» (divide-and-conquer classifiers).

В действительности, приведенное разнообразие используемой терминологии отражает также и разнообразие постановок задач, предположений, типы выходов классификаторов, стратегии объединения. [3] Задачей настоящей диссертационной работы является создание метода и алгоритма объединения решений классификаторов для качественного распознавания классов целей, для дальнейшего использования при решении задачи целераспределения. Это позволит решать задачу целераспределения более эффективно.

Литература

1. Кругликов, С.В. Методика решения задачи многофакторного целераспределения в автоматизированной системе управления / С.В. Кругликов // Доклады БГУИР. – 2013. – № 5. – С 93–99.

2. Липлянин, А.Ю. Методика учета важности цели при решении задачи распределения летательных аппаратов между огневыми средствами / А.Ю. Липлянин, А.С. Шеин, А.В. Хижняк // Доклады БГУИР. – 2017. – № 2. – С 77–84.

3. Городецкий, В.И.Методы и алгоритмы коллективного распознавания: обзор / В.И. Городецкий, С.В. Серебряков // Труды СПИИРАН. – 2006. – Вып. 3, т. 1. – С. 139 – 171.

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ В АЛГОРИТМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Липницкий, Л.В. Михайловская

Различные аспекты, связанные с решением алгебраических уравнений, часто и довольно неожиданно возникают при практической реализации тех или иных криптографических систем. Так, криптосистема Рабина своим базовым алгоритмом дешифрования ставит проблему решения квадратного уравнения в кольце классов вычетов по составному модулю – произведению двух простых нечетных чисел. Как ни странно, такие квадратные уравнения в общем случае имеют четыре, а не два корня.

Решение уравнения легальными пользователями сводит задачу по китайской теореме об остатках в минимальных полях Z/pZ и Z/qZ. Если p и q относятся к классу простых чисел Блюма, т.е. имеют вид $4t+3$, t – натуральное число, то задача легко решается возведением дискриминанта в строго определенную степень. Если же $p = 4t+1$, то при нечетных t существуют аналогичные формулы, а при четных t поиск квадратных корней осуществляется процедурой перебора, хотя и достаточно ограниченного перебора. Поэтому реальные пользователи криптосистемы Рабина стараются брать простые числа вида, рассмотренного в первом случае. Хакер вынужден вначале факторизовать модуль n в произведение простых множителей, т.е. решить ту же проблему, что и в криптосистеме *RSA*. Глубокое владение теорией чисел позволяет строить совершенные криптографические системы, удобные и практичные в применении.

ГРУППА АВТОМОРФИЗМОВ БЧХ-КОДА И ЕЕ ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ

В.А. Липницкий, Е.В. Середа

По сути дела, группа автоморфизмов G любого БЧХ-кода порождена циклической и циклотомической подстановками, а потому является некоммутативной. Нормы синдромов – основной объект, разработанный белорусскими кодировщиками ТНС – теории норм синдромов – явились эффективными инвариантами группы Γ циклических сдвигов: норма синдрома так специфично определена через компоненты синдрома, что является одинаковой для всех векторов каждой Γ-орбиты ошибок, поэтому данный уникальный параметр и назван нормой Γ-орбиты. Выяснялось, что нормы Γ-орбит любой корректируемой совокупности векторов-ошибок попарно различны. Практическим следствием данной теории явилось семейство перестановочных норменных методов и алгоритмов коррекции ошибок БЧХ-кодами, на порядок ускоряющих работу декодеров по сравнению с традиционными синдромными алгоритмами.

В докладе рассматриваются полиномиальные инварианты всей группы G автоморфизмов БЧХ-кодов. Каждая G-орбита представляет собой объединение строго определенного ряда Γ-орбит, связанных друг с другом посредством циклотомической подстановки и ее степеней. Нормы циклотомически связанных Γ-орбит являются сопряженными элементами в конечном поле – поле определения соответствующего БЧХ-кода. Семейство взаимно сопряженных элементов поля Галуа составляет полную группу корней неприводимого полинома любого из элементов этого семейства. Согласно формулам Виета, всякий полином однозначно определяется своими корнями. Таким образом, полное семейство попарно сопряженных норм Γ-орбит, составляющих данную G-орбиту, задают однозначно определенный полином, корнями которого они являются. Это и есть полиномиальный

инвариант данной G-орбиты. Предлагаемые полиномы являются своеобразными уникальными индикаторами каждой G-орбиты векторов-ошибок. Следовательно, полиномиальные инварианты могут служить основой обобщения ТНС, которая допускает укрупненную классификацию векторов-ошибок, то есть разбиение их на G-орбиты. Вычисление полиномиального инварианта очередной корректируемой ошибки позволит определить однозначно G-орбиту, которой принадлежит искомая ошибка. Дальнейший поиск ошибки будет проводится среди Γ-орбит, входящих в данную G-орбиту. Данные обстоятельства резко сужают переборные элементы полиномиально-перестановочного алгоритма декодирования, что делает его более эффективным даже в сравнении с норменными методами.

ОБ АЛГОРИТМЕ ПОДСЧЕТА КОЛИЧЕСТВА ОРБИТ (0,1)-МАТРИЦ

В.А. Липницкий, Н.В. Спичекова

Матрицы как двумерные массивы информации относятся к базовым объектам высшей математики. Бинарные матрицы, то есть матрицы с элементами 0 и 1, приобрели важное значение в дискретной математике, теории графов и теории групп, теории информации и помехоустойчивом кодировании, медицине и биологии. Большой вклад в исследование класса $P(n)$ квадратных (0, 1) – матриц порядка n, содержащих в точности n единиц, внес английский математик П. Кэмерон. На исследование этого же класса матриц вышла белорусская школа помехоустойчивого кодирования [1].

Мощность класса $P(n)$ стремительно растет с ростом n. Например, $P(8)$ содержит 4 426 165 368 элементов. Поэтому целесообразно множес тво $P(n)$ делить на подклассы каким-то достаточно естественным образом. С середины XIX века в математике приобрела массовое применение идея разбиения множеств на орбиты – классы эквивалентности под действием на этих множествах тех или иных групп. Математические и технические приложения класса $P(n)$ показывают, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк между собой или же перестановки столбцов между собой. Иными словами, наибольший интерес для пользователей представляют орбиты на множестве $P(n)$, которые образуются под действием квадрата симметрической группы. Естественным образом возникает задача о количестве таких орбит в классе $P(n)$.

Самый очевидный – переборный - способ вычисления количества орбит на множестве $P(n)$ представляет собой вычислительно сложную задачу. Поэтому применение класса $P(n)$ на практике предполагает разработку эффективных алгоритмов подсчета количества орбит этого множества. В докладе представлен реккурентный алгоритм подсчета количества орбит множества $P(n)$. Алгоритм основан на лемме Бёрнсайда [2]. Для нахождения числа матриц, инвариантных относительно действия фиксированной подстановки, используется линейная развертка бинарной матрицы. Получена оценка сложности предлагаемого алгоритма.

Литература

1. Цветков, В.Ю. Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов / В.Ю. Цветков, В.К. Конопелько, В.А. Липницкий. – Мн.: Издательский центр БГУ, 2014. – 224 с.

2. Харари, Ф. Теория графов / Ф. Харари. – М.: Мир, 1973. – 300 с.

РАСПОЗНАВАНИЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ С ПОМОЩЬЮ ЦИФРОВЫХ КАМЕР МОБИЛЬНЫХ УСТРОЙСТВ

А.М. Мажейко

Отрасль биометрического определения пользователя в информационных системах с каждым годом становится все шире и шире. Если 20 лет назад биометрические считыватели использовались исключительно в специализированных целях, то в последнее десятилетие сканеры отпечатка пальца внедряются в ноутбуки и мобильные телефоны. Однако вопрос использования еще более дешевых сканеров и методов распознавания остается открытым. Одним из самых распространенных устройств ввода на мобильных устройствах являются: микрофон и фотокамера. Исследования в Томском политехническом университете показали о

возможности эффективного распознавания ладони при анализе видеопотока камеры [1]. Это позволяет использовать цифровые камеры для получения информации о пользователе компьютера. Также в работе Бакиной И.Г. приводятся алгоритмы распознавания исключающие ошибки «склеивания пальцев» и длинных ногтей [2].

В настоящее время крупные производители компьютерной техники выпустили прототипы программного обеспечения для авторизации в системе ноутбуков. Среди них самые примечательные образцы: VeriFace от компании Lenovo, Face Recognition от Toshiba и SmartLogon от Asus. К сожалению, в алгоритмах этих программ заложены функции сравнения получаемого от камеры изображения лица с заданным образцом. Здесь высока вероятность ложного доступа в систему по представлению распечатанного изображения пользователя. Попытки устранения этой уязвимости предприняла компания NeuroTechnology в своем продукте VeriLook. Предпринятые попытки обмануть систему фотографией не увенчались успехом. Данный факт позволяет утверждать: а) технология биометрического распознавания пользователей по фото веб-камеры имеет перспективы развития; б) методика распознавания требует значительных доработок для повышения эффективности.

Литература

1. Нгуен Тоан Тханг. Алгоритмическое и программное обеспечение для распознавания формы руки в реальном времени с использованием SURF-дескрипторов и нейронной сети / Нгуен Тоан Тханг, В.Г. Спицын // Известия Томского политехнического университета. – 2012. – № 5 (320).

2. Бакина, И.Г. Генерация признаков для сравнения ладоней при наличии артефактов / И.Г. Бакина // Журнал «Прикладная информатика». – 2009. – № 4 (22).

ЧИСЛЕННОЕ ОПРЕДЕЛЕНИЕ РИСКОВ БЕЗОПАСНОСТИ СВЯЗИ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.В. Макатерчик

В настоящее время значительно возрастает роль современных инфокоммуникационных систем специального назначения (ИКС СН). Развитие и совершенствование таких систем ведется в соответствии с общемировыми тенденциями. Активное внедрение новых средств связи, протоколов и инфокоммуникационных технологий привело к появлению неизученных угроз безопасности связи, возможность реализации которых злоумышленниками негативно влияет на обеспечение информационной безопасности государства и организаций различных форм собственности. Под угрозой безопасности связи понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба системе связи или ее компонентам.

Выделяют следующие виды возможных атак на ИКС СН: пассивная, активная (отказ в обслуживании, модификация потока, создание ложного потока, повторное использование). При этом реализация атаки на ИКС СН включает следующие этапы: сбор информации, выбор метода реализации и типа атаки, реализация выбранного типа атаки, завершение атаки.

На основе проведенного анализа реализации угроз информационной безопасности численное определение рисков безопасности связи для элемента ИКС СН определен способ численного определения рисков безопасности связи для элемента инфокоммуникационных систем специального назначения использованием выведенной формулы. Полученные для каждого элемента ИКС СН значения в дальнейшем используются в ходе определения численного значения рисков безопасности связи для всей ИКС СН. Предложенный подход позволяет определить численное значение рисков безопасности связи для ИКС СН с учетом как существующих, так и потенциальных уязвимостей на основе оценки мероприятий по обеспечению безопасности связи.

КОРРЕКЦИЯ МОДУЛЬНЫХ ОШИБОК БЛОКОВЫМИ КОДАМИ, ПОСТРОЕННЫМИ НА ОСНОВЕ СОСТАВНЫХ САМООРТОГОНАЛЬНЫХ СВЕРТОЧНЫХ КОДОВ

Е.Г. Макейчик, А.И. Королёв, В.К. Конопелько, М.Д. Исакович,
А.С. Ковалевский, Ю.Е. Яворко

Предложен метод построения канального кодека блокового кода на основе составного самортогонального сверточного кода (СССК) с пороговым алгоритмом декодирования со скоростью $R \geq 2/3$. Определены параметры канального кодека, реализующего блоковый способ кодирования и декодирования информации, построенного на основе составного самоортогонального сверточного кода с пороговым алгоритмом декодирования. Установлено, что метод построения канальных кодеков на основе составных самоортогональных сверточных кодов с пороговым алгоритмом декодирования и реализующий блоковый способ кодирования и декодирования информации, обеспечивает увеличение в $\alpha(\alpha \geq 2)$ раз корректирующую способность базового СССК. Для практического применения предложенного метода построения канальных кодеков для коррекции модульных (зависимых) ошибок достаточно использование коэффициента внутреннего перемежения информационных символов $\alpha = 2.$

Литература

1. Радченко А.Н., Мирончиков Е.Г. // Радиотехника и электроника. 1961. № 11. С. 18–33.
2. Дмитриев О.Ф. // Радиотехника. 1964. Т. 19, № 4. С. 68–75.

КОРРЕКЦИЯ ЗАВИСИМЫХ ОШИБОК НА ОСНОВЕ РАВНОМЕРНЫХ СВЕРТОЧНЫХ КОДОВ

Е.Г. Макейчик, А.И. Королёв, В.К. Конопелько

Рассматриваются методы $(n_0 = k_0 + 2)$-канального кодирования и декодирования зависимых ошибок на основе систематических равномерных сверточных кодов (СРСК), обеспечивающие повышение скорости передачи кода и корректирующую способность исходных СРСК. Оценивается эффективность предложенных методов кодирования. Разработан метод $(n_0 - 1, n_0 \geq 3)$-канального кодирования/декодирования зависимых ошибок на основе двух систематических равномерных сверточных кодов, обеспечивающий повышение в 2 и более раза скорость передачи кода и увеличение в 1,33 раза корректирующую способность канального кодека. Разработан метод $(n_0 - 1, n_0 = k_0 + 2, k_0 = 1)$-канального кодирования/декодирования зависимых ошибок на основе систематического равномерного сверточного кода, обеспечивающий коррекцию ошибок заданной кратности при увеличении в 1,34 раза скорости передачи СРСК канального кодера. Установлено, что предложенные методы кодирования и декодирования обеспечивают увеличение скорости передачи исходных (базовых) СРСК и уменьшают вероятность ошибочного декодирования.

Литература

1. Конопелько В.К., Липницкий В.А., Дворников В.Д. и др. Теория прикладного кодирования. Минск, 2004.
2. Кудряшов Б.Д. // Пробл. передачи информ. 1990. Т. 26, вып. 2. С. 18–26.

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ МОДИФИКАЦИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В.В. Маликов, М.А. Бабич, А.В. Макатерчик

Использование стеганографических технологий модификации конфиденциальной информации позволяет преодолеть защиту традиционных средств и систем информационной безопасности применяемых в организациях. В рамках исследования проведено тестирование эффективности DLP-системы на стеганографические технологии модификации файлов. Для оценки эффективности перехвата модифицированной информации была выбрана DLP-система

«SecureTower» российской компании Falcongaze [1]. В качестве эксперимента 2 тестовых файла (формат: doc, rar; объем: до 50 КБ) с конфиденциальной информацией с использованием стенографического ПО «OpenPuff» (v.4.00 /настройки качества: по умолчанию/, LSB-метод) [2] встраивались в файл-контейнер (формат: png, jpg, pdf). Эффективность перехвата оценивалась в процентах от детекции сформированной тестовой базы из 6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [3]).

На основании проведенного исследования можно сделать вывод, что использование DLP-системы в настоящее время не позволяет детектировать стеганографические технологии модификации файлов. Эффективность перехвата данных DLP-системой по заданному перечню стеганографических модификаций файлов составила 0 % («цифровой отпечаток» (Digital Fingerprints) / контрольная сумма (хэш)).

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. OpenPuff team // download.cnet.com [Электрон. ресурс]. – 2017. – Режим доступа: http://download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html. – Дата доступа: 23.04.2017.

3. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ ПЕРЕХВАТА ДАННЫХ DLP-СИСТЕМЫ

В.В. Маликов, Е.О. Перхальский, И.И. Лившиц

Внедрение и использование DLP-систем позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Для оценки эффективности была выбрана DLP-система «SecureTower» российской компании Falcongaze [1], которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [2]).

Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы: POP3, SMTP, HTTP и др.). Назначение портов приложений использовались по умолчанию. Эффективность перехвата оценивалась в процентах от детекции сформированных тестовых баз из 20 файлов / сообщений в 2-х режимах DLP-системы (настройки по умолчанию / специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы:

1. Программная среда функционирования DLP-системы Falcongaze «SecureTower» в настоящее время поддерживает все основные ОС семейства Microsoft «Windows».

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов / портов составила от 90 % до 100 %.

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ FANET

А.В. Малолетний, А.Е. Кудлай, М.Ю. Хоменок

Необходимость расширения приложений беспроводных сенсорных сетей WSN (wireless sensornetwork) и качества предоставляемых услуг явились причиной проведения исследований по разработке этой сети в комбинации с мобильной Ad Hoc сетью MANET (Mobile Ad Hoc Netwoks). MANET как и WNS, используется как в гражданской так и военной областях. В [1] отмечается возможность крупномасштабного развертывания сети WSN-MANET, по технологии smart city, представляющей широкий спектр услуг: мониторинг шума, света, загрязнения окружающей среды, движения транспортных средств, противоугонная защита, контроль по предотвращению обрушения старых зданий, мостов, экстренная медицинская услуга, услуги пожилым людям и др.

Другим значимым примером развертывания сети WSN-MANET в комбинации с летающей Ad Hoc сетью является ЛСС (летающая сенсорная сеть) FANET (Flying Ad Hoc Netwoks), которая включает беспилотные летающие аппараты БПЛА (Unmanned Air Vehicles, UAVs), используемые для удаленного получения изображений, мониторинга стихийных бедствий, видеотрансляции и др. [2]. Сеть FANET имеет более сложные проблемы информационной безопасности (ИБ) по сравнению с MANET. Одними из причин является более высокая мобильность и соответственно более быстрое изменение топологии сети, а также большие расстояния между БПЛА, чем между узлами в MANET.

При проектировании ЛСС стоит задача выбора узла иерархии в качестве шлюза для взаимодействия с группой БПЛА в FANET. При этом важную роль имеет анализ угроз ИБ при получении шлюзом на каждом уровне полных и корректных сенсорных данных. В докладе рассматриваются вопросы обеспечения информационной безопасности ЛСС иерархической структуры от воздействия атак DoS.

Литература

1. Convergence of MANET and WSN in IoT Urban Scenarios / P. Bellavista [et al.]. // IEEE Sensors Journal. – 2013. – Vol. 13, № 10. – P. 3558–3567.

2. Razzaqi, A.A. Antenna array design for multi-UAVs communication in next generation Flying Ad-Hoc Networks (FANETs). High-capacity Optical Networks and Emerging / A.A. Razzaqi, M. Mustaqim, B.A. Khawaja // Enabling Technologies (HONET): 11th Annual. – 2014. – P. 25–28.

О ПРИМЕНЕНИИ СТАТИСТИЧЕСКИХ МЕТОДОВ ДЛЯ ОЦЕНКИ КАЧЕСТВА КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

М.В. Мальцев, В.Ю. Палуха, Ю.С. Харин

Для надежного шифрования необходимы криптографические генераторы – устройства, вырабатывающие последовательности случайных или псевдослучайных чисел. Выходные последовательности криптографического генератора должны быть неотличимы от «чисто случайной» или равномерно распределенной случайной последовательности (РРСП) [1]. Для оценки качества таких выходных последовательностей применяются вероятностно-статистические методы. В частности, критерием надежности генератора может служить энтропия, причем помимо классической энтропии Шеннона перспективным направлением является применение энтропии Тсаллиса и Реньи. Энтропийный анализ используется для статистического тестирования и распознавания криптографических генераторов [2].

Элементы РРСП независимы в совокупности, но псевдослучайные последовательности вырабатываются генераторами по определенным детерминированным алгоритмам и в таких последовательностях присутствуют зависимости, как правило, большой глубины. Для описания таких зависимостей адекватной моделью является цепь Маркова порядка s. К сожалению, использовать ее на практике зачастую невозможно, поскольку число параметров этой модели увеличивается экспоненциально с ростом s. В связи с этим необходимы так называемые малопараметрические марковские модели, число параметров которых зависит от s полиномиально [3]. Авторами данной статьи разработан ряд малопараметрических моделей для анализа зависимостей в выходных последовательностях криптографических генераторов.

Литература

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

2. Палуха, В.Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности // Вес. Нац. акад. навук Беларуси. Сер. фіз.-мат. навук. – 2017. – №1. – С. 79–88.

3. Мальцев, М.В. Малопараметрические марковские модели в задачах защиты информации / М.В. Мальцев, Ю.С. Харин // Электроника ИНФО. – 2013.– С. 202–207.

СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОЛОСОВОГО ТРАКТА

М.Г. Матуть, В.А. Вишняков

Контроль телефонных переговоров остается одним из наиболее распространенных видов промышленного шпионажа и действий злоумышленников. Причины – низкий уровень затрат и риск реализации угроз, необязательность захода в контролируемое помещение, разнообразие способов и мест съема информации. В широком смысле можно выделить средства противодействия: физическая защита информации, включающие в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации; криптографическая защита информации.

Криптофон представляет собой смартфон с установленным специальным программным обеспечением. Современные криптофоны используют, в основном, алгоритмы шифрования AES и Twofish. В сфере IP-телефонии можно рассматривать варианты использования IPsec (Internet Protocol Security) на сетевом уровне, либо протоколы TLS (Transport Layer Security) и SRTP (Secure RTP) на транспортном уровне.

В качестве основы разрабатываемого программного средства был выбран проект с открытым исходным кодом – CSipSimple, который является бесплатным SIP-клиентом, работающим под ОС Android и распространяющимся по лицензии GNU GPL. Выбор CSipSimple обусловлен наличием в нем открытых реализаций протоколов SIP over TLS, SRTP и ZRTP; поддержка различных кодеков (Speex, G.711, GSM-FR, G.729, G.722 и другие) и возможность добавления новых, при помощи плагинов; наличие плагина для осуществления видеозвонков, одновременно может быть активно до 10 аккаунтов.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.Р. Мацылевич

Автоматизация управления защитой информации в информационных сетях специального назначения (ИССН) позволит максимально исключить влияние так называемого «человеческого фактора», который является не только фактором, снижающим эффективность системы защиты информации в ИССН, но, в некоторых условиях, становится угрозой безопасности информации высокого потенциала.

Основными вопросами автоматизации управления защитой информации являются:

представление защиты информации как объекта управления (определение входных и выходных переменных, метрик пространства состояний, описание поведения защиты информации в пространстве ее состояний и другие);

постановка целей, определение методов их достижения, а также критериев управления защитой информации адекватных целям, задачам и условиям функционирования ИССН;

разработка порядка применения средств и систем автоматизированного управления защитой информации в ИССН;

разработка методов контроля эффективности и оптимизации управления защитой информации в ИССН с учетом специфики их функционирования.

В настоящее время уже существуют подходы для создания систем управления организационно-техническими процессами, к которым относится защита информации [1]. Одним из подходов в автоматизации управления защитой информации в ИССН является применение научно-методологического аппарата теории автоматического управления.

О выявленных в ходе научных исследований по вопросам автоматизации управления защитой информации в ИССН некоторых проблемных вопросах и предлагаемых путях их решения ведется речь в докладе.

Литература

1. Интеллектуальные системы управления организационно-техническими системами / А.Н. Антамошин и [др.]; под ред. проф. А.А.Большакова. – М.: Горячая линия – Телеком, 2006. – 160 с.: ил.

ЗАЩИТА ИТКС ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.С. Мешков, В.П. Ширинский, И.Г. Некрашевич

Для современного этапа развития общества характерен непрерывный процесс информатизации. Сфера внедрения телекоммуникаций и вычислительных систем постоянно расширяется. В связи с этим важной задачей является обеспечение достаточной защищенности таких систем. При рассмотрении вопроса безопасности функционирования информационно-телекоммуникационной системы (ИТКС) определяющую роль играют угрозы, реализуемые посредством удаленного воздействия с объектом взаимодействия, или так называемые сетевые атаки. Большинство распределенных систем функционируют и проектируются с учетом использования в них технологии межсетевого взаимодействия, реализованной в Интернет. При этом ИТКС базируется на применении протоколов межсетевого воздействия TCP/IP. Поэтому в РТКС могут реализовываться большинство атак, характерных для Интернет.

Для оценки систем защищенности ИТКС в условиях воздействия на ее компоненты некоторого набора угроз необходимо перейти к категории риска. Риск – это сочетание величины ущерба и возможности реализации исхода, влекущего за собой такой ущерб.

Угрозы информационной безопасности имеют вероятный характер. Анализ возможных угроз и анализ рисков служит основой для выбора мер по защите ИТКС, которые должны быть осуществлены для снижения риска до приемлемого уровня.

Предполагаемая работа заключается в исследовании и разработке методики анализа информационных рисков и управления защищенностью ИТКС от угроз несанкционированного доступа к ее компонентам.

Литература

1. Бобов, М.Н. Протоколы аутентификации в сетях телекоммуникаций / М.Н. Бобов. – Мн.: БГУИР, 2004. – 26 с.

2. Мельников, Д.А. Информационные процессы в компьютерных сетях: протоколы, стандарты, интерфейсы, модели / Д.А. Мельников. – М.: Кудиц-образ, 1999. – 256 с.

3. Щербаков, А.Ю. Современная компьютерная безопасность: теоретические основы, практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 351 с.

4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин. – М.: Форум, 2016. – 591 с.

ОБРАБОТКА ДАННЫХ ИДЕНТИФИКАЦИИ ПО СЕТЧАТКЕ ГЛАЗА

А.И. Митюхин, Р.П. Гришель

Изображение кровеносных сосудов глазного дна является биометрическим параметром индивидуального организма человека и может использоваться для решения задачи идентификации человека с помощью технической системы с особыми требованиями по надежности или в криминалистике. В сравнении с другими биометрическими параметрами, используемыми для идентификации личности (например, отпечатки пальцев – качество отпечатков зависит от возраста; распознавания по лицу – систему распознавания можно обмануть с помощью маскировки и пр.), достоинством распознавания по сетчатке глаза является постоянство биометрического параметра. Уникальное изображение отдельных фрагментов сосудистой сети глазного дна описывается совокупностью элементов (пикселями), представляющими эту сеть.

В работе приводятся результаты исследования, связанные с цифровой обработкой и распознаванием по изображению кровеносных сосудов глазного дна на основе статистического подхода и энтропийного кодирования. Для этого рассчитывались статистические характеристики изображения сети кровеносных сосудов. Сеть представлялась рядом цифровых последовательностей с числом точек (отсчетов), количество которых определялось размером обрабатываемого фрагмента или длиной линии, описывающей кровеносный сосуд. Определенная степень линейной зависимости между совокупностями данных, описывающих сеть, и применение в качестве дескрипторов распознавания коэффициентов разложения по базису собственных функций позволила уменьшить размерность области распознавания. Фильтрация значений дескрипторов осуществлялась на основе дисперсионного критерия [1]. Такая процедура выбора признаков распознавания позволила упростить процесс правильной классификации, измерения сходства биометрических образцов.

Литература

1. Мультиспектральное наблюдение / А.И. Митюхин // Технические средства защиты информации материалы XI Белорусско-российской науч.-техн. конф. Минск, 4–5 июня 2013 г. – С. 44–45.

ПОДДЕРЖКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

М.Г. Моздурани Шираз, В.А. Вишняков

Наиболее распространенной нейросетевой структурой, используемой для решения задач защиты информации, является многослойный персептрон. Построена обучающая выборка для многослойного персептрона, определяющего, содержит ли данная программа (ее исполняемый файл) вредоносный код или нет. В ходе работы было проведено обучение данной нейросетевой структуры при помощи специально построенной выборки исполняемых файлов двух состояний: «отсутствие вредоносного кода» и «наличие вредоносного кода». Обучение проводилось в SPSS Statistics – программе, произведенной компанией IBM. Для обучения многослойного персептрона данные обучающей выборки приведены к десятичному представлению. Для автоматизации решения данной задачи на языке JavaScript был написан конвертер чисел между различными системами счисления.

Исследована эффективность работы нейронной сети с помощью контрольной выборки исполняемых файлов после ее обучения. Относительная погрешность классификации файлов составила 5 %, однако, следует отметить, что при обучении данной нейронной сети использовалась относительно небольшая выборка исполняемых файлов; для использования же нейронной сети при решении реальных задач защиты информации, например, во внутрикорпоративных системах, выборка файлов должна быть больше, и вредоносные коды, которые внедряются в часть файлов из выборки, должны быть более разнообразными.

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС НА БАЗЕ СОВ И МСЭ

М.Г. Моздурани Шираз, В.А. Вишняков

Представлено два подхода к реализации системы предотвращения вторжений: первые при выявлении атаки реконфигурируют активное сетевое оборудование (например, Snort SAM); вторые при выявлении атаки принимают решения, на основе правил, о дальнейшем действии с пакета (например, Snort inline). Недостатком первого подхода является то, что на создание правила, передачу его межсетевому экрану, реконфигурирование самого межсетевого экрана уходит время. Система Snort_inline при обнаружении следов атаки в пакете сама уничтожает пакет, что эффективней первого решения.

Представлена структура защищаемой сети. Сервер работает под управлением Slackware Linux 10.2 с ядром версии 2.4.31. Данная версия ядра является наиболее исследованной, стабильной и содержит минимальное число обнаруживаемых уязвимостей. Сервер защищен с помощью межсетевого экрана IPTables (v1.3.3).

В результате объединения IDS Snort и МСЭ IPTables получается двухуровневая система защиты: на первом уровне iptables проверяет входящий пакет на соответствие своим правилам фильтрации, если пакет получил разрешение на прохождение через межсетевой экран, его проверяет система обнаружения вторжений на наличие вредоносного кода в теле входящего пакета. Представлен скрипт конфигурирующий Snort_inline и IPTables для совместной работы.

ОБ ОДНОЙ МОДИФИКАЦИИ АЛГОРИТМА XOR

И.В. Молчанов, М.А. Калугина

Обратимость логической операции исключающего ИЛИ позволила успешно использовать ее в синхронном шифровании. Однако основанный на ней классический алгоритм XOR рекомендуется применять лишь однократно из-за его уязвимости к криптоанализу при достаточно большом количестве перехваченных зашифрованных данных.

Реализованный в утилите для Windows алгоритм на основе простого XOR предназначен для приложений, использующих уникальный ключ для шифрования каждого конкретного блока информации. Он состоит из шифрования данных простым алгоритмом XOR и добавления «шума» с использованием специальной рекуррентной последовательности псевдослучайных чисел. Эта последовательность формируется заранее по следующей схеме: $a_0=A$, $a_1=B$, $a_{i+1}=\alpha \bullet a_{i-1}+ \beta \bullet a_i$, − где A, B, α, β – псевдослучайные числа, которые вычисляются до исполнения.

Ключ генерируется как последовательность псевдослучайных байтов или как ключевая фраза, задаваемая пользователем (данная реализация включает псевдослучайный ключ на основе вычисления количества байтов в шифруемом файле). Частью ключа являются значения A, B, α, β.

Шифрование. Пусть M , K , E – массивы символов (байтов) в файле ввода, в ключе и в файле вывода соответственно. Тогда $E_i = M_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, $E_i = T$ – псевдослучайный символ, если совпадает. Расшифровка. Пусть E, K, M – массивы символов (байтов) в файле ввода (зашифрованная информация), в ключе и в файле вывода соответственно. Тогда $M_i = E_i$ xor K_i, если i не совпадает с каким-либо элементом последовательности, E_i игнорируется, если совпадает.

Таким образом, попытка узнать длину ключа путем циклического сдвига (первый шаг по взлому XOR) не осуществима из-за разных дистанций между a_i и a_{i+1}. Кроме того, при разработке утилиты особое внимание было уделено не только реализации данного алгоритма, но и распространению такого подхода на асинхронный алгоритм шифрования.

ИСПОЛЬЗОВАНИЕ КОДОВ ХЭММИНГА ДЛЯ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБОК В DWDM СЕТЯХ

Б.А. Монич

В системах оптических магистралей, которые работают на терабитных и мультигигабитных скоростях, используется уплотненного волнового мультиплексирования (DWDM). Алгоритм обнаружения и исправления ошибок методом кодов Хэмминга на DWDM транспортной системы Optix OSN 8800 компании Huawei был впервые опробован на одном из 10G каналов. В Республике Беларусь данная транспортная система также является частью сети передачи данных. Функции выявления ошибок реализуются на транспортировке в составе блока избыточной служебной информации, по которой смотрят степень достоверности принятой информации.

Для обнаружения ошибок разработаны и применяются различные алгоритмы. Среди них основными являются следующие.

1. Контроль по паритету. Представляет собой наиболее простой метод контроля данных. Метод заключается в суммировании по модулю 2 всех бит контролируемой информации. Существуют горизонтальный и вертикальный контроль по паритету.

2. Циклический избыточный контроль. Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. В качестве контрольной информации рассматривается остаток от деления этого числа на известный делитель R.

3. Вертикальный и горизонтальный контроль по паритету. Исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы.

4. Коды Хэмминга. Самостоятельно находят и исправляют ошибки, даже изолированные, то есть искаженные отдельные биты которые могут быть разделены большим количеством правильных битов.

Построение кодов Хэмминга основано на принципе проверки на четность числа единичных символов: к последовательности добавляется такой элемент, чтобы число единичных символов в получившейся последовательности было четным, ($S = 0$ – ошибок нет, $S = 1$ – однократная ошибка). Матрица преобразования соответствующей размерности умножается на матрицу-столбец кодового слова и каждый элемент полученной матрицы-столбца берется по модулю 2. На аппаратном уровне, в Optix OSN 8800, коды Хэмминга реализуются в модуле OTN tributary unit, на плате TN52TOG.

ИСПОЛЬЗОВАНИЕ ЖУРНАЛА ИЗМЕНЕНИЙ ФАЙЛОВ NTFS В КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

О.Р. Мысливец

При проведении компьютерно-технической экспертизы, а именно при анализе файловой системы NTFS, часто встает необходимость в поиске удаленных файлов и их анализе. Несмотря на то, что методы поиска удаленных файлов и их восстановления для файловой системы NTFS [1] не представляют особой сложности, не всегда возможно полностью восстановить файл для последующего анализа. В подобных случаях, если не удается восстановить файл полностью либо частично, существует возможность получить информацию о том, хранился ли файл в файловой системе в определенный промежуток времени и определить действия, проводимые над файлом. Информацию такого рода можно получить из журнала изменений файлов NTFS. Наряду с именами файлов и информацией об их MFT-записях, данный метафайл хранит в себе информацию о действиях, произведенных над файлами, а также временные метки произведенных действий [2]. С помощью данной информации можно однозначно установить факт хранения и использования некоторого файла, вплоть до получения полной последовательности произведенных над файлом действий за определенный промежуток времени. Недостатками данного подхода можно считать возможное отсутствие метафайла, вследствие его преднамеренного удаления или отключение опции журналирования для конкретного тома, а также ввиду ограничений на размер журнала изменений файлов, некоторые записи в журнале могут быть перезаписаны более новыми, что может повлиять на конечный результат. Несмотря на все недостатки данного подхода, в ходе исследований выяснилось, что в процессе анализа журнала изменений файлов NTFS существует вероятность получения информации о файлах, удаленных более 3 месяцев назад, но и не более 6 месяцев с момента удаления при условии активного использования накопителя информации.

Литература

1. Кэрриэ, Б. Криминалистический анализ файловых систем/ Кэрриэ Б. – СПб.: Питер, 2007. – 470 с.

2. USN_RECORD_V2 structure [Электронный ресурс] / Microsoft TechNet – Режим доступа: https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa365722(v=vs.85).aspx – Дата доступа: 17.05.2017.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ХРАНЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ БАЗЫ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Е.А. Нестерович, С.А. Зайкова

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в настоящее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных (СУБД), в особенности реляционные, стали доминирующим инструментом в этой области. Обеспечение информационной безопасности СУБД приобретает решающее

значение при выборе средства обеспечения необходимого уровня защиты для компании либо предприятия в целом. Организация защиты требует комплексного подхода и учета всех возможных коммуникационных каналов, обеспечение физической безопасности, шифрование резервных копий и информации, покидающей периметр компании, а также ряда организационных мероприятий. В работе проведен анализ предметной области, связанной с обеспечением безопасного хранения и защиты от несанкционированного доступа в базу данных, а также разработаны инструменты защиты базы данных в соответствии с требованиями к безопасности хранения и передачи данных. Спроектирована функциональная модель базы данных, предназначенная для хранения зашифрованных данных, введенных пользователем (на примере военного комиссариата Гродненской области). Решены следующие задачи: рассмотрены и проанализированы наиболее популярные уязвимости баз данных MySQL, спроектирована архитектура базы данных для специализированного программного обеспечения «Модуль социальной защиты ветеранов» военного комиссариата Гродненской области, разработан и испытан прототип приложения, произведена оценка его эффективности, даны рекомендации по организации обеспечения безопасного хранения и защиты информации от несанкционированного доступа.

Литература

1. Смирнов, С Безопасность систем баз данных / С. Смирнов. – Гелиос АРВ, 2007. – 352 с.
2. Шустова, Л. Базы данных / Л. Шустова, О. Тараканов. – М.: Инфра-М, 2016. – 304 с.

ПОВЫШЕНИЕ РАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ, ПОЛУЧАЕМЫХ ПРИ АЭРОКОСМИЧЕСКОМ МОНИТОРИНГЕ ЗЕМЛИ

П.М. Никуленко, В.Ю. Цветков, Д.Ю. Туча

В настоящее время все большую необходимость получают алгоритмы повышения разрешения изображений. Алгоритмы супер-разрешения позволяют повышать качество изображений, не затрагивая аппаратуру космических аппаратов. Супер-разрешение – технология, позволяющая повышать разрешающую способность изображений (способность передавать мелкие детали). Алгоритмы супер-разрешения основаны на получении дополнительной информации из каких-либо источников (копии снимков со смещениями и под другим ракурсом, база данных изображений). Супер-разрешение на основе обучающегося множества имеет преимущество над другими методами в виду того, что не требует модификаций съемочной аппаратуры, так как использует информацию, хранящуюся в базе данных при наземной обработке. Основной принцип предлагаемого алгоритма заключается в нахождении среди изображений базы данных наиболее схожих и подходящих высоких частот для построения повышенного разрешения. Результат повышения детализации будет зависеть от того, насколько большое количество высокочастотных участков будет находиться в базе снимков, при этом даже при небольшой степени сходства четкость изображений будет увеличиваться в виду наложения слоя высоких частот, а возможные ошибки будут корректироваться степенью их прозрачности. Главной проблемой алгоритма является уменьшение ошибок при повышении разрешения, для этого применяется автоматическая коррекция прозрачности накладываемых частот, исходя из степени сходства изучаемых участков. Также существует необходимость развития алгоритма по принципу нейронных сетей, для автоматической выборки из обрабатываемых изображений недостающих в базе высокочастотных участков и последующего накопления их.

УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ МОНИТОРИНГА ГИДРОЛОГИЧЕСКОГО РЕЖИМА ВОДНЫХ ОБЪЕКТОВ

Е.В. Новиков, Д.А. Мельниченко

Для мониторинга состояния и прогнозирования динамики гидрологического режима водных объектов широко используются данные дистанционного зондирования Земли. Специализированный распределенный сетевой программный комплекс мониторинга русловых процессов и гидрологического режима рек с использованием таких данных в качестве

информационной основы использует банк цифровых карт, космических и аэрофотоснимков и предполагает решение целого ряда отдельных задач, связанных, прежде всего, с защитой окружающей среды. При этом задачи могут использовать одни и те же исходные снимки, но, однако, резко отличаются по сфере применения, кругу пользователей, требуемому наполнению цифровых карт.

В связи с этим при реализации комплекса возникает ряд проблем, связанных с защитой информации и управлением доступом к ней. Для решения этих проблем комплекс включает, кроме модуля управления входными данными и модулей расчета отдельных характеристик водных объектов, модуль администрирования банка данных. Последний обеспечивает ведение базы метаданных, выбор форматов хранения файлов, видов объектов на формируемых тематических картах, группировку пользователей с назначением им прав доступа к данным и действиям. Особенностью комплекса является использование для обращения к банку данных и расчетных модулей web-интерфейса, автоматически настраиваемого в соответствии с группой, в которую включен пользователь, с сокрытием всех элементов управления и информационных панелей, не относящихся к решаемой этим пользователем задаче.

СЖАТИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ КОДИРОВАНИЯ ДЛИН СЕРИЙ

В.А. Панас

Предлагается алгоритм сжатия изображения на основе кодирования длин серий. На первом этапе алгоритма происходит разложение исходного изображения на битовые плоскости. Это позволяет сократить диапазон значений пикселей и увеличить число серий из повторяющихся пикселей. На втором этапе происходит выбор оптимальной битовой длины блока данных для каждой плоскости. Таким образом предотвращается нерациональное использование старших битовых разрядов блока данных, имеющее место в классическом алгоритме [1]. После этого следует этап кодирования длин серий, после чего все закодированные данные объединяются с помощью мультиплексирования. Процедура сжатия не применяется к младшим битовым плоскостям. Это обусловлено тем, что младшие плоскости представлены в виде шумов, а семантическая информация появляется на старших битовых плоскостях. Количество сжимаемых плоскостей варьируется для каждого изображения. Предлагаемый алгоритм обеспечивает более высокую степень сжатия, чем классический алгоритм RLE и не уступает ему во времени выполнения [2]. Схема сжатия нового алгоритма изменяется в зависимости от характера изображения. Это позволяет получать для каждого изображения оптимальные коэффициенты сжатия. Алгоритм может найти применение в системах резервного копирования данных, которые являются одним из средств защиты информации.

Литература

1. Сэломон, М. Сжатие данных, изображений и звука / М. Сэломон. – М. : Техносфера, 2004. – 368 с.

2. Сжатие полутоновых изображений без потерь на основе кодирования длин серий / Аль-Бахдили Х.К [и др.] // Доклады БГУИР. – 2016. – № 2. – С. 63–69.

ДИНАМИЧЕСКАЯ РЕКОНФИГУРАЦИЯ СЕРВИСОВ ОБЛАЧНЫХ СИСТЕМ

М.П. Ревотюк, О.В. Кот

Задача динамической реконфигурации сервисов облачных систем по узлам глобальной сети возникает в случаях необходимости обеспечения гарантированной производительности или реактивности отклика системы обслуживания в условиях ограниченной пропускной способности коммуникаций. Миграция сервиса, его репликация и активизация технически возможна в любой момент времени в рамках альтернатив размещения серверов и порталов. Этот процесс может быть синхронизирован со временем посредством кусочно-линейной аппроксимации интенсивностей запросов клиентов порталов с привязкой к часовым поясам.

Формально модель обслуживания может быть представлена как динамическая задача размещения транспортного типа с ограничением пропускной способности: задано множество мест

размещения серверов сервисов, множество мест размещения порталов и матрица пропускной способности; известна производительность серверов и объем трафика каждого из порталов на каждом интервале времени; необходимо выбрать подмножество мест размещения серверов сервисов с назначением приоритета обслуживания порталов при условии баланса производительности и объема трафика. Рассматриваемая задача может быть решена перебором с отсечениями среди множества классических задач Хичкока для всех сочетаний узлов размещения серверов сервисов среди возможных мест на каждом интервале времени. Порождение сочетаний методом вращающейся двери с единичным расстоянием Хэмминга между соседними сочетаниями позволяет заменить полный цикл решения очередной транспортной задачи анализом последствий изменения единственной строки матрицы предыдущей задачи. Используя метод потенциалов[1], удается снизить на порядок вычислительную сложность такого анализа на порядок, а также досрочно прерывать решение задачи для бесперспективного варианта размещения.

Литература

1. Ревотюк, М.П. Реоптимизация решения транспортных задач Хичкока методом потенциалов / М.П. Ревотюк, П.М. Батура, А.М. Полоневич // Доклады БГУИР. – 2010. – № 7(53). – С. 89–96.

АЛГОРИТМЫ КООРДИНАЦИИ СИСТЕМ АГЕНТОВ

М.П. Ревотюк, А.К. Пушкина

Задачи оптимизации управления системами взаимодействующих агентов в общем случае формулируются в терминах задач о динамическом назначении[1]. В процессе координации таких систем необходимо регулярно решать задачу о назначении свободным агентам возникающих задач 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.

Предлагается учесть дискретность процесса формирования портфеля заявок, явно используя понятия наиболее раннего и позднего срока начала решения задачи для жадного упреждающего поиска окончательного назначения. Так как процедура назначения дополняет граф оптимального паросочетания при поступлении новых заявок, то задержка времени определяется сложностью обработки последней группы заявок. Реализация предлагаемой схемы 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. A Comprehensive Taxonomy for Multi-Robot Task Allocation/G.A. Korsah, M.B. Dias, A. Stentz [Electronic resource]. – Mode of access: http://ashesi.org/wp-content/uploads/2016/03/G.-Ayorkor-Korsah.pdf. – Date of access: 24.02.2016.

СИСТЕМА ЗАЩИТЫ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ МИКРОКОМПЬЮТЕРА RASPBERRY PI

О.Ю. Рыжко, С.А. Зайкова

На сегодняшний день автоматизированные системы являются основой обеспечения большинства бизнес-процессов, как в коммерческих, так и в государственных организациях. Вместе с тем, повсеместное использование автоматизированных систем для хранения, обработки и передачи информации приводит к обострению проблем, связанных с их защитой. Считается, что одной из наиболее опасных угроз является утечка хранящейся и обрабатываемой внутри автоматизированной системы конфиденциальной информации. Все это обуславливает необходимость пристального рассмотрения эффективных способов защиты от

утечки конфиденциальной и корпоративной информации. Защита требует комплексного подхода и учета всех возможных коммуникационных каналов, обеспечение физической безопасности, шифрование резервных копий и информации, покидающей периметр, а также ряда организационных мероприятий. В работе предложено разработать программный модуль анализа сетевого трафика и, таким образом, модифицировать комплексную защиту системы, ее информационную безопасность, предотвратить несанкционированное распространение конфиденциальной информации (на примере филиала ООО "ЮНЛ Солюшнс" г.Гродно). Решены следующие задачи: изучены основные понятия систем предотвращения утечки информации; проанализированы методы анализа информации на предмет содержания конфиденциальных данных; разработан программный модуль анализа информации на языке программирования Ruby; разработана веб-панель управления (с использованием фреймворка Ruby on Rails); развернута система на базе микрокомпьютера Raspberry Pi; проанализирована эффективность программно-аппаратного модуля; даны рекомендации по поддержке, развитию и оптимизации системы защиты от утечек конфиденциальной информации.

Литература

1. Ищейнов, В Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учеб. пособие / В. Ищейнов, М. Мецатунян. – М.: Высшее образование, 2014. – 256 с.

2. Росенко, А Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование / А. Росенко. – Красанд, 2010. – 160 с.

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ДЛЯ ИСПОЛЬЗОВАНИЯ СТЕГАНОКОНТЕЙНЕРОВ В АУДИОФАЙЛАХ

И.А. Сазановец

В докладе представлены исследования автора, отражающие возможности передачи скрытых данных в аудиофайлах, возможность модификации аудосигнала, а также передачи скрытых данных в текстовых компонентах аудиофайла. Стеганография в звуковых файлах может применяться для внедрения цифровых отпечатков, водяных знаков и как инструмент скрытой передачи данных. Все звуковые файлы можно рассматривать во временной или же в частотной области. Для перехода из временной в частотную область используется дискретное преобразование Фурье.

Во временной плоскости работают методы наименьшего значащего бита и кодирования с помощью бита четности. В частотной плоскости работают методы фазового кодирования, эхо кодирования, кодирования с помощью расширения спектра и кодирования с помощью высокочастотного шума.

Методы, работающие в частотной области, не позволяют скрыть большой объем информации, поэтому они больше подходят для внедрения цифровых отпечатков или водяных знаков. Метод наименьшего значащего бита позволяет скрыть значительно больше информации, но при его реализации могут наблюдаться следующие уязвимости: запись бит в промежутки тишины (в звуковых файлах тишина кодируется нулями), левый и правый каналы в стереофайле могут быть побитно одинаковыми и отсутствие шифрования (кроме того, что исходное сообщение шифруется, шифрование усложняет стеганоанализ). Также метод наименьшего значащего бита подвержен статистическому анализу. Также в докладе представлены методы сокрытия данных в метаинформации звуковых контейнеров.

СРАВНЕНИЕ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ СТБ 34.101.45-2013 С РАЗДЕЛЕННЫМ СЕКРЕТОМ ПРИ ИСПОЛЬЗОВАНИИ АЛГОРИТМОВ ХЭШИРОВАНИЯ SHA-2 И SHA-3

С.Б. Саломатин, О.А. Селеня

Использование электронно-цифровой подписи для защиты электронного документооборота предполагает надежность всех алгоритмов в ее составе. В основе любой цифровой подписи лежит алгоритм хэширования для обеспечения существенного изменения конечного значения подписи если подписанный документ при передаче подвергся даже

небольшому изменению. На сегодняшний день самой новым, а значит и самым безопасным считается алгоритм хэширования SHA-3[1]. Его введение было обусловлено нахождением коллизий в семействе алгоритмов SHA-2 индийскими исследователями в 2008 году. Для исследования ЭЦП с использованием этих алгоритмов был применен ряд статистических тестов, опубликованных NIST. За основу была взята модифицированная схема ЭЦП СТБ 34.101.45-2013 с разделенным секретом[2]. Результаты статистических тестов выявили следующее: оба алгоритма прошли тесты с заданным показателем α=0.01, что говорит о том, что обе последовательности носят случайных характер. По результатам побитового теста алгоритм SHA-3 отклоняется от идеального распределения, в то время как SHA-2 показывает близкие к идеалу результаты. Остальные тесты алгоритм с SHA-3 прошел с большей вероятностью, чем его аналог и проявил хорошие показатели по устойчивости, производительности и безопасности. Недостатки SHA-3 из результатов тестирования можно обосновать недостаточной оптимизацией, чем он уступает более ранним версиям, построенным на встроенных библиотеках.

Литература

1. José Luis Gómez Pardo, Carlos Gómez-Rodríguez The SHA-3 family of hash functions and their use for message authentication. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://goo.gl/Cd1hme. – Дата доступа: 19.05.2017.

2. Селеня, О.А. Реализация пороговой схемы электронной цифровой подписи с разделенным секретом на основе СТБ 34.101.45-2013 / О.А. Селеня. – Молодежный сборник научных статей «Научные стремления». 2016. – Вып. № 18. – С. 11–14.

ОЦЕНКА ПРИМЕНИМОСТИ ЭМПИРИЧЕСКИХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ДЛЯ АНАЛИЗА ЭЛЕКТРОМАГНИТНОЙ БЕЗОПАСНОСТИ СЕТЕЙ СОТОВОЙ СВЯЗИ С МИКРОСОТОВОЙ СТРУКТУРОЙ В ГОРОДСКОЙ ЗАСТРОЙКЕ

А.С. Свистунов

В связи с массовым охватом населения услугами беспроводной связи, сопровождающимся увеличением количества абонентских устройств (АУ) на городской территории и базовых станций (БС) для их обслуживания, наблюдается тенденция уменьшения размеров сайтов сетей сотовой связи до размеров в несколько сотен метров. Проведение анализа электромагнитной безопасности сотовых радиосетей для населения связано с применением моделей условий распространения радиоволн (РРВ) между БС и АУ для определения уровня полезного сигнала. Однако широко используемые эмпирические модели условий распространения радиоволн (РРВ), как правило, определены для расстояний между БС и АУ не менее 1 км и для ограниченной полосы радиочастот, поэтому необходима дополнительная оценка возможности их использования для малых размеров сайтов, характерных для городских сотовых сетей с микросотовой структурой. Для этого выполнено моделирование условий РРВ на расстоянии 0,1…1 км с использованием трехмерного алгоритма РРВ и трехмерной модели участка типовой городской застройки с высотой зданий 6-20 м при размещении АУ вне зданий на земной поверхности, а также выполнено сравнение оценок уровней входного сигнала, полученных с помощью эмпирических моделей (Окамура-Хата, COST231-Хата, COST231-Уолфиш-Икегами, Ли, Эриксон) и трехмерной многолучевой модели РРВ. Результаты оценок уровня сигнала, в наибольшей степени совпадающие с результатами, полученными с помощью трехмерной модели РРВ на рассматриваемой территории городской застройки, могут быть получены с помощью моделей условий РРВ Окамура-Хата, COST231-Хата и COST231-Уолфиш-Икегами; модели Окамура-Хата и COST231-Hata могут быть применены для расстояний между БС и АУ 0,4…1 км.

АКТУАЛЬНАЯ ПРОБЛЕМА БЕЗОПАСНОСТИ xPON

Н.Н. Сергеев, В.Н. Урядов

Наиболее серьезным недостатком xPON является незащищенность обратного канала от действий злоумышленников. На физическом уровне неисправность лазера обратного канала или контроллера этого лазера может вывести из строя всю систему. Такие случаи отслеживаются системами управления терминала. Однако, используя оптическую розетку

(ОРА), а доступ к ней получить весьма легко, злоумышленник так же может вывести из строя весь сегмент сети, путем примитивного засвета лазером в линию. Это произойдет в том случае, когда мощность излучаемого в линию сигнала превысит допустимую мощность фотодиода OLT. В xPON используется принцим временного разделения TDM [1], поэтому очевидно, что злоумышленник после некоторых манипуляций с перепрограммированием ONT или подключением ПК с установленным специальным программным обеспечением к ONT может добиться того, что будет получать информацию, адресованную другим пользователям, всего лишь подобрав необходимый интервал. Это можно сделать с каждой оптической розетки (ОРА). Снятие информации нисходящего потока достаточно просто реализуемо, поскольку обычный приемник обеспечивает прием сигнал любого приемника, если использовать другой временной интервал. Более сложна в реализации снятия информации контролируемого абонента с другой абонентской розетки поскольку используется отраженный сигнал от ответвителя или разъемного соединения [2] При использовании отраженного сигнала, необходимо учесть, что в пассивной оптической сети существуют возвратные потери в неоднородностях.

Литература

1. Урядов В.Н., Бунас В.Ю., Глущенко Д.В // Докл. БГУИР. 2012. № 8 (70). С. 81–87.
2. Булавкин И.А. // Технологии и средства связи. 2006. IW2. С. 104–108.

СНЯТИЕ ИНФОРМАЦИИ НИСХОДЯЩЕГО ПОТОКА В ПАССИВНОЙ ОПТИЧЕСКОЙ СЕТИ

Н.Н. Сергеев, В.Н. Урядов

Снятие информации нисходящего потока в пассивных оптических сетях достаточно просто реализуемо, поскольку обычный приемник обеспечивает прием сигнал любого приемника, если использовать другой временной интервал. Более сложна в реализации снятия информации контролируемого абонента с другой абонентской розетки поскольку используется отраженный сигнал от ответвителя или разъемного соединения. В случае передачи информации от ONT-1 к ONT-2 затухание будет весомым, а затухание сигнала на стыках и затухание сигнала в разъемном соединении будут небольшими. Возвратные потери определяют долю оптической мощности, которая возвращается обратно к источнику оптического сигнала. Основным фактором, определяющим возвратные потери, являются многократные френелевские отражения. С этой позиции разветвитель характеризуется затуханием на ближнем конце 50 дБ [1]. Квантовый предел детектирования определяется шумами, связанными с сигналами. Падающий на фотодиод стационарный световой поток генерирует пары носителей заряда как независимые случайные события» Такой процесс преобразования фотонов называется пуассоновским [2]. Таким образом, для того чтобы воспользоваться отраженным сигналом и снять информацию абонента с другой соседней оптической розетки, достаточно, чтобы величина отраженного сигнала была в рамках квантового предела детектируемости [3].

Литература

1. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей.
2. Птицын Г.А. Живучесть динамических сетей телекоммуникаций. М.: МТУСИ. 2008. 48 с.
3. Урядов В.Н., Глущенко Д.В. // Современные средства связи : матер. XIV Междунар. науч.-техн. конф. Минск, 29 сент.–1 окт. 2009 г. С. 23.

ДВУМЕРНЫЕ ХАОТИЧЕСКИЕ ОТОБРАЖЕНИЯ В АЛГОРИТМАХ ХЕШИРОВАНИЯ

А.В. Сидоренко, И.В. Шакинко

На современном этапе развития информационных технологий особое место занимают вопросы, связанные с обеспечением безопасности передаваемых данных. Одной из ключевых задач информационной безопасности является контроль целостности данных. Для обеспечения контроля целостности данных традиционно используются алгоритмы хеширования [1]. Эти

алгоритмы позволяют поставить в соответствие данным произвольного размера последовательность бит фиксированного размера, называемую хеш-значением. На основе результата сравнения хеш-значений, вычисленных для исходного и полученного сообщений, делается вывод о том, было ли сообщение модифицировано при его передаче по каналу связи.

В данной работе предложен алгоритм хеширования, основанный на использовании двумерных дискретных хаотических отображений [2]. Применение дискретных хаотических отображений позволяет сократить вычислительные затраты, необходимые на формирование хеш-значения. Предлагаемый алгоритм хеширования включает в себя следующие этапы: реализация итераций хаотических отображений с добавлением к переменным отображений элементов исходного сообщения и реализация итераций хаотических отображений без добавления элементов исходного сообщения. Проведено тестирование предлагаемого алгоритма при использовании следующих дискретных хаотических отображений: отображение «Кот Арнольда», отображение Чирикова, отображение пекаря. Установлено, что при использовании отображений Чирикова и пекаря для предлагаемого алгоритма характерен лавинный эффект, однако, при использовании отображения «Кот Арнольда» лавинный эффект отсутствует. Результаты анализа времени формирования хеш-значения свидетельствует о том, что для сообщений с размером большим 32 Кб предлагаемый алгоритм оказывается быстрее алгоритма «Keccak» более чем на 20 %.

Таким образом, предлагаемый алгоритм хеширования при использовании отображений Чирикова и пекаря может применяться при решении задач, связанных с контролем целостности данных при их передаче по различным каналам связи.

Литература

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

2. Wong, K. Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al] – Berlin, 2009. – Ch. 16. – P. 333–354.

ИСПОЛЬЗОВАНИЕ СЕРВИСА CLOUDFLARE ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Г.И. Сидорин, Е.С. Кайгородова

С ростом количества и популярности веб-приложений остро встает вопрос обеспечения безопасности данных пользователей и их постоянной доступности. Необходимо, чтобы из любой точки планеты из любого устройства, поддерживающего соединение с интернетом, была возможность получить данные, при этом они должны быть надежно защищены от злоумышленников. Создание полноценной инфраструктуры для защиты содержимого веб-приложения, их масштабирования – это длительный и дорогостоящий процесс, требующий усилий и знаний гораздо больших, чем реализация основного функционала сервиса. Были проведены исследования по обеспечению безопасности с помощью облачных веб-сервисов. Наилучшие результаты по простоте использования, эффективности и стоимости показал сервис Cloudflare. Он предоставляет глобальную сеть доставки контента (CDN) с возможностями кеширования статического, ускорения динамического и оптимизации исходящего контента в зависимости от устройств, браузеров и пропускной способности. Благодаря этому веб-приложения отвечают пользователям максимально быстро, в какой точке планеты они бы ни находились. Также он предлагает бесплатную защиту SSL для шифрования веб-трафика в целях предотвращения кражи данных, повышения скорости загрузки веб-приложений и лучшей индексацией поисковыми движками. Атаки типа отказ в обслуживании (DoS) не являются недавним явлением, но методы и ресурсы, доступные для проведения и маскирования таких атак, резко эволюционировали. Cloudflare является одной из крупнейших сетей защиты от DDoS-атак в мире. С помощью его можно успешно бороться с атаками размером более 400 Гбит/с. Сервис предлагает бесплатные серверы доменных имен (DNS), которые являются одними из самых быстрых в мире. Cloudflare работает как обратный прокси-сервер и поддерживает множество новых протоколов: SPDY, HTTP/2, Websocket. Полученные результаты показывают целесообразность использования сервиса Cloudflare для обеспечения безопасности данных и отказоустойчивости веб-приложений. Такой способ особенно подойдет небольшим и средним веб-приложениям.

АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

В.О. Сидорович, А.Е. Варюшина

Практика построения современных СПИ показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений различных источников информации по общей линии связи [1].

В многоканальной СПИ по общему высоко-частотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется уплотнением каналов. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют поднесущими колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется разделением (селекцией) каналов [2].

Литература

1. Принципы многоканальной передачи информации. Элементы теории разделения сигналов [Электронный ресурс]. – 2011. – Режим доступа : http://studopedia.org/8-106652.html – Дата доступа: 26.01.2017.

2. Уплотнение информации в аналоговых системах связи [Электронный ресурс]. – 2017. – Режим доступа: http://studopedia.org/2-74270.html – Дата доступа: 11.03.2017.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИЗАЦИИ ЗДАНИЙ

Д.С. Смоляк, Т.А. Пулко

Одним из частных случаев интернет вещей (физических предметов) (IoT) являются системы автоматизации зданий, такие как системы домашней автоматизации «умный дом», позволяющие автоматизировать ряд рутинных задач и обеспечить контроль и мониторинг использования ресурсов, а также обеспечить владельцу возможность удаленного управления. При построении систем типа «умный дом», рассчитанных на широкого потребителя используются решения, использующие беспроводные протоколы передачи данных. Большое распространение на текущий момент времени получают системы, использующие беспроводные протоколы передачи данных на не лицензируемых радиочастотах, позволяющие использовать оборудование для реализации решения без дополнительных согласований, такие как ZigBee и Z-Wave. В Республике Беларусь телекоммуникационная компания Белтелеком в своей услуге «Умный дом» предлагает решения, рассчитанные на массового потребителя и основанные на беспроводном протоколе ZigBee [1]. Однако, использование беспроводных решений влечет за собой ряд угроз для потенциального потребителя. Например, исследователи из компании Qihoo360 обнаружили возможность перехвата ключей шифрования сетевых сообщений для ряда устройств [2]. Исследователями Eyal Ronen, Colin O'Flynn были обнаружены уязвимости в продукте Philips Hue, позволяющие загрузить вредоносное программное обеспечение в «умную лампочку» [3]. Таким образом, в связи с ростом применения продуктов IoT, следует подвергнуть критической оценке, представленные на рынке решения, оценить уровень их защищенности к различным атакам, а также повысить осведомленность потребителей о возможных последствиях использования небезопасных решений.

Литература

1. Умный дом. [Электронный ресурс]. – Режим доступа: http://beltelecom.by/umnyi-dom.
2. Researchers exploit ZigBee security flaws that compromise security of smart homes. [Электронный ресурс]. – Режим доступа: http://beltelecom.by/umnyi-dom.
3. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. [Электронный ресурс]. – Режим доступа: http://iotworm.eyalro.net.

АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ НА ПЛАТФОРМЕ IOS

Д.В. Судас

В данном докладе рассматриваются преимущества применения атоматизированных тестов при тестировании мобильного приложения. Технологии, используемые при создании автоматизированных тестов, а также процессы, задействуемые для обеспечения качества тестируемого приложения. При создании автоматизированных тестов используется язык программирования Ruby, фреймворк Selenium и Appium. Используется среда разработки Intellij RubyMine для написания кода для тестовых скриптов. Для сокращения времени тестирования, для увеличения эффективности тестирования используются автоматизированные тесты, написанные командой разработчиков. В дальнейшем их использование позволяет повысить качество выпускаемого программного продукта.

ОПЫТ ПРИМЕНЕНИЯ IDS/IPS-СИСТЕМЫ SURICATA В ВЫЧИСЛИТЕЛЬНОЙ СЕТИ МАЛОГО ПРЕДПРИЯТИЯ

Т.О. Титовец, Е.В. Моженкова

IDS/IPS-системы в зависимости от их целевого назначения делятся на системы обнаружения вторжений (IDS, Intrusion Detection System) и системы предотвращения вторжений (IPS, Intrusion Prevention System) [1]. Продукты для решения задач информационной безопасности часто интегрируют внутри себя оба этих подхода.

Применение больших корпоративных систем сетевой защиты не всегда целесообразно, т.к. требует значительных финансовых затрат или реорганизации текущей инфраструктуры предприятия, что так же приводит к дополнительным расходам. Для экономии бюджета предприятия взамен данных систем можно применить бесплатную IDS/IPS-систему Suricata. Suricata – это сетевая система защиты, которая работает в многопоточном режиме, позволяющем оптимально использовать несколько CPU, содержит развитые средства инспектирования HTTP-трафика и контроля приложений [2]. В докладе обсуждается опыт применения IDS/IPS-системы Suricata в вычислительной сети малого предприятия (число сотрудников – 80, число компьютеров – 60). Для возможности функционирования работы Suricata была установлена система на базе Linux с актуальной версией Java 8 и большим количеством CPU и RAM. Проводится анализ инцидентов, обнаруженных с помощью Suricata.

Литература

1. Zuech, R. Intrusion detection and big heterogeneous data: a survey / R. Zuech, T.M. Khoshgoftaar, R. Wald // Journal of Big Data. – 2015.
2. Применение IDS/IPS [Электронный ресурс]. – Режим доступа https://xakep.ru/2012/10/29/ids-ips//. – Дата доступа: 14.05.2017.

МЕХАНИЗМ ОПРЕДЕЛЕНИЯ ВЕРОЯТНЫХ СЦЕНАРИЕВ АТАКИ ИНСАЙДЕРА НА ИНФРАСТРУКТУРУ ИНФОРМАЦИОННОЙ СИСТЕМЫ

А.В. Федорцов

Возникающие в различных информационных системах организаций инциденты информационной безопасности в большинстве случаев следует рассматривать как результат атаки инсайдера. Комплексное тестирование программно-технических средств перед их выпуском на конечном этапе разработки, а также своевременное их обслуживание

(обновление) в целом сводят к минимуму число вышеуказанных инцидентов по причине низкой надежности (нестабильной работы, абсолютных отказов) непосредственно элементов инфраструктуры самой организации. Вместе с тем наличие неизвестных до настоящего времени разработчикам уязвимостей программно-технических средств в совокупности с другими складывающимися в организациях условиями [1] приводят к негативным событиям после осуществления пользователем инфраструктуры злоумышленных и (или) не злоумышленных действий в информационной системе.

При определении вероятных сценариев атаки инсайдера на программно-технические средства информационной системы необходимо исходить из технически реализуемых (допустимых) действий в каждой конкретной ситуации, характеризующейся устойчивыми связями между такими составляющими как: цель (-и) атаки, объект (-ы) атаки, уязвимости программно-технических элементов инфраструктуры, сложившиеся условия и имеющиеся при этом у инсайдера возможности, а также его характеристика. Все потенциальные сценарии атак с участием самого инсайдера целесообразно разделять на три группы: без использования программно-технических средств; с использованием программно-технических средств; «гибридные» сценарии – комбинация действий и используемых программно-технических средств, свойственных сценариям из первых двух групп. В специфическую группу также следует выделять вредоносное программное обеспечение, которое способно осуществлять атаку (а точнее «кибератаку») по определенному сценарию заранее неизвестного злоумышленника, но от имени какого-либо другого пользователя.

Предложенный механизм позволяет формировать базовые наборы вариантов последовательности осуществления атак инсайдерами и впоследствии сопоставлять их с результатами воздействий (нанесенным либо предполагаемым ущербом элементам инфраструктуры информационной системы) для построения «дерева» событий, приводящих к возникновению инцидентов информационной безопасности.

Литература

1. Федорцов, А.В. Анализ условий для реализации атак внутренними нарушителями на программно-технические средства защиты информации / А.В. Федорцов // Тез. доклад. 53-й научн. конф. аспир., магистр. и студ. БГУИР, Минск, 02–06 мая 2017 г. – Минск, БГУИР, 2017.

ЗАЩИТА ИНФОРМАЦИИ В ВЕБ-ПРИЛОЖЕНИИ ДЛЯ ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ПОЛУЧЕНИЕ РАЗРЕШЕНИЯ ДЛЯ ПРОЕЗДА ТЯЖЕЛОВЕСНЫХ ТРАНСПОРТНЫХ СРЕДСТВ ПО АВТОМОБИЛЬНЫМ ДОРОГАМ

Е.И. Шалимо

Рассматривается защита информации в относительно новом веб-приложении для электронной подачи заявления автоперевозчиком для получения специального разрешения на проезд тяжеловесных и (или) крупногабаритных транспортных средств автоперевозчика по автомобильным дорогам республики. Наличие у автоперевозчика названного разрешения на проезд регламентировано Постановлением Минтранса РБ от 10 июля 2012 г. № 33 Помимо электронной подачи заявления веб-приложение предоставляет следующие возможности: 1) автоматизированное оформление специального разрешения по данным электронной заявки, включая проверку соответствия нагрузок и габаритов транспортных средств установленным нормативам, в том числе в период сезонных ограничений; 2) ведение электронного реестра поступивших заявлений с текущей информацией о состоянии (рассмотрено, сделан расчет, сделано техническое заключение, не востребовано, оплата расчета); 3) проверка поступившей платы по выданным расчетам платы.

Эксплуатация в течение последних трех лет новых обновленных релизов веб-приложения показала, что, несмотря на принятые меры по защите информации, инциденты, связанные информационной безопасностью, в новых релизах редко, но все-таки случаются. Эти инциденты относятся к известным проблемам информационной безопасности систем электронного документооборота (например, недостаточной криптозащите электронной подписи), а также к известным уязвимостям веб-приложений. В докладе анализируются принятые и принимаемые меры по сокращению числа вышеназанных инцидентов.

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ МОДЕЛИ ЛОРЕНЦА

А.М. Ярук, Н.Г. Киевец

В криптографической области важным предметом для изучения и усовершенствования являются генераторы случайных чисел (ГСЧ), которые должны формировать надежные ключи.

Конструкция и технология ГСЧ должна позволить формировать непредсказуемые последовательности чисел на его выходе. Помимо этого, к ним предъявляются следующие требования: выходной поток битовой последовательности чисел должен соответствовать статистическим критериям случайности; следующий бит последовательности чисел должен быть случайным (неопределенным); должна быть исключена возможность воспроизведения одного и того же битового потока последовательности случайных чисел.

Рассматривается формирование случайных чисел с помощью ГСЧ, в состав которого входит блок, построенный на основе хаоса. Блок относится к диссипативным динамическим системам, в которых хаос обусловлен наличием странных аттракторов [1]. Примерами таких реализаций являются: входной источник шума и дискретизация с использованием двух генераторов с джиттером, хаотические генераторы с дискретным и непрерывным временем.

В основе ГСЧ лежит физическая случайность, энтропия которой увеличивается благодаря использованию блока, построенного на основе хаоса. Таким образом, начальными условиями для работы блока динамического хаоса служит физическая случайность. Это приводит к возникновению сложной системы: при изменении начальных условий системы образуется эрготичность (хаос) значений.

Реализация ГСЧ выполнена с использованием хаотического генератора на основе модели Лоренца, математически описываемой тремя дифференциальными уравнениями первого порядка. При этом в ГСЧ устанавливается хаотический режим с непрерывными случайными числами на выходе. Показано, что использование рассмотренного ГСЧ улучшает процесс случайности и непредсказуемости результата.

Литература

1. Кузнецов С.П., Динамический хаос / С.П. Кузнецов. – М: Физматлит, 2001.

СЕКЦИЯ 4
ЭЛЕМЕНТЫ И КОМПОНЕНТЫ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

FLEXIBLE ELECTROMAGNETIC RADIATION SHIELDS OBTAINED BY CHEMICAL DEPOSITION OF COPPER ON THE SURFACE OF A FABRIC WITH A NANOSTRUCTURED FERROMAGNETIC MICROWIRE

A.A.A. Ahmed, Y.T.A. Al-Ademi, A.S.J. Alkalbi, A.M. Prudnik

The samples of the fabrics with the ferromagnetic nanostructured microwire produced by Central Scientific Research Institute for Complex Automation of Light Industry (Moscow, Russia). The composition of the amorphous nanostructured microwire in glass insulation is a ferromagnetic alloy of Fe, Co, Ni and metalloids (B, Si, C). Its content was changed by alternating the weft threads with the microwire. The first sample was without microwire, the second sample was with the alternation of weft threads and microwire at 1:2 ratio; the third sample was with the alternation of weft threads with the microwire at 1:3 ratio and the fourth sample was with the alternation of weft threads with the microwire at 1:4 ratio. The investigation of the characteristics of attenuation and reflection of electromagnetic radiation by such samples was carried out in the frequency range 0.7–17 GHz.

The attenuation by the samples without magnetic particles was close to zero. The attenuation of samples with different quantities of a ferromagnetic microwire is 2…8 dB in the frequency range 2–17 GHz. The reflection coefficient of the samples radiation with different quantities of a microwire was –10…–5 dB in the range 3…12 GHz. While using a metal substrate placed behind the sample, there is a significant increase in the radiation (above 40 dB), which is due to the high (up to 99 %) reflectivity of the metal. At the same time, the change in the reflection coefficient of the radiation samples is up to –10…0 dB in the range 5…14 GHz.

These dependences are explained by the influence of the electromagnetic radiation interaction with the material of the microwire contained in the cotton polyester fabric. At the same time, the mass of the microwire and its shape affect the frequency dependence of the reflection coefficient in the range 2…17 GHz negatively. The chemical deposition of copper on the surface of the fabric fibers was carried out from an aqueous solution containing potassium sodium tartrate, copper sulfate (crystalline hydrate), sodium hydroxide. Formalin with the concentration of 40% was used as a reducing agent. The fabric was placed in this solution, kept in it, then it was washed, dried and stabilized on its surface by clusters of precipitated copper.

It was shown that the reflection coefficient of the fabric is –5…–6.5 dB at the radiation transmission coefficient of –5.5…–7 dB in the range 8…12 GHz. The chemical deposition of copper from an aqueous solution onto the surface of fibers of such a fabric results in decreasing of its reflection coefficient by 0.1…1.1 dB in the range of 8…12 GHz, and in decreasing of its transmission coefficient by 0.2…1.6 dB in the range 8…10 GHz and in increasing this parameter by 0.1…0.8 dB in the range 10…12 GHz.

It was shown that the values of the reflection coefficient of the fabric fixed on the metal substrate are –0.4…–1.2 dB in the range 8....12 GHz. The reflection coefficient of the fabric fixed to the metal substrate after the chemical deposition of copper from aqueous solutions onto the surface of its fibers are reduced by 4…6 dB. Decreasing in this parameter may be caused by the effect of interference damping of antiphase electromagnetic waves reflected from the surfaces of the fabric and the metal substrate.

INFLUENCE OF CHEMICAL COPPERPLATING OF TISSUE WITH NANOSTRUCTURED FERROMAGNETIC MICROWAVE ON ITS COMPOSITION

A.A.A. Ahmed, Y.T.A. Al-Ademi, A.S.J. Alkalbi, O.V. Boiprav

The tissue with a nanostructured ferromagnetic microwire is characterized by the reflection and transmission coefficients of electromagnetic radiation in the frequency range 8…12 GHz of –5…–6 dB (at a thickness of less than 1 mm), which is due to the presence of silicon oxides (SiO_2, Si_5O_{10}), brucites ($D_{1,988}MgO_2$, MgH_2O_2), as well as iron niobate (F_6FeNb), characterized by magnetic properties. This determines its application in order to create flexible screens intended for electromagnetic shielding of areas of space in which radio electronic equipment is located.

In order to reduce the values of the transmission coefficient of electromagnetic radiation of such a tissue, its modification is performed by copper plating (including additional conductive components). It was carried out from an aqueous solution containing potassium sodium tartrate, copper sulfate (crystalline hydrate), caustic soda. As a reducing agent, formalin was used, whose concentration is 40 %.

Analysis of X-ray spectrograms of modified tissue showed the presence of copper precipitates on the surface of its fibers. To determine the appearance and composition of the surface of the initial and modified tissues, a Hitachi S4800 scanning electron microscope with an X-ray spectral analysis attachment was used. The relative error in determining the component composition is ±5 %. Analysis of the appearance indicates that after the process of copper deposition on the surface of individual fibers, copper deposits with a thickness of 5…10 μm and a length of up to 50 μm appear. Such results can be explained by the fact that in the implementation of the chosen method of copper deposition, the surface area of the tissue is uneven in area.

DESIGN AND DEVELOPMENT COMPLEX SAFETY SCADA SYSTEMS

Kamiel Iehab Abduljabbar Kamil, M.B. Abrosimov

Capacity development for modern systems in light of recent developments in the world computer, especiallyin the time of the spread of various related technologies with applications that perform key functions in providing essential services (e.g., electricity, naturalgas, gasoline, water, waste treatment, transportation, and nuclear power plants) modern technological systems that support industry and services SCADA system (Supervisory Control and Data Acquisition). SCADA system is one of the most important systems in technological systems operating in many factories and big companies for control.

Many threats that exist in cyber space today that makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and serious disruptions to the nation's critical infrastructure. Other factors that could lead to lack of availability to important information may include accidents such as power outages or natural disasters ready to restore services in case anything happens to your primary data centers will heavily reduce the downtime in case of anything happens.

For achievement fault tolerance in SCADA system and ability of a system to continue performing its intended function in spite of faults. Fault tolerance supports reliability, with successful operation. An important feature primary attributes for fault tolerance system are reliability, availability and safety. Other possible attributes include maintainability, testability, confidentiality, security.

BALANCE AND SECURITY FOR MESSAGING LAYERS

Sudani Hayder Hussein, M.B. Abrosimov

The times we live is the age of technology, technical development, which arrived today to its highest level ever, and this development includes all walks of life, and perhaps most particularly communications world, which has provided the people a lot of time, effort and contributed to the rapprochement between the distances and reach out to others in the easiest ways thanks to modern means of communication. With the increase in telecommunications networks, they become continuously to failure, some of the links or nodes may fail in the network. It becomes important to find the best solution to accomplish the task of communicating the desired number of defects. The F5 Big-IP Global Load-balancing solution feature along. F5 Big-IP system delivers full seamless load balance methodology between different messaging layers to be considered in designing a fault tolerant communication network. F5 Big-IP setup will load-balance SMPP traffic/binds between content providers and Airgate as well as between Airgate and all SMSC sites. Fault tolerance and security are of paramount importance. Solution designs leverage cloud based messaging system architecture and will result in less traffic outages caused by link system failures and will add security layer to messaging system. F5 Big-IP can assign two different networks: one for external access and another one to communicate with messaging node only. In such setup F5 Big-IP will work as firewall to other elements.

ПРИМЕНЕНИЕ КОНФОРМНЫХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ В ПРИЕМНЫХ СИСТЕМАХ ГНСС

А.С. Абукраа, М.А. Вилькоцкий

Известно, что существенную проблему улучшения помехоустойчивости и точности ГНСС представляет создание приемных антенн. Проблема обусловлена противоречивостью требований к диаграмме направленности, которая в большой области пространства, занимаемых наблюдаемыми спутниками, должна быть равномерной и иметь большой уровень, но в тоже время обеспечивать низкий уровень сигналов в направлениях касательных к поверхности горизонта и ниже его. Возможным решением этой проблемы является применение малогабаритных (менее половины длины волны) антенн, размещаемых на экранирующих поверхностях. Однако, последние для обеспечения необходимых характеристик должны иметь значительную толщину и вес [1]. Возможным выходом является применение импедансных поверхностей частотно-селективного типа [2]. Они могут иметь малый вес, но занимают большой объем, что обусловлено необходимостью обеспечения поляризационной изотропности их свойств. Возможным выходом из проблемы, возникающей из-за противоречивости требований, может быть применение конформных конструкций, которые имеют малый объем в нерабочем состоянии, быстро трансформируются в экран большого объема в рабочем состоянии с последующим размещением вблизи приемной антенны ГНСС.

В докладе обсуждаются результаты расчетов и экспериментов по оценке эффективности применения комбинации слабонаправленных малогабаритных антенн и решетчатых импедансных экранов размером до 0,5×0,5×0,1 м, образованных полосковыми элементами. Последние в транспортабельном состоянии трансформируются в плоскую полосу малого объема.

Литература

1. Татарников Д.В. Экраны антенн высокоточной геодезии по сигналам глобальных навигационных спутниковых систем. Часть 1. Полупрозрачные экраны из композитных материалов. М., Радиотехника, 2008. С. 6–19.

2. Абукраа А.С., Вилькоцкий М.А. Применение экранирования при подавлении нежелательных каналов приема абонентских спутниковых навигаторов // Докл. БГУИР. 2017. №2 (104). С. 84–91.

ЭКРАНИРУЮЩИЕ СВОЙСТВА ИМПЕДАНСНЫХ ЭКРАНОВ КОМФОРМНОСНОГО ТИПА

А.С. Абукраа, М.А. Вилькоцкий

Известны экраны импедансного типа в виде периодически повторяющихся элементов. В практике наибольшее распространение получили планарные конструкции, образованные печатными элементами разнообразных форм. Но в ряде случаев необходимые свойства могут быть достигнуты только путем создания трехмерных экранов, имеющих значительную толщину. Часто они имеют весьма сложную трехмерную геометрию, например, так называемые грибовидные структуры [1]. Как следствие этого, такие экраны громоздки и имеют низкую механическую прочность, что затрудняет их практическое использование в процессе транспортировки и эксплуатации. Существует возможность создания экранов из плоских поверхностей, которые в развернутом состоянии образуют объемные фигуры. История создания таких конструкций восходит к искусству оригами. Имеется большое число объемных геометрических фигур, которые трансформируются в плоские конструкции, изготовленные из печатных элементов, расположенных в перпендикулярных плоскостях. Приводятся результаты теоретических и экспериментальных исследований параметров экранов с конформными свойствами, образованные замкнутыми и разомкнутыми элементами рамочной, кольцевой и Ω форм. Обсуждается влияние ограниченности размеров экранов на распределение полей вблизи экранов, а также на пространственные диаграммы источников излучения, расположенных за экранами.

Литература

1. Capolino F., Jackson D.R., Wilton D.R. Fundamental Poperties of the Field at the Trans. AP. 2005. Vol. 53.

УГЛЕРОДСОДЕРЖАЩИЕ КОМПОЗИЦИОННЫЕ ПОКРЫТИЯ НА ОСНОВЕ АНОДНОГО ОКСИДА АЛЮМИНИЯ ДЛЯ МАСКИРОВАНИЯ В УФ И СВЧ ДИАПАЗОНАХ

М.Ф.С.Х. Аль-Камали, Я.Т.А. Аль-Адеми, И.А. Врублевский, Е.В. Чернякова, А.П. Казанцев

Одним из распространенных способов защиты объектов является применение средств маскировки. Маскирование позволяет существенно снизить характеристики обнаружения объектов с помощью оптико-электронных и радиолокационных средств. Разработка мощных эксимерных лазеров открыла возможность использования УФ диапазона в электронных системах обнаружения и разведки. Поэтому в настоящее время усилия разработчиков в области радиопоглощающих материалов направлены на создание широкодиапазонных материалов, позволяющих осуществить маскирование электромагнитного излучения (ЭМИ) с захватом области УФ диапазона.

Эффективным методом создания радиопоглощающих материалов являются использование композиционных материалов, изготовленные на основе пористых матриц. К достоинствам таких материалов относится возможность изменять в широких пределах структуру пористой матрицы и параметры материала наполнителя.

В данной работе представлены результаты исследований поглощения УФ излучения и экранирующих свойств (диапазон частот 8–12 ГГц) пористых матриц на основе углеродсодержащего анодного оксида алюминия. Для исследований использовались образцы пористого углеродсодержащего анодного оксида алюминия толщиной 10, 30 и 60 мкм. Облучение образцов проводили в диапазоне длин волн 275–360 нм. Установлено, что максимум поглощения УФ излучения для анодных пленок наблюдался в диапазоне 330–360 нм. Наибольшее ослабление ЭМИ образцы имели в диапазоне частот 8,0…9,5 ГГц, что является характерным для поглощения ЭМИ углеродсодержащими материалами. Полученные результаты позволяет рассматривать матрицы пористого углеродсодержащего оксида алюминия, как перспективный материал для создания композиционных экранов электромагнитного излучения.

ВЛИЯНИЕ ТЕРМООБРАБОТКИ ОТКРЫТЫМ ПЛАМЕНЕМ ХЛОПКОПОЛИЭФИРНОЙ ТКАНИ С НАНОСТРУКТУРИРОВАННЫМ ФЕРРОМАГНИТНЫМ МИКРОПРОВОДОМ НА ЕЕ СОСТАВ

Аль-Махдави Мустафа Сабах Халил, А.А.А. Ахмед, Я.Т.А. Аль-Адеми, М.Р.Н. Неамах

В настоящее время в целях зонального электромагнитного экранирования помещений предлагается использовать ткань с наноструктурированным ферромагнитным микропроводом (НСФМ). Однако на основе результатов выполненных экспериментов определено, что указанный материал характеризуется малым временем сопротивления открытому пламени (~ 3 с), что не соответствует требованиям норм пожарной безопасности. Установлено, что после сгорания в открытом пламени основными компонентами образовавшегося остатка являются силикат кальция (Ca_2O_4Si) и тиллеулит ($C_2Ca_5O_{13}Si_2$). В связи с этим актуальным представляется проведение исследований, направленных на установление наиболее оптимальных способов модификации ткани с НСФМ, в результате применения которых время сопротивления открытому пламени последней возрастет. В настоящей работе определено, что модифицирование ткани с НСФМ путем ее пропитывания водным раствором $CaCl_2$ марки «Жидкий» приводит к увеличению в 10 раз ее времени сопротивлению открытому пламени. Установлено, что в результате использование указанного способа в межволоконное пространство ткани с НСФМ встраивается комплекс различных минеральных осадков на основе Ca, Al, Fe, Mg, Zr. Высокотемпературная обработка ткани с НСФМ приводит к преимущественному формированию силиката кальция (Ca_2O_4Si) и минералов везувианита ($Al_{5,2}Ca_{9,16}Cl_{0,23}F_{1,674}Fe_{0,62}H_{2,6}Mg_{0,516}Na_{0,04}O_{371}Si_{8,915}Ti_{0,64}$), пироксфероита ($Ca_{0,94}Fe_{6,06}O_{21}Si_7$) и тринатрийфосфатного дикалиевого трифосфидосиликата ($K_2Na_3P_2Si$). При этом открытое пламя отсутствует, что может быть обосновано снижением температуры образца за счет испарения содержащейся в нем воды (до 120 % веса сухого материала) и образовании керамических микровключений, отражающих инфракрасный высокотемпературный нагрев.

Таким образом, можно сделать вывод о том, что основной вклад в формирование

вышеуказанных материалов при термообработке открытым пламенем вносит взаимодействие оксида кремния, содержащегося в стеклянной оболочке микропровода, в тканом основании, рентгеноаморфного кальция и углерода, содержащихся в органических нитях.

АВТОМАТИЗИРОВАННЫЙ ИЗМЕРИТЕЛЬНЫЙ КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ ДИАГРАММЫ АМПЛИТУДНО-ФАЗОВЫХ СОСТОЯНИЙ ПРИЕМО-ПЕРЕДАЮЩЕГО МОДУЛЯ АФАР

Р.А. Богданов, Ю.С. Алькевич, В.А. Симоненко

Радиолокационные станции, спутники и системы радиоэлектронного подавления используют множество приемопередающих модулей (ППМ). Аппаратные средства ППМ устанавливаются за каждым антенным элементом в активной фазированной антенной решетке (АФАР), поэтому потенциально требуются сотни или тысячи модулей для одной радиолокационной станции. Повышение производительности их испытаний и сокращение времени снятия диаграммы амплитудно-фазовых состояний (АФС) ППМ является важным требованием. Типично ППМ нуждаются в большом объеме испытаний, позволяющих гарантировать, что все модули подходят для работы в антенной решетке, в которой они используются, а также в процессе испытаний происходит получение диаграмм АФС, необходимых для последующей корректировки по фазе и амплитуде. Для исследования параметров приемопередающего модуля был разработан автоматизированный измерительный комплекс (АИК). АИК представляет собой совокупность программно-управляемых измерительных, вычислительных и вспомогательных технических средств, реализующих алгоритм получения, обработки и использования измерительной информации. Данный автоматизированный измерительный комплекс предназначен для измерения АЧХ, ФЧХ, КСВН приемного и передающего каналов приемопередающего модуля, диаграммы амплитудно-фазовых состояний ППМ. Для измерения вышеперечисленных параметров и оценки работоспособности ППМ АФАР в целом и субмодуля аттенюатор-фазовращатель в частности используется векторный анализатор цепей, анализатор спектра и СВЧ генератор сигналов, подключенные к персональному компьютеру. Разработанное в среде программирования LabVIEW программное обеспечение позволяет в автоматическом режиме измерить АФС ППМ во всех состояниях аттенюатора и фазовращателя на определенной частоте или в диапазоне заданных частот. Высокая скорость автоматизированных испытаний позволяет измерять все режимы работы модуля и все параметры с высоким разрешением за короткие промежутки времени, что дает возможность выполнения более глубоких испытаний в экстремальных условиях (температура, механическое воздействие, влияние окружающей среды), поскольку электрические параметры могут быть измерены быстрее, чем изменяются внешние условия. Большое количество собранных данных может быть также использовано для улучшения моделирования компонентов.

Литература

1. Богданов, Р.А. Система функционального контроля субмодуля аттенюатор – фазовращатель приемопередающего модуля X-диапазона / Р.А. Богданов // Метрология и приборостроение. – 2016. – № 4. – С. 6–10.

ЭФФЕКТЫ ПЕРЕКЛЮЧЕНИЯ И ПАМЯТИ В ХАЛЬКОГЕНИДНЫХ ПОЛУПРОВОДНИКАХ

М.А. Борисов

В настоящее время продолжается активный поиск материалов, которые целесообразно использовать для создания электрически стираемого перепрограммируемого постоянно запоминающего устройства (ЭСППЗУ). Из всего многообразия неупорядоченных халькогенидных (ХГ) соединений, в которых наблюдаются эффекты переключения и памяти, можно выделить два, наиболее характерных: это SiTeAsGe (STAG) и GeTeSb (GTS). Из анализа этих соединений следует, что основным («активным») химическим элементом в этих соединениях является теллур (Te). Теллур – это элемент VI группы периодической таблицы.

Структура валентной оболочки теллура – $5s_2 5p_4$. Два из четырех *p*-электрона образуют ковалентные связи с соседними атомами. Между цепочками действуют менее прочные связи Ван-дер-Ваальса. В образовании этих связей принимает участие оставшаяся одиночная пара *p*-электронов (lone-pare). Кристаллическая структура Te гексагональная и анизотропная. В предлагаемой статье анализируется возможность создания тонкопленочных элементов памяти и порогового переключения на основе одного халькогена-теллура.

Литература

1. Волькенштейн, Ф.Ф. Физико-химические свойства поверхности полупроводников / Ф.Ф. Волькенштейн. – М.: Наука, 1973. – 340 с.

2. Luth, H. Solid surfaces, interfaces and thin films / H. Luth. – Berlin: Springer, 2012. –577 p.

3. Infrared absorption of Ag- and Cu- photodoped chalcogenide films / A.I. Stetsun [et. al] // J. Non-Crys. Sol. – 1996. – Vol. 202. – P. 113–121.

МОДЕЛИРОВАНИЕ В СРЕДЕ MATLAB ПАРАЛЛЕЛЬНОГО МАНИПУЛЯТОРА НА ТРЕХОСЕВОМ ПРИВОДЕ

А.Ю. Войтов

Дальнейшее повышение функциональных возможностей манипуляционных систем перемещений при обеспечении больших скоростей и ускорений на рабочей платформе, а так же повышенных характеристик точности и быстродействия в настоящее время связывается с применением параллельных манипуляторов [1].

В работе предложена алгоритмизация математической модели параллельного манипулятора на новом гибридном треугольном приводе прямого действия, для которой разработан подход и математическая модель формализованного описания, сегментирования алгоритмов и исследования кинематики и динамики. Вычислительное решение по нахождению линейных и угловых координат платформы по заданным обобщенным линейным координатам ведущих звеньев выполняется по аналитическому описанию векторного условия многоконтурной замкнутости параллельных кинематических цепей в виде фундаментальной нелинейной системы из трех уравнений.

При этом алгоритмически обеспечено сохранение начальных конфигурационных условий во всем диапазоне изменений искомых переменных с обеспечением однозначного визуального отображения на персональном компьютере положения платформы, всех звеньев и механизма в целом в режиме реального времени.

Разработана имитационная модель кинематики, которая позволила выполнять решение прямой и обратной задач кинематики. На основании предложенных сегментированных алгоритмов разработана имитационная модель в среде MATLAB для проведения интерактивного компьютерного моделирования решения прямой и обратной задач кинематики и прямой и обратной задач динамики с учетом конструктивных ограничений, накладываемых на координатные перемещения электро-магнитных модулей на треугольном статоре.

Литература

1. Системы многокоординатных перемещений и исполнительные механизмы для прецизионного технологического оборудования / В.В. Жарский [и др.] ; под ред. д-ра техн. наук, проф. С.Е. Карповича. – Минск : Бестпринт, 2013. – 208 с.

ПОРОГОВОЕ НАПРЯЖЕНИЕ MIS-HEMT С ПОДЗАТВОРНЫМИ HIGH-K ДИЭЛЕКТРИКАМИ

В.С. Волчёк

AlGaN/GaN транзисторы с высокой подвижностью электронов (high electron mobility transistor, HEMT) являются перспективными элементами сенсорных устройств, используемых в системах информационной безопасности. В стандартной технологии HEMT затвор формируется на основе барьера Шоттки и характеризуется большими токами утечки. Для уменьшения токов утечки транзистора между электродом затвора и барьерным слоем AlGaN

располагают диэлектрик, образуя таким образом структуру металл/диэлектрик/полупроводник (metal/insulator/semiconductor, MIS). В структуре MIS применяются high-к диэлектрики, материалы с высокой диэлектрической проницаемостью, позволяющие увеличить емкость затвора, не прибегая к уменьшению его толщины.

Значение работы выхода электронов из металла, расположенного на high-к диэлектрике, отличается от значения, полученного для случая вакуума, что приводит к сдвигу порогового напряжения транзистора. Модель для расчета эффективной работы выхода электронов из металла, основанная на понятии нейтрального уровня диэлектрика, представлена в статье [1].

Для исследования влияния материала подзатворного диэлектрика на пороговое напряжение AlGaN/GaN MIS-HEMT выбрана структура, состоящая из барьерного слоя $Al_{0,2}Ga_{0,8}N$, буферного слоя GaN, омических контактов к истоку и стоку, подзатворного диэлектрика и платинового электрода затвора. Моделирование выполнялись в программном комплексе компании Silvaco. Пороговое напряжение транзистора с SiO_2 в качестве подзатворного диэлектрика составляет –2,6 В, а в случаях с HfO_2 и La_2O_3 равняется –1,5 и –1,1 В, соответственно. Таким образом, величина сдвига порогового напряжения в положительном направлении пропорциональна диэлектрической проницаемости подзатворного материала, которая является единственным значимым параметром в расчетах, и зависит от эффективной работы выхода электронов из металла электрода затвора.

Литература

1. Yeo, Y.-C. Metal-dielectric band alignment and its implications for metal gate complementary metal-oxide-semiconductor technology / Y.-C. Yeo, T.-J. King, C. Hu // J. Appl. Phys. – 2002. – Vol. 92, № 12. – P. 7266–7271.

ПРИМЕНЕНИЕ La_2O_3 В КАЧЕСТВЕ ПОДЗАТВОРНОГО ДИЭЛЕКТРИКА MIS-HEMT

В.С. Волчёк

AlGaN/GaN транзисторы с высокой подвижностью электронов (high electron mobility transistor, HEMT) являются перспективными элементами сенсорных устройств, используемых в системах информационной безопасности. В стандартной технологии HEMT затвор формируется на основе барьера Шоттки и характеризуется большими токами утечки. Для уменьшения токов утечки транзистора между электродом затвора и барьерным слоем AlGaN располагают диэлектрик, образуя таким образом структуру металл/диэлектрик/полупроводник (metal/insulator/semiconductor, MIS). В структуре MIS применяются high-к диэлектрики, материалы с высокой диэлектрической проницаемостью, позволяющие увеличить емкость затвора, не прибегая к уменьшению его толщины. Однако, на границе раздела большинства high-к диэлектриков с барьерным слоем AlGaN формируется положительный связанный заряд, который приводит к сдвигу порогового напряжения транзистора в отрицательном направлении, что затрудняет процесс выключения прибора. Одним из немногих high-к диэлектриков, создающих отрицательный связанный заряд на границе раздела с барьерным слоем AlGaN, является La_2O_3.

Применение La_2O_3 в качестве подзатворного диэлектрика AlGaN/GaN MIS HEMT позволяет уменьшить ток утечки затвора на три порядка по сравнению с транзистором с затвором Шоттки. Отрицательный связанный заряд, величина которого может регулироваться параметрами технологических процессов, на границе раздела с барьерным слоем AlGaN приводит к смещению порового напряжения в положительном направлении, что делает La_2O_3 перспективным материалом для создания HEMT с нормально закрытым каналом [1].

Литература

1. Threshold voltage engineering in GaN-based HEMT by using La2O3 gate dielectric / M. Minhan [et al.] // Phys. Status Solidi. – 2016. – Vol. 13, № 5–6. – P. 325–327.

ТЕРМОДИНАМИЧЕСКИЕ СВОЙСТВА МАГНИТНЫХ НАНОКОМПОЗИТОВ НА ОСНОВЕ ПОРИСТОГО АНОДНОГО ОКСИДА АЛЮМИНИЯ ДЛЯ ЭЛЕМЕНТОВ ОБРАБОТКИ ИНФОРМАЦИИ

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

Мембраны из пористого анодного оксида алюминия (ПАОА), изготовленные двухступенчатым анодированием алюминиевых заготовок (пластин или фольги) в водном растворе щавелевой кислоты, являются самыми популярными шаблонами, используемыми при получении магнитных нанокомпозитов. Многообразие вариантов использования ПАОА матриц стимулирует проведение детальных исследований их физико-химических свойств различными методами. Сравнительный анализ методов исследования термических свойств ПАОА и нанокомпозитов на его основе показал, что для исследования термодинамических характеристик наиболее подходит метод дифференциально-термического анализа. Практический интерес исследований в этом направлении связан также с тем, что встраивание различных наноэлементов в химически и термически инертную матрицу из оксида алюминия является одним из способов повышения их стабильности. Основная цель исследования состояла в том, чтобы определить, сохраняет ли такая мембрана упорядоченную пористую наноструктуру при температурах выше 800 °С. Это увеличило бы диапазон полезных свойств (температура и чистота) по сравнению с коммерческими мембранами (T_{max}= 600–700°С) и мембранами, изготовленными в фосфорнокислом электролите. Были проведены комплексные исследования состава, структуры и термодинамических характеристик, в частности особенностей фазовых переходов I рода (кристаллизации) в ПАОА 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 ПАОА начинаются при температурах выше 850 °С. В целом экспериментально показано, что мембраны ПАОА изготовленные из А1 фольги (99,995 %) двухступенчатым анодированием в 4 %-ном водном растворе щавелевой кислоты, как описано в работе [1], являются в достаточной степени химически и термически стойкими в интервале температур от комнатной до 850°С.

Такие мембраны, с сохранившейся после отжига упорядоченной структурой и не содержащие примесей, можно будет также использовать при синтезе термостойких материалов, используемых в процессах катализа и газоразделения при высоких температурах, и в качестве матриц (template) для формирования массивов УНТ CVD и PVD методами в среде аргона.

Литература

1. Vorobjova A.I., Shimanovich D.L., Yanushkevich K.I. et al. // Beilstein J. Nanotechnol. 2016. № 7. P. 1709–1717.

ИССЛЕДОВАНИЕ ПОКРЫТИЙ НА ОСНОВЕ КОМБИНИРОВАННЫХ ОГНЕЗАЩИТНЫХ СМЕСЕЙ С РАДИОПОГЛОЩАЮЩИМИ СВОЙСТВАМИ В ИНФРАКРАСНОМ И СВЧ ДИАПАЗОНАХ

Л.Л. Ганьков, Т.А. Пулко

Для формирования покрытий с радиопоглощающими свойствами в пожароопасных промышленных и выделенных помещениях при проведении строительных и ремонтных работ целесообразно использовать огнезащитные составы с добавлением вспученного вермикулита. Цель работы заключалась в исследовании экранирующих характеристик полученного комбинированного покрытия в диапазоне частот 8…17 ГГц и его термограмм в пределах среднего и дальнего ИК-диапазонов. При измерении термограмм источник инфракрасного излучения генерировал направленный поток воздуха с температурой 80 ºС при температуре окружающей среды 24 ºС, а нагревание исследуемых образцов производилось равномерно до стабилизации температуры поверхности образца. Проводились измерения характеристик трех образцов комбинированных покрытий на основе огнезащитного состава толщиной 5 мм с

добавлением вспученного вермикулита (образец № 1), вспученного вермикулита и 40%-го водного раствора $CaCl_2$ (образец № 2), а также вспученного вермикулита, 40%-го водного раствора $CaCl_2$ и силикагеля (образец № 3). Установлено, что в диапазоне частот 8...17 ГГц образец № 3 обладает наилучшими значениями коэффициента отражения ЭМИ (–0,794…–16,669 дБ) при значениях коэффициента передачи ЭМИ 0…–2,357 дБ; образец № 2 обладает наилучшими значениями коэффициента передачи ЭМИ (–4,274…–6,997 дБ) при значениях коэффициента отражения ЭМИ 0…–10,44 дБ; образец №1 обладает средними значениями коэффициентов отражения (0…–12,282 дБ) и передачи ЭМИ (–1,218…–3,712 дБ). При этом установлено, что для всех образцов (№ 1, 2, 3) кратность снижения температуры экрана относительно температуры источника излучения составила 2 раза. Полученные результаты исследований позволяют предложить применение разработанных комбинированных покрытий с экранирующими свойствами в диапазоне частот 8…17 ГГц и диапазоне длин волн 8…12 мкм для отделки производственных и выделенных помещений.

ОСОБЕННОСТИ ГЕТЕРОСТРУКТУР, ПРИМЕНЯЕМЫХ В СЕНСОРНЫХ УСТРОЙСТВАХ

Д.Ч. Гвоздовский, М.С. Баранова, В.Р. Стемпицкий

Интерес к наноматериалам связан с новыми фундаментальными научными проблемами и физическими явлениями, а также с перспективами создания устройств наноэлектроники, спинтроники и информационных технологий нового поколения. Спин-орбитальное взаимодействие является важной составляющей физических процессов, происходящих при работе спинтроных устройств. При определенных условиях, например, когда отсутствует центр инверсии, в наноразмерных структурах возникает перпендикулярное электрическое поле, которое взаимодействует с электронами проводимости. Это взаимодействие в конечном итоге приводит к расщеплению энергетических уровней на спин-вверх и спин-вниз в немагнитных структурах [1].

Проведено квантово-механическое моделирование влияния воздействия внешнего электрического поля на гетероструктуру, состоящую из графенподобного ZnS и графена. Расчеты проводились в программном комплексе VASP, который реализует метод теории функционала электронной плотности [2]. Взаимодействие между атомными остовами и валентными электронами описывалось методом присоединенных плоских волн (PAW). Структурная оптимизация считалась достигнутой при разнице полной энергии менее 1×10^{-6} эВ между двумя последними шагами. Интегрирование в импульсном пространстве проводилось по сетке *k*-точек 8×8×1 сгенерированной по Гамма схеме. Энергией обрезания составляла 450 эВ. Для описания волновых функций валентных электронов был выбран функционал DFT-D2, учитывающий силы Ван-дер-Ваальса. Показано, что нарушение трансляционной симметрии приводит к возникновению релятивистского эффекта, который связан со спин-орбитальным взаимодействием, что в конечном итоге приводит к вырождению по спину. Наличие данного эффекта позволяет использовать материал в сенсорных устройствах.

Литература

1. R.Winkler, Phys.Rev. B. 2004. Vol. 10. P. 045317
2. Kresse, G. VASP the guide: tutorial / Austria, U. of Vienna. – 2003. – P. 94–104.

МАЛОГАБАРИТНЫЙ ОБЪЕКТИВ С ПЕРЕМЕННЫМ ФОКУСНЫМ РАССТОЯНИЕМ

В.В. Давидович, А.Г. Черных, В.В. Шульгов

В основе функционирования объектива лежит эффект электросмачивания (electrowetting), т.е. изменения коэффициента смачивания поверхности под воздействием электрического поля или тока. Аберрационный расчет оптической системы позволил определить конструктивные элементы системы и состав применяемых жидкостей с минимальным значением отношения показателей преломления. Объектив представляет собой цилиндр из алюминиевого сплава АД-1н диаметром 22 мм и длиной 14 мм, герметично закрытый с двух торцов прозрачным стеклом. Положительным электродом устройства является

сам цилиндр, отрицательным – гидрофильное проводящее покрытие верхнего стекла. До сборки внутренняя поверхность цилиндра и его торцы анодируются, толщина оксида – 200 нм. После приклеивания нижнего стекла внутренняя поверхность полученного стакана покрывается прозрачным водоотталкивающим составом, благодаря чему впоследствии водная компонента принимает сферическую форму, т.е. становится линзой. Далее стакан заполняется двумя несмешивающимися текучими композициями, сначала – силиконовым маслом ПМС-200, а затем – водным раствором лимонной кислоты. Верхнее стекло с одной стороны покрывается гидрофильным прозрачным проводящим покрытием, выходящим на торец стекла и этой стороной приклеивается к торцу цилиндра. Авторами исследовались зависимости угла смачивания от приложенного напряжения и толщины оксида. С использованием программного пакета COMSOL выполнено моделирование фокусного расстояния объектива. Управляющее напряжение менялось от 20 до 50 В, при этом фокусное расстояние составляло 58–12 мм. Рабочее напряжение устройства можно снизить путем увеличения диэлектрической проницаемости оксидной пленки или уменьшения ее толщины. В частности, использовать для изготовления устройства другие металлы, такие как титан, тантал или ниобий. Минимальная толщина диэлектрика ограничивается его электрической прочностью.

АЛГОРИТМ ФОРМИРОВАНИЯ ТЕКСТА ДЛЯ СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА БЕЛОРУССКОМ ЯЗЫКЕ

Г.В. Давыдов, П.С. Какоренко

Одним из наиболее эффективных средств защиты речевой информации в возможных каналах утечки акустической информации считается речеподобный шум. Суть его заключается в создании помех, представляющих собой последовательно воспроизводимые элементы речи диктора. К структурным единицам речи относятся аллофоны, дифоны, трифоны, полифоны, слоги, отдельные слова и словосочетания. При использовании в качестве структурных единиц речи более длинных по звучанию фрагментов, речь становится более естественной, однако необходимы при этом большие объемы памяти и большие базы структурных единиц речи, создание которых является трудоемким процессом[1]. Поэтому было принято решение об использовании аллофонов в качестве структурной единицы для формирования текста.

Весь алгоритм формирования текста базируется на статистических данных используемого языка, которые включают в себя статистические данные о длине предложений, длине слов, а также вероятности появления определенных фонем. Например, в белорусском языке в среднем от 1 до 7 слов в предложении, слова из 5-6 букв встречаются чаще других, а самым редким аллофоном считается **Ф**. С учетом этих данных и значений, полученных от генератора псевдослучайных чисел, определяется сначала число слов в предложении, затем длина каждого слова и, наконец, какой аллофон должен стоять на данной позиции в слове. Процесс будет выполняться до тех пор, пока не будет определен последний аллофон в предложении. Далее начинается формирование последующих предложений таким же образом.

Для достижения натуральности и естественности звучания речи слова должны быть сформированы с учетом основных фонетических особенностей белорусского языка. В данный алгоритм были включены следующие ограничения и правила/

1. Если слово состоит из 1 буквы, этими буквами могут быть только **А**,**Б**,**Ж**,**З**,**У**,**Я**, **І**, **Ў**.
2. В словах из 2-х букв не должно быть подряд идущих гласных или согласных, кроме сочетаний **яе** и **ёю**.
3. Должны быть исключены повторы рядом стоящих букв, за исключением **Е**, **Н**, **С**.
4. Не допускать три согласные или гласные идущие подряд.
5. **Ь**, **Ы** и **Й** не могут идти в слове после гласных, букв **Ў**, **Ь**, а также стоять в начале слова.
6. Если подряд идут **С** и **Ч**, следует их заменить на **Ш**;
7. После **Ж, Р, Ш, Ч, Т, Д** необходимо сделать замены **Я** на **А**, **І** на **Ы**, **Ю** на **У**, **Ё** на **О** и **Е** на **Э.**
8. После гласных **У** должно меняться на **Ў.**

Данный алгоритм реализован и отработан программно.

Литература

1. Синтез речеподобных сигналов на белорусском языке / Г.В. Давыдов [и др.] // Доклады БГУИР. – 2015. – № 4 (90). – С. 27–32.

СНИЖЕНИЕ ВЛИЯНИЯ ВНЕШНЕГО ИЗЛУЧЕНИЯ НА ИЗМЕРЕНИЯ МАЛЫХ КОЛЕБАНИЙ ТЕМПЕРАТУРЫ С ПОМОЩЬЮ ТЕПЛОВИЗОРА

Г.В. Давыдов, А.И. Кухаренко

Для обнаружения малых изменений в работе электронного устройства с помощью инфракрасного излучения необходимо использовать чувствительный тепловизор с микроболометрической матрицей. Измерения проводились с помощью тепловизора FLIR Tau 2 640, работающего в инфракрасном диапазоне 8–14 мкм, имеющего чувствительность < 50 мК и разрешение 640×512 пикселей. Во время проведения измерений были выявлены пути снижения влияния внешних помех на проводимые измерения.

Для обнаружения малых изменений температуры поверхности компонентов проверяемых устройств необходимо экранировать объект проверки и тепловизор от тепловых фоновых шумов. Шумы представляют собой тепловое излучение от экспериментатора, световое излучение, поступающее в помещение через окна, конвекционные тепловые потоки, излучение от самого тепловизора. Для исключения влияния на результаты измерений ИК излучения от экспериментатора или от людей, находящихся в комнате, необходимо испытуемый объект и тепловизор размещать в отдельной комнате. Помещение для проведения проверки должно состоять из двух комнат, в одной комнате размещается испытуемый объект и тепловизор, в другой располагается остальное оборудование и находятся люди.

На результаты проверки вычислительной техники оказывают влияние вибрации испытуемого объекта и тепловизора. Вибрации приводят к смещению изображения объекта и усложнению цифровой обработки изображений. Для исключения влияния этого фактора на результаты проверки, необходимо применять меры по виброизоляции как объекта, так и тепловизора. На результаты проверки негативное влияние могут оказывать конвекционные потоки и сквозняки. Поэтому при проведении проверки необходимо плотно закрывать двери и окна в комнате, где проводятся проверки. Многократно переотраженное световое и инфракрасное излучение, попадающее в комнату через окна, негативно влияет на точность измерений. Окна в комнате, где проводятся проверки, должны быть зашторены для исключения влияния на результаты проверки проходящего через стекла излучения.

Тепловое излучение от тепловизора можно частично заблокировать с помощью теплоизоляционного экрана, в котором проделано отверстие с диаметром равным диаметру объектива. В таком случае, остается излучение только от германиевой линзы объектива.

ВЛИЯНИЕ ФОКУСНОГО РАССТОЯНИЯ ОБЪЕКТИВА ТЕПЛОВИЗОРА НА СПОСОБНОСТЬ ИЗМЕРЯТЬ ТЕМПЕРАТУРУ МАЛЫХ ОБЪЕКТОВ

Г.В. Давыдов, А.И. Кухаренко

Измерение инфракрасного излучения от радиоэлектронных компонентов, размещенных на печатной плате устройства, может быть использовано для диагностики различной радиоэлектронной аппаратуры, поиска неисправностей, выявления некорректной работы компонентов или обнаружения потенциальных точек отказа и утечек информации в аппаратуре. Для обнаружения малых изменений в работе современного электронного устройства необходимо иметь высокую пространственную разрешающую способность инфракрасной камеры. Это необходимо для контроля за всеми электронными компонентами устройства, даже имеющими самые малые размеры. Резисторы поверхностного монтажа имеют широкий диапазон размеров и, на сегодняшний день, широко используются миниатюрные резисторы типоразмера SMD01005, имеющие размеры близкие к 400 мкм в длину и 200 мкм в ширину. Начинают использоваться еще меньшие размеры, например, SMD 008004. Обнаружение изменения температуры таких электронных компонентов возможно при правильно выбранном и настроенном оборудовании. На пространственную точность влияют количество пикселей тепловизора, минимальная дистанция фокусировки (MDF) объектива, фокусное расстояние

(FD), поле зрения, разрешение на пиксель. Для тепловизора FLIR Tau 2 640, имеющего размер пикселя 17 мкм и разрешение 640×512 пикселей была составлена таблица для всех фокусных расстояний и определено разрешение на минимальной дистанции фокусировки.

Таблица параметров объективов тепловизора FLIR Tau 2 640

FD (mm)	**7,5**	**9**	**13**	**19**	**25**	**35**	**50**	**60**	**100**
FOV (h*v angle)	90*69	69*56	45*37	32*26	25*20	18*14	12*10	10*8	6*5
MDF (cm)	2,5	3	8	16	30	60	150	230	700
IFOV (mrads)	2,27	1,89	1,3	0,89	0,68	0,48	0,34	0,28	0,17
x/pix (mm)	0,0567	0,0567	0,1040	0,1424	0,204	0,288	0,51	0,644	1,19

Значение разрешения (x/pix) значительно меняется и достигает минимального значения в 57 мкм у короткофокусных объективов и выходит за пределы 200 мкм в объективах с FD более 25 мм. Однако объективы с FD 7,5 и 9,0 мм не подходят из-за малого расстояния до объекта и связанных с этим искажений изображения. Оптимальным выбором является объектив с FD равным 19 мм.

ДАТЧИК ХОЛЛА С ИНТЕГРАЛЬНЫМ МАГНИТНЫМ КОНЦЕНТРАТОРОМ

Дао Динь Ха

В современной микромагнитоэлектронике все чаще применяются интегральные магнитные концентраторы (ИМК, англ. Integrated Magnetic Concentrator), в первую очередь для уменьшения размеров сенсорных приборов с сохранением возможности детектирования слабых магнитных полей (от 0,01 мкТл до 2,0 мТл). Использование ИМК из ферромагнитного материала дискообразной формы обеспечивает возможность создания сенсоров для измерения трех компонентов магнитного поля, обладающих высокой магнитной чувствительностью без ухудшения шумовых характеристик по сравнению с традиционным элементом Холла. В ряд важнейших вопросов, решаемых в рамках указанных научных направлений, входит задача разработки и оптимизации конструктивных параметров сенсорных устройств с ИМК, а также задача разработки соответствующих методов моделирования, реализованных в программных средствах, является важной и актуальной.

Интегральной магнитной концентратор представляет собой дискообразную форму с диаметром D, толщиной l и углом отклонения θ. В качестве материала ИМК использовались супермендюр (англ. supermendur) с высокой индукцией магнитного насыщения $B_s = 2{,}8$ Тл. Проведено исследование влияния геометрии и размеры ИМК на магнитные характеристики сенсорного устройства при внешнем магнитном поле $B_0 = 1{,}0$ мТл.

Таким образом, целью описанных в работе исследований являлась разработка, выбор материала и оптимизация геометрических параметров конструктивных решений магнитных концентраторов дискообразной формы, используемых в системах трехмерного датчика магнитного поля, и предназначенных для повышения коэффициента усиления магнитного потока G.

Полученные результаты свидетельствуют об эффективности предлагаемого решения для практического применения в трехмерном датчике Холла, предназначенного для детектирования слабых магнитных полей. Оптимальные значения геометрических параметров интегрального магнитного концентратора дискообразной формы составили: диаметр $D = 200$ мкм, толщина $l = 10$ мкм и угол отклонения $\theta = 60°$. Применение супермендюра в качестве материала из которого изготовлен концентратов обеспечило повышение коэффициента усиления G до 10,81 и максимального значения внешнего магнитного поля B_0 до 100 мТл.

ПОДХОДЫ К БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ТРЕХМЕРНОЙ РЕКОНСТРУКЦИИ

А.В. Доменикан, Е.А. Головатая

Многофакторная аутентификация с использованием фотографии пользователя в последнее время набирает значительную популярность, в первую очередь благодаря значительному распространению устройств с фронтальной камерой (смартфоны, ноутбуки,

планшетные ПК). Существует множество подходов к решению задачи аутентификации по лицу, одним из которых является трехмерная реконструкция.

Основная цель трехмерной реконструкции состоит, в простейшем виде, в извлечении информации о расстоянии до присутствующих на изображении объектов. Для решения этой задачи могут использоваться разнообразные аппаратные и программные средства. Эти средства можно условно разделить на активные и пассивные сканирующие системы.

Активные системы характеризуются тем, что для получения трехмерной модели осуществляют некоторое воздействие на объект и считывают отклик. В случае задачи трехмерной реконструкции лица часто используется объемное сканирование с использованием структурированного света или структурированной дальнометрии. Значительный недостаток такого рода систем состоит в необходимости использования дополнительных аппаратных средств. Тем не менее, в большинстве случаев реконструкция является достаточно точной.

Пассивные сканирующие системы направлены на построение трехмерной модели без дополнительного воздействия на исследуемый объект. К таким системам можно отнести системы бинокулярного зрения, системы параллаксного сдвига (structure from motion) и инфракрасные камеры. Такие системы требуют дополнительных вычислительных затрат для непосредственного построения модели, а также обуславливают необходимость разработки специализированных алгоритмов трехмерной реконструкции с использованием изображений.

В качестве основы некоторых алгоритмов трехмерной реконструкции используется теорема о центральном сечении. Согласно теореме, двумерные Фурье-преобразования сечений или проекций трехмерного объекта эквивалентны центральным сечениям трехмерного частотного пространства, по которому с использованием обратного трехмерного преобразования Фурье можно восстановить исходный объект. Анализ данного алгоритма показал возможность получения высокой степени детализации, однако, для построения модели с его использованием требуются значительные вычислительные затраты.

Литература

1. Solomon, J. Numerical Algorithms: Methods for Computer Vision, Machine Learning, and Graphics/ J. Solomon. CRC Press, 2015. – 400 p.

2. Shirley, P. Fundamentals of Computer Graphics/ P. Shirley, S. Marschner. CRC Press, 2009. – 804 p.

ПОВЕРХНОСТНО–БАРЬЕРНЫЕ СТРУКТУРЫ НА ОСНОВЕ МОНОКРИСТАЛЛОВ $(FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$

М.А. Жафар

В работе представлены результаты исследования поверхностно-барьерных структур $In/(FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$. Указанные структуры были созданы на основе монокристаллов $(FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$, выращенных методом Бриджмена. Для этого из полученных монокристаллов вырезали плоскопараллельные пластинки, которые механически шлифовали и полировали с двух сторон, а затем травили в травителе состава $Br_2 : C_2H_5OH = 1:3$. Средние размеры пластин после такой обработки составляли 5×5×1 мм. Структуры получали вакуумным термическим испарением металлического индия (толщина слоя ~ 2 мкм) на поверхность монокристаллов, находившихся при комнатной температуре и не подвергавшихся какому-либо нагреву при напылении слоев металлов, что позволяло не принимать в учет возможность образования на границе слоя с подложкой других фаз. Омический контакт создавался нанесением серебряной пасты.

Проведенные исследования вольт–амперных характеристик созданных структур $In/(FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$ показали, что они обладают выпрямлением, характеризуемым отношением прямого тока к обратному $K \approx 5$ при напряжениях смещения $U < 5$ В. При освещении их интегральным светом лампы накаливания воспроизводимо проявляется фотовольтаический эффект, знак которого согласуется с направлением выпрямления, а изменения в локализации светового зонда на фотоприемной поверхности таких структур, энергии падающих фотонов и интенсивности освещения не влияют на знак фотонапряжения. Эти результаты служат основанием для того, чтобы наблюдаемый фотовольтаический эффект

приписать возникновению энергетического барьера на контакте металла (In) с монокристаллами. $FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$ Вольтовая фоточувствительность (S_U) поверхностно–барьерных структур преобладает при их освещении со стороны барьерной пленки. Установлено, что созданные структуры $In/(FeIn_2S_4)_{0.5}\cdot(CuIn_5S_8)_{0.5}$ обеспечивают фоточувствительность в спектральном диапазоне от 1,2 до 3,5 эВ при T = 300 К.

ФУНКЦИОНАЛЬНЫЙ И ТЕСТОВЫЙ КОНТРОЛЬ ЦИФРОВЫХ УСТРОЙСТВ

Л.А. Золоторевич, А.В. Павлова

Проблемы проектирования СБИС, СБИС типа «система на кристалле» и, в первую очередь, проблемы функциональной верификации проектов связаны не только с обеспечением функциональной устойчивости изделия, но так же с выявлением в проекте несанкционированного расширения или нарушения функциональности. Оказывается, что решение вопроса может находиться в определенной степени в области применения тестового контроля структуры.

В настоящее время технологические возможности производства интегральных схем позволяют размещать на кристалле порядка десяти миллиардов транзисторов, а линейный размер транзистора составляет единицы нанометров. В этих условиях на первый план выходит не проблема расширения функциональности, а проблема обеспечения надежности, функциональной устойчивости. Это требует развития методов и средств проектирования и, в первую очередь, верификации проектов и построения тестов контроля на разных этапах проектирования в разных системах идентификации [1]. В настоящее время имеет место, и еще более усугубляется очевидное отставание в области контроля корректности проектирования, построения тестов и систем контроля на всех этапах жизненного цикла изделий. Решение данной задачи лежит в направлении совмещения подходов контролепригодного проектирования, построения средств встроенного самотестирования, систем функционального и тестового контроля и развития методов построения тестов.

В докладе рассматриваются вопросы построения тестов контроля проектов цифровых сложнофункциональных СБИС на начальных этапах проектирования, в разных системах идентификации, анализа контролепригодности, типы рассматриваемых неисправностей. Предлагается простой по сравнению с известными методами [2] алгоритм определения количественных мер управляемости и наблюдаемости логических структур цифровых устройств, представленных в виде взаимосвязей элементов, заданных их автоматными моделями.

Литература

1. Zolotorevich, L.A. Project verification and construction of superchip tests at the RTL level / L.A. Zolotorevich // Automation and Remote Control. – 2013. – Vol. 74, iss. 1. – P. 113–122.

2. Jervan, G.A Hybrid BIST Architecture and its Optimization for SoC Testing / G. Jervan, Z. Peng, R. Ubar, H. Kruus // IEEE 3rd International Symposium on Quality Electronic Design (ISQED'02). – 2002. – P. 273–279.

СИСТЕМА СОВМЕЩЕНИЯ НА КОЛЬЦЕВОМ ПРИВОДЕ

С.Е. Карпович, Г.А. Зубов, М.М. Форутан, А.Г. Салманзадех

Технические средства, используемые при создании специального оборудования защиты информации, как правило, основаны на реализации операции совмещения, когда многокоординатная система перемещений работает совместно с сенсорной системой дистанционного сбора информации по маякам, расположенном в физическом пространстве. При этом автоматически выполняется вывод приемника в нужную зону опроса с точным определения координаты объекта. Разработанная система совмещения на кольцевом приводе состоит из системы перемещений, построенной на комбинации исполнительного механизма параллельной кинематики в виде раскрывающегося тетраэдра и многокоординатного кольцевого привода прямого действия [1], который конструктивно состоит из одного или нескольких неподвижных сегментов с трехфазной системой обмоток, залитых теплопроводящим компаундом, и

подвижного стального кольца статора (ротора) с регулярно наклеенными редкоземельными постоянными магнитами. В систему такого двигателя может быть встроен инкрементный датчик положения для реализации регулирования по законам перемещения. Высокая равномерность вращения при этом достигается благодаря синусоидальной коммутации токов в фазах двигателя. Такой двигатель характеризуется прямым преобразованием энергии в механическое движение без дополнительных механических редукторов и передач. Он обладает высоким точностным разрешением и высокой плавностью перемещения, простотой встраивания в технологическое оборудование, полым валом, при необходимости достаточно большого диаметра. Представленная в работе система перемещений на кольцевом приводе характеризуется повышенной жесткостью кинематических соединений в результате которой достигается точность позиционирования и программируемых перемещений, превышающая такие характеристики в известных подобных системах.

Литература

1. Прецизионная система совмещения с шестью степенями свободы на кольцевом приводе прямого действия / С.Е. Карпович, Г.А. Зубов, М.М. Форутан, Г. Салманзадех // Теоретическая и прикладная механика. – 2017. – №32. – С. 94–100.

ЭКРАНИРУЮЩИЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ ПОКРЫТИЯ НА ОСНОВЕ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ ДЛЯ АРХИТЕКТУРНОГО ЭКРАНИРОВАНИЯ

Т.Р. Колесова, Г.А. Пухир, М.Ш. Махмуд

В настоящее время электромагнитное излучение является самым распространенным неблагоприятным фактором среды обитания человека. Во-первых, это негативное влияния на здоровье человека. Во-вторых, это возможность перехвата конфиденциальной информации по каналу ПЭМИН. Источники электромагнитных полей разнообразны (промышленное, медицинское и научное оборудование, компьютеры, высоковольтные линии электропередачи, средства спутниковой и сотовой связи и др.). Электромагнитное загрязнение окружающей среды является объективной реальностью, поэтому так актуальна разработка средств и методов защиты от электромагнитных факторов.

Существуют 2 способа защиты от атак на канал утечки информации ПЭМИН: активный и пассивный. При активном методе используется генератор шума, излучение которого неблагоприятно влияет на здоровье человека и говорит о наличии конфиденциальной информации. А при пассивном методе уменьшается мощность самого излучаемого сигнала за счет экранирования, как отдельного оборудования, так и помещений в целом [1].

В рамках настоящей работы решается задача архитектурного экранирования при помощи разработки композиционных материалов на основе влагосодержащих компонентов, эффективных в радиочастотном диапазоне и исследования эффективности их экранирования.

В процессе исследования были изготовлены образцы экранирующих покрытий на основе измельченной влагосодержащей древесины в цементном связующем в равных объемных долях соотношения всех компонентов. Выбор состава материала обоснован его хорошими экранирующими и эксплуатационными характеристиками. Экранирующие характеристики оценивались на основе измерений коэффициента пропускания и коэффициента отражения в диапазоне частот 0,7 – 3 ГГц. Коэффициент передачи образцами толщиной порядка 10 мм составляет порядка −15…−20 дБ во всем исследуемом диапазоне частот. Минимальный коэффициент отражения таких покрытий составляет −3…−5 дБ. Полученные результаты позволяют предложить данный композит для покрытия стен экранированной комнаты для защиты информации от утечки по каналу ПЭМИН.

Литература

1. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В Домарев.– К.: ООО «ТИД ДС», 2002. – 688 с.

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ДИНАМИЧЕСКИХ МОДЕЛЕЙ МЕХАНИЗМОВ ПАРАЛЛЕЛЬНОЙ КИНЕМАТИКИ

В.В. Кузнецов

В некоторых системах технических средств защиты информации в качестве исполнительных узлов используются механизмы параллельной кинематики. Концепция построения их динамических моделей в настоящей работе основывается на алгоритмизации математических моделей прямой и обратной задач кинематики и реализации на их основе имитационного моделирования в среде MATLAB [1].

При построении динамических моделей механизма в среде MATLAB/Simulink реализованы следующие основные этапы: конфигурирование параметров кинематических звеньев (Body blocks) механизма, при котором для каждого кинематического звена задаются геометрические размеры, положение и ориентация в пространстве, массовые свойства (масса, тензор моментов инерции, координаты центра масс); конфигурирование параметров кинематических пар (Joint blocks), при котором каждая кинематическая пара в системе характеризуется числом степеней свободы, которые она может реализовать, расположением и ориентацией собственных базовых осей; определение функциональных элементов библиотеки пакета Simscape Multibody для представления механической структуры объекта в среде MATLAB/Simulink; разработка функциональной блочно структуры рассматриваемого механизма параллельной кинематики в соответствии с его кинематической топологией; анализ, выбор и включение в блок-схему модели функциональных элементов управления.

Разработанная компьютерная модель динамики позволяет выполнить решение прямой и обратной задач динамики с интерактивной визуализацией пространственных состояний всех подвижных звеньев при реализации прецизионных программируемых движений.

Литература

1. Карпович, С.Е. Имитационное моделирование кинематики системы перемещений с интерактивной визуализацией результатов / С.Е. Карпович, В.В. Кузнецов, М.М. Форутан // Докл. БГУИР – Минск, 2016. – №. 3. – С 22–28.

СВЧ-СВОЙСТВА ОДНОДОМЕННЫХ ФЕРРОМАГНИТНЫХ ЧАСТИЦ, СОЕДИНЕННЫХ УГЛЕРОДНОЙ НАНОТРУБКОЙ

А.В. Кухарев

В настоящее время большое внимание уделяется исследованиям радиопоглощающих и экранирующих свойств наноразмерных структур и нанокомпозитов, в особенности на основе углерода и ферромагнитных материалов (кобальт, железо, никель) [1]. Настоящий доклад посвящен СВЧ-свойствам структур на основе многостенных полупроводниковых углеродных нанотрубок с внешним диаметром 20–30 нм, с обоих концов которых осаждены магнитные наночастицы железа, либо внедрены во внутренний канал нанотрубки. Таким образом, размеры прикрепленных к нанотрубке ферромагнитных частиц не превышают 30 нм, и их состояние является однодоменным [2].

Поскольку длина нанотрубки составляет порядка сотни нанометров, то влияние дипольного момента одной ферромагнитной частицы на другую пренебрежимо мало. Между тем связь между частицами возможна за счет косвенного обменного взаимодействия через электроны проводимости нанотрубки. Расчеты на основе РККИ-модели показывают, что за счет большой величины спин-орбитального взаимодействие в полупроводниковой нанотрубке расстояние косвенного обменного взаимодействия может достигать 100 нм и выше.

Результаты моделирования намагниченности частиц железа в приближении «макроспина» показывают, что наличие косвенного обменного взаимодействия между частицами железа посредством электронов проводимости нанотрубки приводит к сдвигу частоты ферромагнитного резонанса. Поскольку энергия обменного взаимодействия осциллирует с увеличением расстояния, то сдвиг частоты зависит от длины нанотрубки, соединяющей ферромагнитные частицы, и может быть как в сторону увеличения, так и

уменьшения. В совокупности для массива рассматриваемых наноструктур характерно увеличение ширины полосы резонансного поглощения за счет вклада косвенного обменного взаимодействия между ферромагнитными частицами.

Литература

1. Excellent microwave absorption property of Graphene-coated Fe nanocomposites / X. Zhao [et al.] // Scientific Reports. 2013. Vol. 3. P. 3421.

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

ЭЛЕКТРИЧЕСКОЕ 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, представляющих собой микросистемы с чипами памяти. Одним из возможных вариантов защиты таких накопителей, является разрушение их микросхем при несанкционированном доступе. Для этих целей может применяться пористый кремний совместно со стандартной кремниевой К-МОП технологией изготовления ИС. Наноструктурированный пористый кремний, пропитанный твердотельным окислителем, демонстрирует процессы горения, что может быть использовано в саморазрушающихся системах.

Установлены закономерности инициирования реакций быстрого окисления наноструктурированного кремния при помощи электрического тока, протекающего через алюминиевые дорожки, контактирующие с исследуемым материалом. Установлены пороговые плотности электрического тока, обеспечивающие разогрев металлических дорожек до необходимых температур. Разработана микросистема электрического инициирования, обеспечивающая разрушение кремниевого чипа за счет реакции быстрого горения наноструктурированного кремния. Проведенные испытания показали, что для исследуемой системы необходимо использование пассивирующего покрытия пористого слоя, предотвращающего воздействие атмосферной влаги, что в конечном счете обеспечивает повторяемость полученных результатов.

Полученные результаты могут быть использованы при изготовлении саморазрушающихся кремниевых чипов и МЭМС, использующих энергию горения наноструктурированного кремния для перемещения в пространстве.

ЛАВИННЫЕ СВЕТОДИОДЫ НА ОСНОВЕ НАНОСТРУКТУРИРОВАННОГО КРЕМНИЯ ДЛЯ ОПТИЧЕСКИХ МЕЖСОЕДИНЕНИЙ В ИНТЕГРАЛЬНЫХ СХЕМАХ

С.К. Лазарук, А.А. Лешок, Ле Динь Ви, А.С. Сычевич, В.И. Грицков

Оптические межсоединения обладают рядом преимуществ в сравнении с электрическими аналогами. Главные преимущества – это высокое быстродействие и высокая степень защиты при передаче информации за счет локализации информационного потока внутри световодов, соединяющих источники светового сигнала (светодиоды) и фотоприемника.

Нами разработана система оптических межсоединений на основе лавинных светодиодов, содержащих наноструктурированный кремний. Световой сигнал передается через планарные световоды из анодного оксида алюминия к фотоприемникам, чувствительным к оптическому сигналу видимого диапазона. Вся разработанная система изготовления по кремниевой технологии и может быть интегрирована в процесс изготовления кремниевых ИС.

Особое внимание уделено стабилизации оптических и электрических свойств наноструктурированного кремния, что позволило достичь 1000 часов непрерываного светоизлучения без заметного деградирования интенсивности оптического сигнала.

Разработанная система способна работать в гигагерцевом диапазоне, что открывает новые возможности для кремниевой интегральной электроники.

ИССЛЕДОВАНИЯ ЭКРАНИРУЮЩИХ СВОЙСТВ БЕТОНА С ДОБАВКАМИ НАНОЧАСТИЦ МАГНЕТИТА

А.Б. Лесбаев, С.М. Манаков, Б. Элоуди

Для защиты от электромагнитного излучения используются радиопоглощающие материалы или же материалы отражающие электромагнитное излучение. Сейчас разработаны и разрабатываются многочисленные экранирующие материалы, где лидируют материалы с добавками нанокомпозитов. Среди их многообразия можно выделить магнитные наноматериалы, например магнитные однодоменные частицы, которые нашли широкое применение в различных областях техники.

В работе для синтеза магнетита использован жидкофазный метод химической конденсации. Полученные частицы имеют размеры от 10 нм до 30 нм сферической формы и имеют маленький разброс по размерам. Исходя из этого можно предположить что применение их в виде добавок очень приемлем. Далее были подготовлены образцы бетона с добавками наночастиц магнетита в разных концентрациях. После высыхания бетона, измерялась экранирующая способность для электромагнитного излучения в диапазоне от 0,7 ГГц до 2 ГГц. Результаты измерений показали что коэффициент передачи изменялся в зависимости от концентраций добавок магнетита в образце и максимальное ослабление ЭМИ наблюдается на частоте 1,5 ГГц для всех образцов. Для сравнения был подготовлен базовый образец № 1 без добавок, максимальное ослабление ЭМИ которого составляет –12 дБ. Для образца № 2, где концентрация магнетита по массе составила 0,25 %, максимальное ослабление ЭМИ составляет –21 дБ. При концентрации 0,5 % для образца № 3 максимальное ослабление ЭМИ составляет –20 дБ. Образец № 4 с концентрацией в 1 % показал ослабление ЭМИ –18 дБ. Как видно из результатов, значительное ослабление ЭМИ достигается при концентрации то 0,25 до 0,5% по массе, что не повлияет на механические свойства бетона.

УГЛЕРОДСОДЕРЖАЩИЕ ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Л.М. Лыньков, Х.А.Э. Айад, А.М.А. Мохамед, Т.А. Пулко

Основным компонентом, взаимодействующим с электромагнитным излучением в композитах, являются проводящие, металлические, углеродные, магнитные включения в виде порошков или волокон. Использование тканых и волокнистых материалов в качестве основы позволяет разработать гибкие конструкции экранов ЭМИ.

В качестве материала основы предложено использование нетканого игольнопробивного полотна, которое на 60 % состоит из полиэфирных волокон, на 20 % из полипропиленовых волокон, на 10 % из угольного волокна УГЦВ-1-Р. В качестве покрытия предлагается использование огнезащитного состава «АгниТерм М» с добавкой порошкообразных мелкодисперсных материалов, обладающих свойствами поглощения энергии электромагнитного излучения в широком диапазоне частот: технический углерод, активированный уголь. Для реализации поставленной цели были сформированы образцы экранов ЭМИ с площадью основания 0,6×0,6 м^2 с плоской формой поверхности. После замеса связующего материала с сухими смесями, композиционные покрытия были нанесены на поверхность нетканого игольнопробивного полотна толщиной 0,3 мм. Измерение экранирующих характеристик проводилось на автоматизированном измерителе модуля коэффициентов передачи и отражения SNA 0.01–18 в диапазоне частот 0,7…3,0 ГГц.

Результаты измерений разработанных гибких конструкций экранов ЭМИ на основе углеродсодержащих порошковых материалов показали, что образцы экранов ЭМИ на основе активированного угля позволяют получить значение коэффициента передачи в диапазоне частот 0,7…3,0 ГГц порядка –0,1…–2,9 дБ при коэффициенте отражения ЭМИ –5,0…–23,0 дБ (–1,0…–4,0 дБ в режиме короткого замыкания). С ростом частоты в диапазоне 2…17 ГГц наблюдается увеличение коэффициента передачи ЭМИ до -7,0 дБ. Для образцов экранов ЭМИ на основе технического углерода характерен коэффициент передачи –1,0…–2,6 дБ при коэффициенте отражения –5,0…–10,0 дБ (–1,0…–3,0 дБ в режиме короткого замыкания). В

диапазоне частот 2…17 ГГц наблюдается увеличение коэффициента передачи до –6,0 дБ при коэффициенте отражения –2,0…–10,0 дБ (–4,0…–12,0 дБ в режиме короткого замыкания).

Полученные результаты позволяют рекомендовать разработанные гибкие экраны электромагнитного излучения с углеродсодержащими покрытиями для экранирования СВЧ-источников, обеспечения экологической защиты пользователей ПК, обслуживающего персонала медицинских и промышленных установок.

СВЧ МОДУЛЬ ПОЛУДУПЛЕКСНОЙ СИСТЕМЫ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

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

Большой диапазон частот миллиметрового диапазона длин волн (ММДВ) и возможность обеспечения малой узкой диаграмм направленности при малых габаритах антенных устройств, позволяют улучшить пространственную и энергетическую скрытность системы связи. Произведена разработка малогабаритного приемо-передающего модуля восьмимиллиметрового диапазона длин волн, работающего в полудуплексном режиме.

Основные параметры канала передачи: диапазон частот – 36–36.8 ГГц; мощность выходного сигнала передающего устройства, более 2 Вт; значение промежуточной частоты входного сигнала, содержащего передаваемую информацию – 2 ГГц; длительность фронта радиоимпульса – 0,3 10^{-6} с; уровень побочных излучений, менее –50 дБ; допустимая входная мощность сигнала на входе приемного канала 1 Вт. Основные параметры канала приема: диапазон частот – 36–36,8 ГГц; коэффициент шума – 4 дБ; время включения и выключения канала приема 0.3 10^{-6} с.; полоса частот – 20 МГц; подавление зеркального канала, более 50 дБ.

Высокую стабильность частоты и скачки частоты выходного сигнала обеспечивает внешний синтезатор частот. Диапазон частот синтезатора 8,5–8,7 ГГц. Время переключения частоты выходного сигнала, менее $0{,}3 \cdot 10^{-6}$ с. Быстрое переключение частот выходного сигнала синтезатора позволяет обеспечить расширение спектра сигнала для обеспечения высокой энергетической скрытности работы системы связи. В разработанном блоке сигнал синтезатора частот усиливается и поступает на умножитель частоты на 4. На выходе умножителя установлен фильтр с полосой пропускания 34–34,8 ГГц. В канале передачи квадратурный смеситель сдвига формирует суммарное значение частот выходного сигнала умножителя и входного сигнала промежуточной частоты и формирует выходной сигнал передающего устройства 36–36,8 ГГц. При скачках частоты синтезатора частот изменение частоты выходного сигнала модуля в 4 раза больше, чем в выходном сигнале синтезатора. Синтезаторы частот канала приема и канала передачи синхронизированы, поэтому квадратурный смеситель канала приема формирует промежуточную частоту 2 ГГц, содержащую принимаемую информацию.

СИНТЕЗАТОР ЧАСТОТ С БЫСТРОЙ ПЕРЕСТРОЙКОЙ ЧАСТОТЫ И МАЛЫМ УРОВНЕМ ФАЗОВЫХ ШУМОВ

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

В настоящее время в системах телекоммуникаций все более широкое применение находят широкополосные сигналы. Они позволяют обеспечить шифрование и скрытность передаваемой информации. Одним из методов расширения спектра является скачкообразная перестройка частоты (FHSS). Реализация таких систем требует создания синтезаторов частот с малым временем переключения частоты выходного сигнала, малым уровнем фазовых шумов, большим диапазоном частот выходного сигнала. Широко используемые в системах телекоммуникаций синтезаторы частот с ФАПЧ не позволяют обеспечить требуемую совокупность параметров, поэтому в разработанном синтезаторе использованы методы прямого аналогового и прямого цифрового синтеза. Методом прямого аналогового синтеза формируются крупная и средняя сетки частот синтезатора, методом прямого цифрового синтеза – мелкая сетка частот. Крупная сетка частот формируется путем умножения частоты кварцевого генератора и выделением требуемых частотных составляющих выходного сигнала умножителя полосовыми фильтрами. Умножители частоты выполнены на диодах с

накоплением заряда. Выбор требуемого частотного канала крупной сетки частот обеспечивается коммутатором. Средняя сетка частот формируется путем деления частоты одной из спектральных составляющих крупной сетки частот. Мелкая сетка частот формируется синтезатором DDS. Требуемая частота выходного сигнала формируется путем суммирования одной из спектральных составляющих каждой сетки частот. Разработанный синтезатор частот позволяет обеспечить диапазон рабочих частот более 2 ГГц; время перестройки частоты выходного сигнала $0.3 \cdot 10^{-6}$ секунды; шаг сетки частот менее 1 МГц; уровень побочных излучений, менее –70 дБ; спектральную плотность мощности фазовых шумов выходного сигнала –105dBc/Hz@1kHz. Объем синтезатора частот при отсутствии средств виброзащиты не превышает $1.5\ 10^{-3}$ м^3.

МОДЕЛИРОВАНИЕ ТРАНЗИСТОРНЫХ СТРУКТУР С ИСПОЛЬЗОВАНИЕМ МОНОСЛОЯ ГРАФЕНА

В.В. Муравьёв, В.Н. Мищенко

Рассмотрены вопросы моделирования основных параметров и характеристик транзисторных структур с использованием монослоя графена. Высокая подвижность носителей заряда (максимальная подвижность электронов среди всех известных материалов) и другие его свойства делают графен перспективным материалом для использования в самых различных приложениях, в частности, широкого применения в интегральных приборах и микросхемах. Разработан алгоритм моделирования, составлена и отлажена программа численного моделирования методом Монте-Карло. Для моделирования использовался многочастичный метод Монте-Карло совместно с решением уравнения Пуассона для трехмерной области приборной структуры. На основе метода статистического моделирования проведены исследования основных механизмов рассеяния при переносе носителей заряда в полупроводниковых приборах на основе графена. Получены зависимости частот рассевания от энергии поля при рассеивании на полярных оптических фононах, на примесях, при акустическом рассеянии, при электрон-электронном рассеивании, а также суммарная зависимость по всем механизмам рассеивания. Установлено преобладание электрон-электронного рассеивания над другими видами рассеивания в области умеренных величин энергии поля. 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, типа 4H-SiC. Исходя из полученных результатов моделирования, выработаны рекомендации по формированию и совершенствованию технологии формирования приборов с улучшенными выходными параметрами в диапазонах СВЧ и КВЧ. Использование исследованных приборных структур со слоями графена позволит создать транзисторы, которые найдут применение в системах обнаружения сигналов и их обработки на крайне высоких частотах.

ВЛИЯНИЕ ДОБАВОК TiO_2 И ТЕХНИЧЕСКОГО УГЛЕРОДА НА ХАРАКТЕРИСТИКИ ЭКРАНОВ ЭМИ НА ИХ ОСНОВЕ

Дэйвис Исаиас Пеньялоса Овальес, М.В. Тумилович

Исследовались образцы экранирующих материалов на основе абразивного зерна электрокорунда, который представляет собой кристаллический оксид алюминия, искусственно получаемый в результате переплавки глинозема и глинозем-содержащего сырья непрерывным способом в дуговых печах с последующей кристаллизацией вещества. Электрокорунды принято подразделять в зависимости от процентного содержания глинозема в составе абразива и технологии производства. Чем больше в электрокорунде содержится окиси алюминия, тем тверже, прочнее и белее по цветовой характеристике получаемое корундовое абразивное зерно.

Для получения наполнителей с проводящими и диэлектрическими свойствами использовались дополнительные компоненты (30 % масс. содержания) в виде добавок диоксида титана (TiO_2), характеризующегося диэлектрическими свойствами и технического углерода, представляющий собой высокодисперсный аморфный наноматериал с поглощающими свойствами. Для реализации поставленной цели были сформированы образцы экранов ЭМИ в виде сухих смесей толщиной 5 мм. Для исследования экранирующих характеристик

сформированных образцов для экранов ЭМИ использовались панорамные измерители КСВН и ослабления. Измерения проводились в диапазоне частот 8,0…11,5 ГГц после проведения стандартных калибровок на прохождение и отражение.

Результаты измерений показали, что образцы на основе электрокорунда обеспечивают ослабление ЭМИ в диапазоне 8…12 ГГц порядка 4…5,5 дБ при коэффициенте отражения порядка –6…–8 дБ (в режиме короткого замыкания порядка –8…–9 дБ). При добавлении диоксида титана в основной состав экранирующего материала ослабление ЭМИ составляет порядка 3…5 дБ при коэффициенте отражения в пределах –6…–7,5 дБ (–10 дБ в режиме короткого замыкания). Использование технического углерода в качестве проводящего компонента позволило увеличить значение ослабления до 8…9 дБ при коэффициенте отражения –3…–5 дБ (–5…–9 дБ в режиме короткого замыкания).

Полученные результаты позволяют рекомендовать разработанные порошковые композиты для электромагнитного экранирования СВЧ-источников, обеспечения экологической защиты пользователей ПК, обслуживающего персонала медицинских и промышленных установок.

ЭКРАНИРОВАНИЕ СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ И КОНСТРУКЦИЙ ДЛЯ ЗАЩИТЫ ОТ УЛЬТРАФИОЛЕТОВОГО ИЗЛУЧЕНИЯ

Т.М. Печень, А.М. Прудник

В настоящее время на рынке стройматериалов представлены различные виды утеплителей, которые кроме теплоизоляционной функции выполняют еще и декоративную. Термопанели из пенополиуретана с клинкерной плиткой являются достаточно популярными в своём классе. Ультрафиолетовое излучение является одним из факторов, который может не только изменять внешний вид таких материалов, но и ухудшать их свойства в процессе эксплуатации.

Для обеспечения защитных свойств от излучения в диапазоне длин волн 200…400 нм необходимо наносить дополнительный слой светопоглощающей краски толщиной 100…200 мкм [1]. Клинкерная плитка изготавливается из керамики, как правило, толщиной 7…15 мм. Для улучшения показателей надёжности, стойкости и прочности можно использовать каолин как связующий материал.

В качестве заменителя утеплителей из полипропилена с клинкерной плиткой может выступить зернистая декоративная штукатурка с акриловым связующим. Компонентами такой штукатурки являются цветной песок и прозрачная акриловая дисперсия (20%) в качестве связующего с некоторыми технологическими добавками.

Однако, пенополиуретан обладает хорошими клеящими свойствами [2]. Показана возможность исключения акрилового связующего и нанесения цветного декоративного наполнителя на внешний слой полиуретановой пены, что позволило существенно снизить стоимость материала.

Литература

1. Qin J., Qu J., Song J.R., Song Z.N., Zhang W.D., Shi Y.X., Zhang T., Xue X., Zhang R.P., Zhang H.Q., Zhang Z.Y., Wu X. The optical properties of black coatings and their estimated cooling effect and cooling energy savings potential // Journal of Power and Energy Engineering. 2014. Vol. 2. P. 68–75.

2. Witkiewicz W., Zielinski A. Properties of The Polyurethane (PU) Light Foams. Advances in Materials Science, Vol. 6, No. 2 (10), October 2006.

ЭЛЕКТРОННЫЕ СВОЙСТВА ПРОВОДЯЩИХ КАНАЛОВ ПРИ ОБРАТИМОМ ЭЛЕКТРИЧЕСКОМ ПРОБОЕ НАНОСТРУКТУРЫ С ДИОКСИДОМ ГАФНИЯ

Д.А. Подрябинкин

В настоящее время активно исследуются наноструктуры с оксидными диэлектриками для устройств резистивной памяти с произвольным доступом (RRAM). В настоящей работе анализируется механизм формирования метастабильного состояния диоксида гафния в проводящих токовых каналах (филаментах), состоящий в сильном разогреве вплоть до

плазменного состояния, росте давления, последующем остывании и конденсации в виде метастабильного стеклообразного состояния. После снятия электрического импульса и остывания вещества в канале (после окончания электроформовки) испаренное вещество оседает на стенках канала, аморфизуется под давлением в области анода и превращается в стеклообразную неравновесную неупорядоченную систему. Между катодом и стеклообразным участком формируется область, в которой вещество отсутствует, т.е. вакуумная полость.

Проведено моделирование электронных свойств метастабильных атомарных структур, которые возникают в диоксиде гафния, содержащем кислород и кислородные вакансии, при формовке в электрических полях. Показано, что в зависимости от значений конфигурационных параметров ангармонический бистабильный потенциал ловушечных центров изменяет свою симметрию, а также глубину и ширину потенциальных ям.

Наличие периодического воздействия и шума приводит к переключению ловушечного состояния в диоксиде гафния из одного метастабильного состояния в другое. С увеличением амплитуды периодического воздействия частота переключений из одного состояния в другое растет. С ростом частоты периодического воздействия увеличивается частота переключений, а с ростом фазы увеличивается время нахождения ловушечного центра в одном из метастабильных состояний. Время переключения составляет порядка единиц наносекунд, а его величина снижается с ростом амплитуды периодического воздействия и интенсивности шума.

ЭКРАНИРУЮЩИЕ ХАРАКТЕРИСТИКИ ПОРОШКОВ КРИСТАЛЛОВ $AgIn_5S_8$ В СВЧ-ДИАПАЗОНЕ

Г.А. Пухир, Т.Г. Баругу

Соединение $AgIn_5S_8$ образуется в разрезе $Ag_2S–In_2S_3$ и относится к дефектным полупроводникам с концентрацией вакансий в катионной подрешетке ~ 25 %. В связи с наличием значительного количества дефектов электрические свойства этого соединения практически не изменяются при различных радиационных воздействиях, что позволяет выделить соединение $AgIn_5S_8$ в класс перспективных для создания ряда новых высокоэффективных радиационно-стойких оптоэлектронных приборов [1], [2]. Определенный интерес представляют электромагнитные свойства новых высокотехнологичных кристаллов в радиочастотном диапазоне и возможность их использования для создания экранов электромагнитного излучения (ЭМИ) и экранирующих покрытий. В работе проведены исследования экранирующих характеристик порошка монокристаллов $AgIn_5S_8$ в диапазоне 8…12 ГГц. Монокристаллы выращивали методом Бриджмена. Измерение характеристик ослабления и отражения проводилось с помощью панорамного измерителя КСВН и ослабления Я2Р-67 с использованием генератора ГКЧ−61 в диапазоне 8…12 ГГц. Ослабление ЭМИ образцами толщиной порядка 0,5 мм составляет порядка 6 дБ с равномерной дисперсией. Коэффициент отражения для исследуемых образцов на основе порошка $AgIn_5S_8$ составляет −3…−4 дБ в диапазоне 8…12 ГГц. Полученные результаты можно учитывать при необходимости электромагнитной совместимости компонентов при проектировании радио- и оптоэлектронных приборов и устройств. Применение порошков монокристаллов $AgIn_5S_8$ перспективно также для создания тонкопленочных экранирующих покрытий, эффективных в СВЧ-диапазоне.

Литература

1. Боднарь, И.В. Выращивание и свойства монокристаллов $AgIn_5S_8$ / И.В. Боднарь, Х.Т.М. Альрекаби, Т.Г. Баругу // Доклады БГУИР. – 2016. – №5(99). – С. 67–72.

2. Paorici, C. Crystal growth and properties of the $AgIn_5S_8$ compound / C. Paorici, L. Zanotti, N. Romeo, G. Sberveglieri, L. Tarricone // Materials Research Bulletin. – 1977. – Vol.12, Iss. 12. – P. 1207–1211.

СЛОЖНОКОМПОЗИТНЫЕ МАТЕРИАЛЫ ДЛЯ РАДИОПОГЛОТИТЕЛЕЙ ДИАПАЗОНА ЧАСТОТ 8–12 ГГЦ

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

Для известных типов конструкций радиопоглотителей (резонансных, градиентных, многослойных, с геометрически неоднородной поверхностью) применяются различные

материалы с резистивными, магнитными и диэлектрическими свойствами [1]. Величина проводимости, диэлектрической проницаемости и потерь, магнитной проницаемости сложнокомпозитных материалов, формируемых из радиопрозрачного связующего с порошковыми наполнителями, зависит от состава, концентрации, формы и размеров частиц наполнителей. Получены характеристики поглощения и отражения электромагнитного излучения сложнокомпозитных материалов на основе диэлектрических компонентов (TiO_2, ZrO_2, SiO_2, Al_2O_3, AlO), проводящих включений (на основе различных видов углерода), магнитных компонентов (Ni-Zn, Ni-Mn) в диапазоне частот 8–12 ГГц. С использованием алгоритма Николсона-Росса рассчитаны действительные и мнимые части диэлектрической и магнитной проницаемости сформированных сложнокомпозитных материалов. В специализированном пакете ПО CST Microwave Studio проведено электродинамическое моделирование характеристик отражения различных конструкций радиопоглотителей на основе полученных электрофизических свойств сформированных материалов.

Вследствие высокой действительной части диэлектрической проницаемости и низкого тангенса потерь материалы с исследованными диэлектрическими компонентами предложено использовать для формирования промежуточных диэлектрических слоев между резистивными покрытиями, что приводит к снижению рабочей толщины радиопоглотителя.

На основе образцов, содержащих проводящие включения, были смоделированы резонансные и многослойные радиопоглощающие структуры, с постепенным изменением резистивных потерь.

Магнитные компоненты сложнокомпозитных материалов обеспечивают дополнительное поглощение ЭМИ в диапазоне 8–12 ГГц при введении в многослойную конструкцию. Коэффициент отражения ЭМИ такими материалами составляет –12,0…–6,14 дБ.

Литература

1. Мицмахер М.Ю., Торгованов В.А. Безэховые камеры СВЧ. – М.: Радио и связь, 1982. – 128 с.

КОНСТРУКЦИЯ РАДИОПОГЛОЩАЮЩЕГО ПОКРЫТИЯ НА ОСНОВЕ ВЛАГОСОДЕРЖАЩЕГО КЕРАМЗИТА И ТИТАНОМАГНЕТИТА

С.Э. Саванович, Т.В. Борботько, А.А.А. Аль-Мамури

Одним из действенных методов, обеспечивающих противодействие получению информации о наземных объектах, например, военной техники, в диапазоне частот 2–12 ГГц является применение радиопоглощающих покрытий (РПП). Противодействие утечке информации посредством РПП обеспечивается в результате взаимодействия электромагнитных излучений (ЭМИ), распространяющихся в электромагнитном канале, с материалом покрытия, наносимого на поверхность защищаемых объектов. Выбор материалов, используемых для изготовления покрытий, осуществляется исходя из их радиоэкранирующих характеристик в диапазоне частот применения РПП, обусловленных магнитными и диэлектрическими потерями или потерями на проводимость.

Перспективным направлением представляется создание конструкций РПП на основе влагосодержащего керамзита, в поры которого введены водные растворы электролитов [1]. Повышение эффективности покрытий (снижение их коэффициента отражения), выполненных на основе влагосодержащего керамзита, может достигаться путем введения в радиопоглощающий композиционный материал компонента с отличной от нуля мнимой частью магнитной проницаемости μ'', порошкообразных ферритов.

Установлено, что введение в материал покрытия титаномагнетита позволяет снизить значения коэффициента отражения конструкции РПП, размещенной на металлической подложке в диапазоне частот 2–12 ГГц. Показано, что конструкция РПП, выполненная на основе влагосодержащего керамзита обеспечивает снижение значений коэффициента отражения в пределах –2,1 … –14,8 дБ, при введении в композиционный материал 20 % (по массе) титаномагнетита аналогичная конструкция обеспечивает снижение значений коэффициента отражения в пределах –2,4 … –19,8 дБ.

Литература

1. Саванович, С.Э. Радиоэкранирующие свойства электромагнитных экранов на основе влагосодержащего керамзита // С.Э. Саванович, В.Б. Соколов // Доклады БГУИР. – 2014. – №4 (82). – С. 48–51.

МОДЕЛЬ КРЫЛА ДЛЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

К.Н. Савик, В.П. Бурцева

Проблема создания беспилотных летательных аппаратов сегодня актуальна как никогда. Эти миниатюрные бесшумные «разведчики» обладают широким спектром сбора информации. Сканируя местность, беспилотники с помощью специальной аппаратуры могут производить фото и видео съемки; регистрировать все виды электромагнитного излучения в диапазоне – (радиоволны –γ-излучение); обнаруживать и определять положения различных объектов и т.д.

Основными задачами при создании беспилотных летательных аппаратов, особенно, специального назначения являются: уменьшение их собственного веса и увеличение их полезной нагрузки при поддержании лучших аэродинамических характеристик.

Аэродинамика крыла сложна и на сегодняшний день известна лишь в общих чертах. В истории авиации и воздухоплавания можно выделить несколько периодов, в течение которых среди ученых и изобретателей наблюдался повышенный интерес к идее машущего крыла и его аэродинамики. Ввиду неудач и сопряженных с ними разочарований интерес к этой проблеме временами ослабевал, а затем появлялся вновь. Проблема остается нерешенной и в наши дни. В течение 200 лет со времени построения первой летающей модели все попытки воспроизведения машущего крыла оказались практически безрезультатными.

В целях установления физической картины полета такого типа создана компьютерная модель крыла, на основании которой изучены его строение и принцип работы; рассчитаны скорость полета, число колебаний в секунду и максимальный угол поднятия крыла в воздухе; установлены вид полета (машущий, волнообразный), максимальный размах крыльев и максимальная площадь крыла.

ПРЕОБРАЗОВАТЕЛИ ДЛЯ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Т.А. Сайкалиев, А.В. Потапович, Г.В. Давыдов

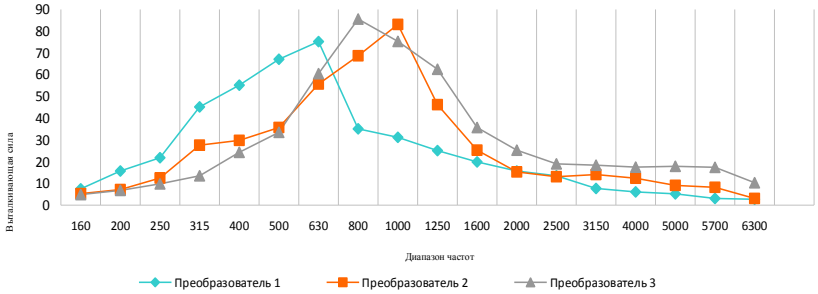
Защита речевой информации от утечки по виброакустическим каналам наиболее часто реализуется методом активной защиты, основанным на формировании маскирующих помех в ограждающих элементах конструкций помещений, воздушных вентиляционных каналах и воздушных объемах дверных тамбуров. Одним из определяющих элементов эффективной работы такой системы являются преобразователи, создающие маскирующие помехи в воздушных пространствах (вентиляционных каналах и дверных тамбурах) и преобразователи, создающие вибрационные маскирующие помехи в ограждающих элементах помещений (стены, пол, потолок, оконные стекла, трубы отопления и водоснабжения). В работе рассматриваются принципы построения и особенности конструкций преобразователей, создающих вибрационные маскирующие помехи. В связи с тем, что механизм прохождение звуковых волн, несущих речевую информацию, через ограждающие элементы конструкций помещений описывается процессами возбуждения в них многомодовых резонансных изгибных колебаний, а не процессами преломления акустических волн, потому и принципы создания в ограждающих конструкциях маскирующих помех и построения преобразователей должны учитывать это. Возбуждение изгибных колебаний в ограждающих конструкциях осуществляется по модели многоточечного силового воздействия, которая включает наличие инерционной массы и источника силы, расположенного между инерционной массой и ограждающей конструкцией. Преобразователи систем защиты речевой информации могут быть электромагнитными, электродинамическими и пьезоэлектрическими. Недостаток пьезоэлектрических преобразователей низкая выталкивающая сила на частотах до 400 Гц, а пьезоэлектрических – низкая выталкивающая сила на высоких частотах выше 4000 Гц. С конструктивной точки зрения электромагнитные и пьезоэлектрические преобразователи просты в изготовлении и надежны в эксплуатации по сравнению с электродинамическими

преобразователями. В конструкцию преобразователей предлагается внести изменения, основанные на сочетании электромагнитного и пьезоэлектрического преобразования электрических маскирующих сигналов в силовое воздействие на элементы ограждающих конструкций защищаемых помещений.

ИССЛЕДОВАНИЕ ВЫТАЛКИВАЮЩЕЙ СИЛЫ ПРЕОБРАЗОВАТЕЛЕЙ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

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

Эффективность работы активной системы защиты речевой информации определяется также и параметрами выталкивающей силы вибрационных преобразователей. Исследование выталкивающей силы вибрационных преобразователей проводились на установке, включающей генератор синусоидальных колебаний, датчик силы с предварительным усилителем, милливольтметр и инерционную массу. Инерционная масса представляла собой стальное цилиндрическое тело диаметром 100 мм и длиной 350 мм, что обеспечивало превышение массы тела в отношении массы исследуемых преобразователей более чем в 200 раз. На торец инерционной массы устанавливался датчик силы, на который устанавливался исследуемый вибрационный преобразователь, подключенный к генератору синусоидальных колебаний. Выталкивающая сила преобразователей определялась расчетным путем с учетом коэффициента преобразования датчика силы и показаний милливольтметра, подключенного к предварительному усилителю датчика силы. Исследования проводились на вибрационных преобразователях электромагнитного типа. Преобразователи включали ферритовый кольцевой магнит со стальным сердечником, закрепленным на пластине, прилегающей к одной из сторон магнита, мембрану, расположенную на расстоянии 0,3 мм от магнита с другой стороны и катушку возбуждения, установленную на стальной сердечник с магнитопроводом в виде круглой пластины и подключенную к генератору синусоидальных колебаний. В центре мембраны устанавливался шток для крепления преобразователя к ограждающим элементам конструкций помещений. Исследование выполнялись для диапазона частот от 160 до 5700 Гц при напряжении возбуждения преобразователя 3 В. На рисунке приведена зависимость выталкивающей силы от частоты возбуждения для различных конструктивных особенностей вибрационных преобразователей.



Преобразователь 1 – мембрана и магнитопровод толщиной 1 мм, преобразователь;
2 – мембрана толщиной 1 мм, магнитопровод толщиной 2 мм, преобразователь;
3 – мембрана и магнитопровод толщиной 2 мм

Рисунок 1. Зависимость выталкивающей силы от частоты возбуждения

ИСПОЛЬЗОВАНИЕ ЛАТЕНТНОГО РАЗМЕЩЕНИЯ ДИРИХЛЕ ДЛЯ ПОСТРОЕНИЯ ВЕРОЯТНОСТНЫХ ТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕКСТОВЫХ КОЛЛЕКЦИЙ

М.И. Селюк

В настоящее время в связи с бурным развитием сети Интернет наблюдается обилие электронной неструктурированной информации, представленной текстами на естественных языках. Все более востребованными становятся задачи автоматической обработки таких текстов с целью извлечения структурированных данных, в частности – задача тематической кластеризации (разбиения корпуса документов по тематике). На сегодняшний день все чаще данная задача решается с помощью вероятностных тематических моделей. Самым

распространенным алгоритмом построения тематических моделей является LDA, лишенный практически всех недостатков своих предшественников. Латентное размещение Дирихле (LDA, Latent Dirichlet Allocation) – это модель, объясняющая результаты наблюдений с помощью неявных групп, что позволяет получить объяснение, почему некоторые части данных схожи. Например, если наблюдениями являются слова, собранные в тексты, утверждается, что каждый текст представляет собой смесь небольшого количества тем и что появление каждого слова связано с одной из тем документа. LDA впервые был представлен в качестве графической модели для обнаружения тем Дэвидом Блеем, Эндрю Нг и Майклом Джорданом в 2002 году. Модель LDA устраняет такие недостатки популярных ранее моделей, как склонность к переобучению, невозможность вычислить вероятность нового документа и отсутствие закономерности при генерации документов из сочетания полученных тем.

Литература

1. Blei D., Ng A., Jordan M. Latent Dirichlet Allocation // Journal of Machine Learning Research. – MIT Press, 2003. – No. 3. – P. 993–1002.

2. Воронцов К. В. Математические методы обучения по прецедентам (теория обучения машин) // Курс лекций ВМК МГУ и МФТИ. – 2011.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНОГО ЛАТЕНТНТНО-СЕМАНТИЧЕСКОГО АНАЛИЗА ДЛЯ ПОСТРОЕНИЯ ВЕРОЯТНОСТНЫХ ТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕКСТОВЫХ КОЛЛЕКЦИЙ

М.И. Селюк, Н.Н. Шинкевич, М.В. Стержанов

Одной из важных задач автоматической обработки текстов является кластеризация текстовых коллекций. Для выявления скрытых тем в текстовых коллекциях в последнее время все чаще применяются вероятностные тематические модели. Одним из наиболее часто используемых алгоритмов для построения тематических моделей является PLSA.

Вероятностный латентно-семантический анализ (индексирование) (PLSA, Probabilistic Latent Semantic Analysis) был предложен Томасом Хоффманом в 1999 году. В основе метода лежит аспектная модель (aspect model), которая связывает скрытые (латентные) переменные тем с каждой наблюдаемой переменной словом или темой. Задача состоит в выявлении латентных переменных. Таким образом, каждый документ может относится к некоторым темам с некоторой вероятностью, что является отличительной особенностью этой модели по сравнению с походами, не основанными на вероятностном моделировании.

Достоинством метода можно считать его способность выявлять зависимости между словами, когда обычные статистические методы бессильны. PLSA также может быть применен как с обучением (с предварительной тематической классификацией документов), так и без обучения, что зависит от решаемой задачи. К недостаткам модели можно отнести склонность к переобучению и неприменимость к большим наборам данных, невозможность вычислить вероятность документа, которого нет в наборе данных, а также отсутствие какой-либо закономерность при генерации документов из сочетания полученных тем.

Литература

1. Manning C. D. Introduction to Information Retrieval // MIT Press, 2008.

2. Hofmann Thomas. Probabilistic latent semantic indexing // In Proc. of the SIGIR99.

ЭЛЕКТРОННЫЕ СВОЙСТВА ДЕФЕТНЫХ СТРУКТУР ФОСФОРЕНА

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

Точечные дефекты и примеси часто оказывают значительное влияние на физические свойства материала. Экспериментальное определение дефектов обычно крайне сложное и косвенное, кроме того, требует невероятных сочетаний различных методов. При исследовании дефектов, первопринципные методы показали себя как мощный теоретический подход, достаточно надежный, чтобы использоваться как предсказательный инструмент. Проведено квантово-механическое моделирование влияния моновакансии в слое черного фосфора (фосфорене), на его

структурные свойства. Расчеты проводились в программном комплексе VASP, который реализует метод теории функционала электронной плотности [1]. Данные моделирования показали, что наличие вакансии приводит к образованию трех оборванных связей, две из которых, благодаря гибкости фосфорена, соединяются друг с другом, а третья может иметь положительный, отрицательный и нейтральный заряд. Энергия образования нейтральной вакансии составила 1,88 эВ. Расчет электронной структуры нейтральной вакансии показал, что фосфорен теряет свою прямозонную природу за счет появления разрешенных состояний в запрещенной зоне.

Литература

1. Kresse, G. VASP the guide: tutorial / G. Kresse. –Vienna, 2003.

МНОГОСЛОЙНЫЕ ПЛЕНОЧНЫЕ ЭКРАНЫ НА ОСНОВЕ СПЛАВОВ NiFe ДЛЯ ЗАЩИТЫ ОТ ВНЕШНИХ МАГНИТНЫХ ПОЛЕЙ

А.А. Солобай, С.С. Грабчиков, А.В. Труханов

Над решением проблемы защиты изделий электронной и радиоэлектронной техники от воздействия различного типа внешних электромагнитных полей работают ведущие специалисты многих стран мира [1–3]. Известно, что наиболее эффективным способом защиты является экранирование. Была исследована эффективность экранирования переменных электромагнитных и магнитостатических полей многослойными пленочными структурами на основе сплавов NiFe, полученных методом электролитического осаждения, с целью разработки высокоэффективной защиты корпусов приборов и аппаратуры широкого спектра назначения. Было отмечено, что с ростом толщины экранов эффективность возрастает, что связано с увеличением площади экрана и, соответственно, снижением магнитного сопротивления, а пик максимума эффективности смещается в область более высоких магнитных полей. Для сопоставления полученных результатов с характеристиками промышленных материалов были измерены полевые зависимости экранов, изготовленных из промышленной аморфной ленты 84КХСР и электролитического сплава $Ni_{80}Fe_{20}$. Обнаружено, что магнитная проницаемость аморфной ленты высока только в ограниченном диапазоне, а затем резко падает, в отличии от магнитных электролитически осажденных пленок, которые эффективные в более высоких полях, начиная с 200 А/м. Сделан вывод, что при подборе изготовлении экранов для магнитостатической защиты следует учитывать как основные магнитные характеристики, так и роль неоднородности магнитного поля в объеме материала экрана, и связанную с этим нелинейность магнитной проницаемости.

Литература

1. Апполонский, С.М. / Расчеты электромагнитных полей / С.М. Апполонский, А.Н. Горский. – М.: Маршрут, 2006. – 992 с.

2. Gabower J.F. Electromagnetic interference shields for electronic devices: pat. USA № 7358447.

3. Кечиев, Л.Н. Экранирование технических средств и экранирующие системы / Л.Н. Кечиев, Б.Б. Акбашев, П.В. Степанов. – М.: Группа ИТД, 2010. – 470 с.

ПРОЕКТИРОВАНИЕ И ДИЗАЙН НА ОСНОВЕ ЦИФРОВЫХ ПРОТОТИПОВ AUTODESK ALIAS

В.А. Столер

Известно, что успех любого изделия определяется его качеством, стоимостью и брендом. Вместе с тем, в настоящее время тенденции таковы, что, более важную роль играет скорость создания модели изделия и его дизайна – они является главным преимуществом продукта. В докладе описываются особенности создания моделей различных изделий, в том числе защитных экранов ЭМИ, используя их цифровые прототипы и дизайн, разработанные на основе программы Autodesk Alias – популярной программы компании Autodesk (США).

Так как моделирование и дизайн определяют сколько времени и ресурсов придется потратить для создания изделия, то применение Alias делает ее незаменимой графической программой с возможностью получения математических моделей. Прогрессивная технология

цифровых прототипов Autodesk предоставляет конструкторам возможность проанализировать изделие еще на этапе его проектирования, и таким образом сократить общую стоимость разработки. Это позволяет активно экспериментировать с эскизами, трехмерными моделями редактируя их, сохраняя при этом историю изменений и сам процесс продвижения от начального эскиза до модели конечного продукта, создавая в то же время несколько вариантов его дизайна. В Alias есть возможность создавая эскизы, совмещать их с моделью, выбирая лучший вариант. Наличие в программе функций деформации и изменения геометрии позволяет управлять формой модели изделия, применяя такие инструменты, как Lattice Rig – создание произвольных форм используя так называемую решетку, Bend – управление деформацией, Conform – управление геометрией. Autodesk Alias позволяет работать с чертежами, созданных в других программах компании Autodesk, например AutoCAD и Inventor, для их дальнейшей доработки. Модели образцов изделий можно распечатать на 3D принтере, используя FDM технологию [1].

Литература

1. Столер В.А. // Технические средства защиты информации: тез. докл. XIV Белорусско-российской НТК. Минск, 25–26 мая 2016 г. С. 70.

ОСОБЕННОСТИ АВТОЭЛЕКТРОННОЙ ЭМИССИИ КРЕМНИЕВЫХ ОСТРИЙНЫХ КАТОДОВ

А.Г. Трафименко

В настоящее время активно исследуются наноструктуры, содержащие вакуумные промежутки. Такие наноструктуры перспективны для создания нового поколения твердотельных приборов обработки информации в силу имеющихся очевидных преимуществ, таких как высокая скорость электронов, минимизация процессов их рассеяния, снижение рассеиваемой мощности. Особую привлекательность вакуумной наноэлектронике придает тот факт, что они могут быть изготовлены на основе существующей кремниевой технологии. Одной из важнейших задач вакуумной наноэлектроники является исследование процессов автоэлектронной эмиссии для ряда перспективных материалов, в том числе кремния.

В данной работе рассматриваются результаты расчетов туннельной прозрачности и тока автоэлектронной эмиссии кремниевого острийного катода методом фазовых функций. Суть метода состоит в том, что вычисляется не сама волновая функция, а только ее изменение в потенциале, что существенно упрощает расчеты без потери точности. Простота метода состоит в решении обыкновенного дифференциального уравнения первого порядка (уравнения Риккати). Физический смысл фазовой функции заключается в том, что она является фазой рассеяния на соответствующей части потенциального рельефа.

Модель поверхностного потенциального рельефа учитывает наличие силы зеркального отображения, плотности поверхностных состояний, центров рассеяния носителей заряда, состава поверхности (наличия чужеродных включений, понижающих потенциальный барьер).

Анализируются результаты расчетов туннельной прозрачности поверхностного барьера кремния и тока автоэлектронной эмиссии при изменении прикладываемого внешнего электрического поля в зависимости от потенциального рельефа поверхности кремния и ее геометрии. Показано, что такие особенности потенциального рельефа поверхности кремния, как потенциальные ямы, приводят к существенному росту туннельной прозрачности и тока эмиссии.

ОБЕСПЕЧЕНИЕ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ ПРИ ИСПОЛЬЗОВАНИИ МАТЕРИАЛОВ НА ОСНОВЕ ЗАМЕЩЕННЫХ ГЕКСАГОНАЛЬНЫХ ФЕРРИТОВ

А.В. Труханов, С.С. Грабчиков, А.А. Солобай, С.В. Труханов

Требования современной техники в области увеличения скоростей и объемов передачи информации могут быть удовлетворены путем перехода с сантиметрового диапазона длин волн в миллиметровый диапазон (30–100 ГГц). Также при этом остро стоит вопрос об обеспечении внутрисистемной и межсистемной электромагнитной совместимости блоков

микроэлектронного и радиоэлектронного оборудования. На сегодняшний день гексаферриты М-типа (многокомпонентные магнитные оксиды) – наиболее перспективные для практических применений. Диапазон резонансного поглощения данных материалов лежит в области 50 ГГц и существует возможность контролируемого управления поглощающими свойствами в широком диапазоне частот путем незначительного изменения химического состава. Осуществлять частотно-селективное управление поглощающими характеристиками в гексаферритах можно путем смещения частоты естественного ферромагнитного резонанса (ЕФМР) за счет изменения величины магнитокристаллической анизотропии (путем диамагнитного замещения ионов железа или внешним магнитным полем). Проведены измерения коэффициентов прохождения (ослабления ЭМИ) в диапазоне частот 25,8–78,3 ГГц и во внешних магнитных полях до 8 кЭ для керамических образцов твердых растворов Al-замещенных гексаферритов бария М-типа $BaFe_{12-x}Al_xO_{19}$ (x = 0,1–1,2). Показано, что замещение ионами алюминия увеличивает магнитокристаллическую анизотропию в гексаферритах М-типа и индуцирует смещение пика ЕФМР в область более высоких частот (от 51 ГГц для x = 0,1 до 61 ГГц для x = 1,2). Отмечено, что с ростом концентрации ионов алюминия амплитуда пика ЕФМР уменьшается с –30 дБ (x = 0,1) до –20,5 дБ (x = 1,2), обеспечивая уменьшение энергии прошедшего ЭМИ на 2–3 порядка в целом. Причиной снижения амплитуды может являться снижение магнитных потерь из-за фрустрации магнитной структуры гексаферрита. Установлено, что наложение внешнего магнитного поля (8 кЭ) позволяет контролируемо сдвигать пик резонансного поглощения в более высокочастотную область (вплоть до 78 ГГц). Это дает возможность управлять микроволновыми характеристиками допированных ионами алюминия гексаферритов бария в аномально широком частотном диапазоне (от 51 ГГц до 78 ГГц), что открывает перспективу для практических применений в СВЧ-технике и обеспечении ЭМС.

АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ FPGA

Н.С. Уваров, Д.И. Шуманский

В современном мире не обойтись без сохранения данных, алгоритмы шифрования присутствуют везде. В данной работу была поставлена задача реализации DES шифрования на базе FPGA с использованием конвейера. DES (Data Encryption Standard) – симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт.DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм используют комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для Des рекомендовано несколько режимов. DES был национальным стандартом США в 1977- 1980 гг. но в настоящее время DES используется (с дины 56 бит) только для устаревших систем, чаще всего используют его более криптоустройчивый вид (3DES, DESX). 3DES является простой эффективной заменой DES, и сейчас он рассмотрен как стандарт. Алгоритм DES широко применяется для защиты финансовой информации. В работе был реализован алгоритм шифрования DES с конвейерной обработкой на базе FPGA. В ходе работы были получены следующие результаты: рабочая частота, аппаратные затраты и потребляемая мощность.

Литература

1. Панасенко, С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БВХ-Петербург, 2009.

2. Бибило, П.Н. Основы языка VHDL / П.Н. Бибило. – М.: Издательство ЛКИ, 2007.

ТОНКИЕ ПЛЕНКИ КЕСТЕРИТА НА НАНОСТРУКТУРИРОВАННОЙ АЛЮМИНИЕВОЙ ПОДЛОЖКЕ ДЛЯ ФОТОВОЛЬТАИЧЕСКИХ ЭЛЕМЕНТОВ

Е.А. Уткина, А.И. Воробьева, Е.А. Чекмарев

Создание автономных систем электроснабжения средств защиты информации является актуальным направлением современной электроники. Разработка недорогих и экологически безопасных фотоэлектрических элементов и батарей на их основе является одним из таких

направлений. Четверные полупроводники на основе сульфидов меди, цинка, олова–кестерита Cu_2ZnSnS_4(CZTS) интенсивно исследуются в последнее время для использования в качестве слоя-поглотителя тонкопленочных фотовольтаических элементов благодаря оптимальному значению ширины запрещенной зоны (1,5 эВ) и высокому коэффициенту оптического поглощения (10^4 $см^{-1}$). Все составные элементы (и исходные реактивы) нетоксичны и достаточно широко распространены в природе, что позволяет сократить стоимость при высокой эффективности фотопреобразования (достигнутая эффективность фотоэлементов превысила 12 % в 2014 г.).

Для формирования пленок Cu_2ZnSnS_4 использовали метод SILAR, как наиболее простой и экономичный способ формирования многокомпонентных полупроводниковых соединений. Растворы осаждения имели следующий состав: катион-содержащего прекурсора 0.1 M $CuSO_4$, 0.05 M $ZnSO_4$, 0.05 M $SnCl_2$ (раствор 1) и анион-содержащего прекурсора 0.2 M Na_2S (раствор 2). Толщина пленок составляла от 0,1 до 0,7 мкм. В качестве подложки для осаждения пленок кестерита использовали наноструктурированный слой алюминия, полученный после удалением анодного пористого оксида алюминия.

Структурно-фазовые исследования показали наличие в свежеосажденных пленках двух соединений Cu_2SnS_3 и ZnS. В результате химического взаимодействия во время отжига при температуре 250°C в течение 2 ч были получены пленки Cu_2ZnSnS_4. Использование наноструктурированного основания позволило повысить эффективность поглощения солнечного излучения. Установлено также влияние наноструктурированной подложки на эффективную ширину запрещенной зоны.

ПЛАЗМОННЫЕ ЭФФЕКТЫ В ГРАФЕНОВОЙ ПОЛЕВОЙ ГЕТЕРОСТРУКТУРЕ

А.В. Фельшерук, А.Л. Данилюк

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 электромагнитного излучения в терагерцевом диапазоне (1–15 ТГц) в зависимости от величины потенциала полевого электрода, температуры, толщины диэлектрика и плотности поверхностных состояний на границе раздела металл/диэлектрик. 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. 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.

ЭЛЕКТРИЧЕСКАЯ МОДЕЛЬ HISIM2 ДЛЯ СХЕМОТЕХНИЧЕСКОГО МОДЕЛИРОВАНИЯ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

В.Т. Ханько

Непрерывное уменьшение геометрических размеров элементов ИМС, применение новых конструктивных решений и материалов при их производстве сопровождается появлением новых физических эффектов, механизмов генерации и транспорта носителей

заряда в приборах, изготовленных в соответствии с нанометровыми проектными нормами.

Модель HiSIM основана на решении уравнения Пуассона в предположении, что толщина инверсионного слоя равна нулю, и в приближении плавного канала. Эти допущения позволяют получить аналитические зависимости для всех характеристик транзистора в виде функции от поверхностного потенциала у истока и стока [1].

Модель HiSIM2 решает уравнение Пуассона численными методами, что позволяет точно воспроизвести производные тока стока по напряжениям на затворе и стоке. Многие модели МОП-транзисторов используют нефизические параметры для сглаживания электрических характеристик при переходах между различными режимами работы. Модель HiSIM2 использует только один набор уравнений с физическими параметрами, адекватно описывающий функционирование приборов во всех режимах работы. Понятие поверхностного потенциала позволяет получить одно общее выражение для суммы диффузионного и дрейфового тока, что исключает необходимость применения слаживающих функций.

Посредством использования модуля UTMOST программного комплекса Silvaco проведена экстракция параметров модели HiSIM2 для *n*-МОП-транзисторов, изготовленных по технологии, обеспечивающей минимальную длину канала 90 нм. При этом использовалась стратегия экстракции с применением методов оптимизации генетического алгоритма и Левенберга-Марквардта [2]. Для экстракции параметров модели HiSIM2 был использован набор МОП-транзисторов с различной длиной канала (90 нм, 130 нм, 180 нм, 500 нм, 1 мкм, 2 мкм, 5 мкм, 10 мкм). Относительная погрешность вольт-амперных характеристик, рассчитанных с использованием экстрагированного набора параметров модели HiSIM2, в сравнении с экспериментальными данными составила не более 7 %.

Литература

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

2. Mattausch, H. The HiSIM compact model family for integrated devices containing a surface-potential MOSFET core / H.J. Mattausch, M. Miura-Mattausch, N. Sadachika, M. Miyake // Mixed Design of Integrated Circuits and Systems, 2008. MIXDES 2008. – P. 39–50.

ТЕПЛОВОЕ СКАНИРОВАНИЕ ОТПЕЧАТКА ПАЛЬЦА ЧЕЛОВЕКА С ИСПОЛЬЗОВАНИЕМ ПЕРФОРИРОВАННОЙ МАСКИ ИЗ АНОДНОГО ОКСИДА АЛЮМИНИЯ

П.А. Хицун

Известно множество способов защиты как информации, так и физических объектов, которые применяются в зависимости от необходимого уровня безопасности для конкретного объекта. Одними из таких способов защиты являются биометрические системы, а точнее системы идентификации по отпечаткам пальцев. Такие системы приобрели широкое распространение и в дальнейшем имеют хорошие перспективы развития за счет своей адаптивности. Внедрение биометрических технологии и, в частности распознавания отпечатков пальцев, значительно усиливает степень защиты объекта, а также заметно увеличивает качество идентификации за счет исключения необходимости в специальной карте, пропуске, ключе, нужен только уникальный отпечаток, который невозможно забыть или потерять. Системы основанные на дактилоскопии сравнивают полученный отпечаток памяти с другими отпечатками, которые хранятся в базах системы или же с отпечатком конкретного человека, способ сравнения также зависит от сферы применения данной технологии.

Термосканеры (Thermal Scanners) – в таких устройствах используются датчики, которые состоят из пироэлектрических элементов, позволяющих фиксировать разницу температуры и преобразовывать ее в напряжение. При прикладывании пальца к сканеру по температуре прикасающихся к пироэлектрическим элементам выступов папиллярного узора и температуре воздуха, находящегося во впадинах, строится температурная карта поверхности пальца, которая в дальнейшем преобразуется в цифровое изображение. Температурный метод имеет множество преимуществ: высокая устойчивость к электростатическому разряду; устойчивая работа в широком температурном диапазоне; эффективная защита от муляжей.

К недостаткам данного метода можно отнести то, что изображение быстро исчезает. При прикладывании пальца в первый момент разница температур значительна и уровень сигнала, соответственно, высок. По истечении короткого времени (менее одной десятой доли секунды) изображение исчезает, поскольку палец и датчик приходят к температурному равновесию. Одним из перспективных направлений является создание экранов на основе слоев пористого анодного оксида алюминия с встроенными углеродсодержащими соединениями. С одной стороны, анодный оксид алюминия – диэлектрик, который имеет пористую микроструктуру с контролируемыми параметрами, а с другой стороны, образцы, полученные в органических кислотах, могут содержать в своем составе аморфный углерод, который служит активной фазой для поглощения ЭМИ. В литературе в настоящее время отсутствуют данные о применении пористого анодного оксида алюминия с встроенными углеродсодержащими соединениями для экранирования ЭМИ и его экранирующих характеристик.

Литература

1. Электромагнитные излучения методы и средства защиты / В.А. Богуш [и др.]; под общ. ред. Л.М. Лынькова. – Минск: Бестпринт, 2003. – 406 с.

2. Ахмед Али Абдуллах Аль-Дилами. Исследование экранирующих свойств пористых матриц на основе анодного оксида алюминия / Ахмед Али Абдуллах Аль-Дилами, И.А. Врублевский, К.В. Чернякова, Г.А. Пухир // Современные средства связи: материалы XVII Междунар. науч.-техн. конф.

RC-ЗАДЕРЖКА СИГНАЛА В МЕЖСОЕДИНЕНИЯХ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

А.Г. Черных, В.В. Шульгов

Комплексный подход к обеспечению информационной безопасности требует улучшения параметров микроэлектронных приборов защиты информации. Совершенствование микроэлектронных приборов связано с увеличением быстродействия и уменьшением их размеров. Однако при уменьшении размеров проблема межсоединений интегральных микросхем (ИМС) становится главным лимитирующим фактором дальнейшего развития, так как временные емкостно-резистивные задержки (RC-задержки) распространения сигнала между транзисторами ограничивают быстродействие ИМС.

В работе представлена тестовая матрица, которая позволяет провести измерения паразитной емкости трехуровневой структуры металлических межсоединений ИМС. Тестовая структура выполнена по 0.35 мкм КМОП технологии.Согласно упрощенным представлениям, для субмикронных ИМС модель емкости токопроводящих дорожек складывается из емкости параллельных пластинок $C_{L\text{-}G}$ и краевой емкости $C_{L\text{-}L}$. С целью аттестации технологического процесса, было произведено измерение паразитной емкости трехуровневой структуры межсоединений тестовой матрицы с помощью измерителя иммитанса Е7-20. Так же было произведено моделирование паразитной емкости с помощью программного пакета COMSOL Multiphysics. Представлена корреляция полученных результатов.

Проведена оценка влияния материала с низкой диэлектрической постоянной на величину паразитной емкости.Применение материалов с диэлектрической постоянной меньше, чем у диоксида кремния, позволяют на треть снизить емкостную составляющую RC-задержки. Исходя из результатов исследований, можно говорить о целесообразности использования COMSOL Multiphysics для быстрого определения емкостной составляющей RC-задержки сигнала в межуровневой структуре межсоединений интегральных микросхем.

МОДЕЛИРОВАНИЕ ВЛИЯНИЯ ТЕМПЕРАТУРЫ, ИСТОЧНИКА И ИНТЕНСИВНОСТИ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ НА ЭЛЕКТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ СУБМИКРОННЫХ МОП-ТРАНЗИСТОРОВ

Н.А. Яцевич, В.Р. Стемпицкий, И.Ю. Ловшенко

Основным методом оценки и прогнозирования радиационной стойкости интегральных микросхем (ИМС) является изучение механизмов возникающих в твердом теле радиационных эффектов. Известно, что неравновесные носители заряда, возникающие в процессе облучения

МОП-структуры, приводят к изменению заряда в объеме окисла и на границе оксид-полупроводник. Для успешного моделирования процесса накопления заряда в диэлектриках и на границе оксид-полупроводник необходимо учитывать следующие физические процессы: генерация/рекомбинация электронно-дырочных пар, транспорт носителей заряда, захват носителей заряда. С использованием программного комплекса компании Silvaco выполнено моделирование электрических характеристик приборной структуры *n*-канального МОП-транзистора при воздействии ионизирующего излучения рентгеновского и нуклидного источника Co_{60} при вариации температур. Анализ результатов расчетов позволил сделать следующие выводы.

1. Снижение температуры приводит к возрастаю влияния ИИ на ток стока. Так при температуре 303 К максимальный ток стока I_c без воздействия составляет $3{,}5\cdot10^{-5}$ А, с полной поглощенной дозой TID =1 Мрад $I_{срен}=3{,}62\cdot10^{-5}$А для рентгеновского источника (отклонение 3,43 %) и $I_{скоб} = 3{,}65\cdot10^{-5}$А для нуклидного источника Co_{60} (отклонение 4,29 %). При понижении температуры до 233 К $I_c = 5{,}2\cdot10^{-5}$А, $I_{срен} = 5{,}5\cdot10^{-5}$А, $I_{скоб} = 5{,}6\cdot10^{-5}$А (отклонение 5,77 % и 7,69 % соответственно). Для температуры 383 К: $I_c =2{,}3\cdot10^{-5}$А, $I_{срен} = 2{,}35\cdot10^{-5}$А, $I_{скоб} = 2{,}38\cdot10^{-5}$ А (отклонение 2,17 % и 3,4 8% соответственно).

2. Изменение интенсивности излучения от 1 рад/с до 100 рад/с оказывает малое влияние на электрические характеристики (максимально отклонение составляет не более 0,1% от среднего значения, соответствующего поглощенной дозе).

Исследования выполнялись в рамках задания 3.1.02 Государственной программы научных исследований «Фотоника, опто- и микроэлектроника».

СЕКЦИЯ 5
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ

ЗАЩИТА АВТОМОБИЛЕЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В.М. Алефиренко, В.С. Андрушкевич

Проблема угона автомобилей с каждым годом становится все более актуальной, также, как и развитие различных видов защиты от этой угрозы. Рассмотрим основные технические решения, применяемые для защиты автомобилей от несанкционированного доступа (системы защиты), способы обхода этих систем и соответствующие им способы, затрудняющие взлом систем в порядке их развития.

1. Использования ключа с иммобилайзером.

Иммобилайзер – это противоугонное средство, выключение и включение которого должно быть доступно только владельцу автомобиля. В шляпке ключа замка зажигания находится электронный транспондер (чип). Вокруг замка зажигания намотана специальная считывающая рамка (катушка). При включении зажигания катушка создает электромагнитное поле, которое проходит через чип. Чип получает энергию этого поля и передает свой код. Если код верный, иммобилайзер дает команду на запуск двигателя. К способам взлома системы защиты можно отнести: подключение через диагностический разъем и перепрошивка электронного блока управления, копирование ключа. К способам защиты – ввод дополнительной скрытой кнопки включения, блокировка доступа к диагностическому разъему и цифровой шине, ремонт автомобилей только на сертифицированных СТО.

2. Пассивный ключ с дистанционным открыванием дверей.

Дистанционное управление осуществляется с помощью брелока, который совмещен с физическим ключом зажигания. С помощью брелока осуществляется постановка и снятие сигнализации с охраны, а также контроль состояния автомобиля. Связь между сигнализацией и брелоком осуществляется по радиоканалу. Для защиты информации от перехвата осуществляется ее кодирование. К способам взлома системы защиты можно отнести: сканирование радиоканала с применением сканеров-кодграбберов, применение электрошоковых приборов. К способам защиты – использование сигнализаций с динамическим кодом, использование более сложных сигнализаций с наличием дополнительных модулей, позволяющих осуществлять контроль автомобиля в реальном режиме времени (GPS, GPRS и т.д.), оснащение автомобилей высоковольтными разрядниками.

3. Активный ключ с дистанционным открыванием дверей.

Бесключевой доступ – это система доступа к автомобилю с использованием особой электронной карты (смарт-ключа). Компьютер автомобиля на небольшом расстоянии обменивается кодами со смарт-ключом, идентифицирует его и дает команду на открытие дверей. При удалении на некоторое расстояние компьютер теряет смарт-ключ из виду и запирает автомобиль. К способам взлома системы защиты можно отнести: доступ к диагностическому разъему и прошивка новых ключей, использование ретрансляторов, позволяющих увеличить радиус опроса сигнализации. К способам защиты – уменьшение радиуса действия системы сигнализации, использование фольгированных чехлов для брелока, ввод дополнительных радиометок, использование «интеллектуальных» модулей защиты, оснащение смарт-ключа кнопкой выключения питания, изъятие источника питания из брелока после постановки автомобиля на охрану, блокировка доступа к диагностическому разъему и цифровой шине.

МОЩНЫЕ СВЕТОДИОДНЫЕ ПРОЖЕКТОРЫ НА ОСНОВЕ ОБЪЕДИНЕНИЯ АЛЮМИНИЕВЫХ ПЛАТ ДЛЯ СИСТЕМ ОХРАННОГО ОСВЕЩЕНИЯ

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

Современные системы освещения на охраняемом объекте проектируются и устанавливаются совместно с системой видеонаблюдения охранного периметра. Дополнительно система охранного освещения комплектуется аварийным освещением, в задачи

которого входит автоматическое включение по сигналу тревоги от датчиков охраны периметра. Поэтому задачей систем охранного освещения является обеспечение как требуемого уровня освещенности на охраняемом объекте, так и поддержание оптимальной видимости с учетом используемых камер видеонаблюдения по периметру объекта. В настоящее время для решения этих задач все шире находят применение мощные светодиодные прожекторы.

В данной работе представлены результаты разработки мощного светодиодного прожектора на основе четырех светодиодных алюминиевых плат. Плата из алюминия со слоем нанопористого оксида алюминия содержала 24 SMD чипа белых светодиодов. Использование платы из алюминия с низким тепловым сопротивлением позволило снизить температуру кристалла светодиода для рабочего режима до 60–70 °С.

В конструкции светодиодной платы использовался высокостабильный LED драйвер (Интеграл, г. Минск) с питанием от двухполупериодного выпрямителя сети переменного тока. Достоинством разработанного мощного светодиодного прожектора является низкое энергопотребление, яркий и равномерный светодиодный поток, широкий диапазон рабочих температур и повышенная устойчивость к механическим повреждениям.

ОБНАРУЖЕНИЕ МАЛОКОНТРАСТНЫХ ОБЪЕКТОВ В ОПТИЧЕСКОМ ДИАПАЗОНЕ ДЛИН ВОЛН

А.С. Мамченко, Е.И. Хижняк

На сегодняшний день функционирование и развитие Вооруженных Сил Республики Беларусь немыслимо без применения современных средств маскировки и разведки. При осуществлении мероприятий разведки, предусматривающих обнаружение объекта, определение его типа и характеристик, целесообразно использовать оптико-электронные системы (ОЭС) в пассивном или полуактивном режиме функционирования.

Актуальной проблемой является качественный анализ оперативный обстановки на театре военных действий (ТВД), заключающийся в сборе, обработке и предоставлении результирующих данных в виде, удобном как для восприятия командиром, так и автоматизированной системой обработки информации. Как показывает практика, обычные ОЭС, работающие по уже разработанным алгоритмам функционирования, не обеспечивают требуемой скорости и точности обнаружения объекта.

Повышение эффективности ОЭС за счет применения перспективных методов обнаружения позволяет повысить качество восприятия информации командирами, что в конечном итоге приводит к повышению скорости и эффективности выполнения задач боевого управления специальными подразделениями, снижению материальных и временных затрат, повышению эффективности ОЭС разведки в целом.

Важность работы обусловлена необходимостью обеспечения скрытного ведения разведки на ТВД, а также высокой скорости обработки полученных данных.

Таким образом, в настоящее время, важными являются исследования по повышению эффективности существующих ОЭС и разработке рекомендаций по маскировке и ведению технической разведки.

Для решения указанной задачи необходимо выполнить следующие этапы:

– провести анализ работы ОЭС разведки с электронно-оптическим поляризатором в различных условиях;

– разработать методы и алгоритмы обработки полученных данных с помощью программного обеспечения;

– разработать технические рекомендации по маскировке и разведке.

Реализация поставленных этапов позволит значительно увеличить скорость получения и обработки результирующих данных.

Литература:

1. Беляев, Б.И. Оптическое дистанционное зондирование / Б.И. Беляев, Л.В. Катковский. – Минск: БГУ, 2006. – 455 с.

2. Спектрополяризационные контрасты в задачах дистанционного зондирования / Ю.В. Беляев [и др.] //Журн. прикл. спектроскопии. – 2001. – Т. 68, № 2. – С. 258–263.

ОБРАБОТКА ИЗОБРАЖЕНИЙ, ПОЛУЧЕННЫХ ОТ ИСТОЧНИКОВ ИНФОРМАЦИИ ОПТИЧЕСКОГО ДИАПАЗОНА РАЗЛИЧНЫХ ЧАСТОТНЫХ СПЕКТРОВ

Е.И. Михненок, Е.И. Хижняк

Постоянное совершенствование средств разведки, привело к активному развитию многоканальных систем мониторинга фоноцелевой обстановки, предполагающих совместное использование разнообразных приборов и датчиков: оптических, инфракрасных и др. Такие системы мониторинга позволяют получать информацию о наблюдаемой сцене в различных диапазонах электромагнитного излучения. Данные зондирования поступают в виде цифровых многоспектральных изображений для обработки на ЭВМ, поэтому проблематика тесно связана с цифровой обработкой изображений.

Яркость, размеры и форма объектов на изображениях одной и той же сцены могут заметно различаться при регистрации в разных диапазонах электромагнитного излучения в зависимости от свойств поверхности объектов, а также характеристик среды. Чтобы извлечь больше информации из совокупности полученных изображений, прибегают к процедуре их комплексирования. Комплексированием изображений называется процесс объединения информации от нескольких изображений полученных в различных спектральных диапазонах в одно более информативное, чем любое из исходных изображений.

Комплексирование изображений является сложным процессом, который включает в себя получение исходных снимков, их предварительную обработку, оценку информационного содержания, а также саму процедуру комплексирования. Основными проблемами, возникающими при комплексировании, являются низкая контрастность снимков, высокая степень избыточности информации, и, как следствие, большой объем данных, подлежащих обработке.

Существующие на сегодняшний день алгоритмы комплексирования не всегда соответствуют указанным требованиям, поэтому разработка эффективных алгоритмов комплексирования изображений, позволяющих представить регистрируемую информацию в наиболее информативном виде, является актуальной задачей и определяет необходимость проведения исследований.

Литература

1. Обработка и анализ изображений в задачах машинного зрения / Ю.В. Визильтер [и др.] – М.: Физматкнига, 2010.

2. Михеев, С.М. Комплексирование изображений разных диапазонов спектра в многоканальных системах наблюдения / С.М. Михеев. Москва: МАИ, 2011.

ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБОРУДОВАНИЕ ГОСУДАРСТВЕННЫХ ГРАНИЦ

И.В. Щербаков, А.В. Рылик

В 2015–2016 гг. обстановка в странах Европы сложилась неблагоприятная. Увеличилась интенсивность совершения террористических актов, а также незаконного поведения беженцев. В настоящий исторический период страны Европы пытаются остановить поток прибывающих к ним мигрантов, в числе которых могут оказаться потенциальные террористы, агенты иностранных разведок, участники бандформирований. Особую опасность в современных условиях представляет обстановка складывающаяся на приграничной территории европейских стран. В условиях наметившейся в последнее время тенденцией к увеличению незаконной миграции, повышение роли политических, дипломатических, контрольно-административных, оперативно-розыскных подходов к решению возникающих проблем не способствуют ее уменьшению. Проведенный анализ опыта инженерного оборудования границ рядом зарубежных стран показал, что единственным барьером позволяющим сдерживать потоки населения на путях международной миграции остаются инженерно-технические заграждения.

Именно с такой целью США решились на строительство заграждений на рубеже с Мексикой, Индия с Бангладеш и Бирмой, Саудовская Аравия с Ираком и Йеменом, Ботсвана с Зимбабве, Испания с Марокко, Южная Корея с Северной Кореей. Почти во всех этих случаях заграждения закрывали только наиболее проблемные участки границы.

С целью усиления границы в инженерном отношении на наиболее значимых участках устанавливаются технические средства охраны, позволяющие контролировать определенную зону ответственности, оборудуются физические барьеры для затруднения движения нарушителей в виде заборов различной модификации, а для препятствия проезда автомобильной техники – бетонные надолбы. В настоящее время по всему миру существует более 50-ти пограничных барьеров. Ситуация на границах Европейского союза, показывает, что изменения политической ситуации вынуждает правительства этих стран усиливать физическую защиту своих границ, возводить так называемые «стены» с использованием различных инженерных заграждений и технических средств охраны границы.

Таким образом, анализ рассмотренного опыта охраны границ рядом стран подтверждает, что сегодня основным путем по сдерживанию незаконной миграции, контрабанды, терроризма и др. является создание инженерно-технического барьера на государственной границе в сочетании с комплексом организационных, тактических и технических мероприятий.

КЛАССИФИКАЦИЯ ОБЪЕКТОВ ДЛЯ ОБОРУДОВАНИЯ СИСТЕМАМИ ВИДЕОНАБЛЮДЕНИЯ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОГО ПОРЯДКА

В.Н. Ярошевич, Ю.С. Краснов, Д.В. Калинин

В настоящее время в Республике Беларусь прорабатываются вопросы создания республиканской системы мониторинга общественной безопасности (РСМОБ). Основным ядром проектируемой РСМОБ будет являться модуль, основанный на интеграции систем/подсистем видеонаблюдения (телевизионных систем видеонаблюдения / охранного телевидения) объектов различных категорий.

Существующая в настоящее время в Республике Беларусь нормативно-правовая база, регламентирующая вопросы нормативно-правового, организационно-технического и технического обеспечения построения и функционирования систем видеонаблюдения в интересах обеспечения общественного порядка, носит выраженный сегментированный характер критериев / параметров эффективности и практику их применения.

В рамках исследования проведена классификация объектов для оборудования системами видеонаблюдения в интересах обеспечения общественного порядка:

– объекты, подлежащие обязательной охране Департаментом охраны МВД Республики Беларусь (видеонаблюдение зданий и помещений защищаемых объектов);

– объекты с местами массового пребывания людей (городское видеонаблюдение);

– критически важные объекты (атомная станция, объекты электроэнергетики);

– объекты, осуществляющие деятельность в сфере игорного бизнеса на территории Республики Беларусь;

– объекты, связанные с работой дискотек и культурно-развлекательных (ночных) клубов;

– объекты, не попадающие под действие специализированных НПА.

СЕКЦИЯ 6
ОБУЧЕНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБУЧАЮЩИЕ СИСТЕМЫ НА ОСНОВЕ ИНТЕРАКТИВНЫХ МУЛЬТИМЕДИЙНЫХ МОДУЛЕЙ

Л.А. Конюх, Н.И. Кобринец, С.Е. Карпович

Современные информационные технологии позволяют разрабатывать и эффективно применять различные средства обучения, моделирования и интерактивного исследования. Современный уровень персональных компьютеров и их программного обеспечения дают возможность разрабатывать алгоритмы и программное обеспечение обучающих систем, в том числе и в области технических средств защиты информации.

Научные исследования в этом направлении в последние годы ведутся в учебно-научной лаборатории «Математическое моделирование технических систем и информационные технологии» БГУИР [1]. Анимация, интерактивность и средства мультимедиа, применяемые в наших разработках, позволили создать программные средства – мультимедийные модули – для интерактивного исследования колебательных механических систем, пневматических элементов и систем и других технических объектов. Интерактивные мультимедийные модули разрабатываются как вполне законченные информационные страницы, содержащие запрограммированные математические алгоритмы физических законов или технических принципов. При этом алгоритм имитационного моделирования является сегментированным, то есть, каждый элемент, вводимый интерактивно на рабочее поле монитора, имеет алгоритмический интерфейс, согласованный с основным алгоритмом, описывающим объект визуализации. То же относится и к исключению элементов из рабочего поля. Исключенный элемент как сегмент алгоритма, не нарушает функциональность и достоверность расчета по основному алгоритму, обеспечивающему моделирование и визуализацию.

В настоящей работе рассматривается возможность приложения полученных результатов к разработке интерактивных мультимедийных модулей для технических средств защиты информации.

Литература

1. Интерактивный мультимедийный модуль исследования в реальном режиме времени колебательных систем / С.Е. Карпович [и др.] // Теоретическая и прикладная механика. – 2017. – № 32. – С. 117–123.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НОВЫХ ВЫЗОВОВ И УГРОЗ КИБЕРНЕТИЧЕСКОГО И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ХАРАКТЕРА

В.Е. Макаров

В современных условиях одним из важнейших и решающих направлений совершенствования и повышения эффективности организации системы информационной безопасности отдельных организационных структур, общества и государства является подготовка профессиональных кадров, обучающихся в системе высшего профессионального образования по решению не только технических и технологических задач обеспечения технической защиты информации, но и вопросов прогнозирования, выявления, анализу и оценке угроз информационной безопасности; определению основных направлений государственной политики и стратегическое планирование в области обеспечения информационной безопасности; разработке и применению комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз информационной безопасности, локализации и нейтрализации последствий их проявления.

По нашему мнению, многообразие политических и социальных фактов обеспечения информационной безопасности по большому счету, сводится к двум важнейшим проблемам

современности: защите информации и защите от информации, т.е. противодействию информационно-кибернетических операций и информационно-психологических операций. Все это обусловило не только чисто теоретический интерес, но и практическую значимость изучения и исследований информационных операций в контексте реализации управления социальными системами, которое с каждым днем становится все более информационным.

При разработке и реализации учебного плана на кафедре «Информационной безопасности» НИУ МИЭТ г. Москва реализован новый подход в обучении студентов по изучению влияния политических и социальных аспектов на обеспечение информационной безопасности личности, социальных групп, общества и государства в современных условиях усилившегося информационного воздействия со стороны США и некоторых стран Западной Европы. С системных позиций изучаются сведения об эволюции информационного противоборства и о современных технологиях информационного воздействия в социальных системах, анализируется система социальных и политических отношений современного информационного общества как среда организации и проведения тайных операций информационной войны. С современных позиций рассматриваются основные направления противодействия информационной агрессии вероятного противника в современных условиях развития Российской Федерации.

Реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (семинаров в диалоговом режиме, дискуссий, компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий, результатов работы студенческих исследовательских групп, вузовских и межвузовских исследовательских групп, вузовских и межвузовских телеконференций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Литература

1. Макаров, В.Е. Политические и социальные аспекты информационной безопасности / В.Е. Макаров. – Таганрог: С.А. Ступин, 2015. – 352 с.

2. Основы информационной безопасности / Е.Б. Белов [и др.]. – М.: Горячая линия–Телеком, 2006. – 544 с.

3. Брусницын, Н.А. Информационная война и безопасность / Н.А. Брусницын. – М.: Вита-Пресс, 2015.– 280 с.

4. Панарин, И.Н. Информационная война и коммуникации / И.Н. Панарин. – М.: Горячая линия–Телеком, 2014. – 236 с.

ОБУЧАЮЩЕЕ ПРОГРАММНОЕ СРЕДСТВО ПО ДИСЦИПЛИНЕ «ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В.И. Пачинин, А.В. Яковлев

Рассматривается задача проектирования обучающего программного средства по дисциплине «Защита компьютерной информации» для специальности «Программное обеспечение информационных технологий» 2-40 01 01. Для реализации задачи используется несколько алгоритмов шифрования, начиная от простых (алгоритм Цезаря), заканчивая симметричными и асимметричными алгоритмами шифрования. Язык разработки Java. В качестве входных данных используется: ФИО пользователя, алгоритм шифрования, способы защиты информации личной и коммерческой. Программное средство демонстрирует детальное описание способов защиты информации с набором пошаговых действий, начиная от защиты помещений и правил поведения, заканчивая алгоритмами шифрования. На знание правил и способов защиты информации проводится тестирование, где студенту предлагается выбрать правильное действие. Используется несколько этапов изучения шифров. Первый подразумевает пошаговую демонстрацию шифрования данных с указанием вариантов программной реализации. На втором этапе изучения алгоритма, программа предлагает варианты шагов шифрования на выбор, необходимо указать их в нужной последовательности и исключить лишние. Третий этап исключает часть описания, чтобы студент сам его реализовал, после чего

программа проверяет предложенный вариант. За каждый этап выполнения выставляются баллы, после чего они суммируются. Программа учитывает время выполнения задания. Также проводится анализ ошибок с указанием неверных действий.

Программное средство может применяться на практических и лабораторных занятиях. Оно моделирует различные ситуации, при которых полезная информация может подвергнуться угрозе раскрытия или повреждения. Также в разделе «Законодательство» указаны все законодательные акты Республики Беларусь в сфере защиты информации. Использование данного обучающего программного средства позволит сократить время на проверку знаний по итогам изучения алгоритмов шифрования и способов защиты информации.

Примечание редколлегии. Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов
XV Белорусско-российской научно–технической конференции
(Минск, 6 июня 2017 г.)

В авторской редакции

Ответственный за выпуск *Т. В. Борботько*

Компьютерная верстка *О. В. Бойправ*

Подписано в печать 30.05.2017. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 13,71. Уч.-изд. л. 11,1. Тираж 100 экз. Заказ 116.

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.