Секция

ЗАЩИТА ИНФОРМАЦИИ, СПЕЦИАЛЬНЫХ И БИОЛОГИЧЕСКИХ ОБЪЕКТОВ

УДК 621.391

ОПЫТ СОЗДАНИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

А.А. ОБУХОВИЧ, М.Н. БОБОВ

ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»
пр-т Независимости, 117, г. Минск, 220114, Республика Беларусь

Работы по обеспечению защиты информации в информационных автоматизированных системах проводятся на предприятии с 1974 года.

За 40 лет проведено 24 научно-исследовательские работы, результаты которых легли в основу методологии защиты информации в информационных автоматизированных системах.

На основе разработанной методологии создано более 100 систем военного и гражданского назначения. В частности разработаны, внедрены и аттестованы системы защиты информации в государственных межведомственных информационных системах ОАИС, ЕИС КВП, ИАС КНД и ведомственных информационных системах ИСУ Госкомвоенпрома, ИАС УВК и др.

Разработанная методология устанавливает порядок и содержание работ по обеспечению защиты информации на протяжении всего жизненного цикла информационных систем и определяет соответствующее каждому этапу нормативно-методическое обеспечение. Опыт показывает, что методология позволяет обеспечить гарантированность защиты информации, унификацию требований, предъявляемых к средствам и системам защиты, их совместимость при использовании в системах различного уровня и назначения, повышение качества разработки средств защиты и защищаемых систем при одновременном снижении трудоемкости работ, исключении дублирования работ и сокращения общей номенклатуры нормативно-методической документации.

Разработанный в соответствии с методологией пакет нормативно- методических документов состоит из трёх основных групп, включающих в себя документы организационно-системного плана, документы, определяющие порядок разработки, внедрения и приемки защищенных систем, и документы оценке уровня защищенности информации в системах.

Структура и состав разработанных нормативно-методических документов базируются на основных принципах, сформулированных ниже.

Первым принципом является разработка положений нормативно-методических документов исходя из расчета на «худший случай», т.е. документы предполагают задание самых жестких требований и указания условий, когда эти требования могут быть смягчены или носят рекомендательный характер.

Вторым принципом является организационная совместимость документов с действующими государственными стандартами в данной и смежных областях.

Третьим принципом является соблюдение единой терминологии, принятой в данной предметной области.

Четвертым принципом является первоочередность разработки организационно-методических документов, регламентирующих порядок проведения работ по защите информации и взаимоотношения участников создания защищенных систем.

Документы организационно-системного плана являются наиболее важной группой документов, т.к. именно они определяют основные положения по защите информа-

ции при ее электронной обработке, терминологию, используемую в этой области техники, и систему технической документации по защите информации.

Ко второй группе относятся документы, определяющие порядок разработки, испытаний, внедрения и приемки защищённых систем. Эти документы определяют состав и содержание работ по стадиям создания защищенных систем, так как в процессе их создания, внедрения и эксплуатации принимает участие значительное количество заинтересованных сторон: заказчики, головные разработчики, соисполнители, представители специализированных организаций, изготовители и потребители. Регламентация их прав и обязанностей на всех стадиях жизненного цикла систем также является задачей документов данной группы. К этой же группе относятся и типовые проектные решения по защите информации.

К третьей группе относятся документы, регламентирующие работы по оценке уровня защищенности информации в системах.

На основе документов организационно-системного плана при создании защищенных систем производятся следующие важнейшие работы:

– определение объектов защиты в системе;

– формирование правил разграничения доступа к ресурсам системы;

– разработка модели нарушителя;

– обоснованию критериев защищенности информационной системы;

– обоснованию требований безопасности к системе.

Документы второй группы в основном используются:

– при разработке технического задания на систему защиты информации;

– при разработке комплекса мер по реализации гарантийных требований безопасности по СТБ 34.101.3;

– при выборе средств, реализующих функциональные требования безопасности.

Документы по оценке защищенности определяют показатели и критерии защищенности, методики категорирования защищаемых ресурсов системы, методики оценки средств и систем защиты. Документы этой группы используют:

– для оценки и обработки информационных рисков;

– для оценки соответствия разработанных средств требованиям технических нормативных правовых актов по защите информации;

– для инженерной оценки стойкости к преодолению или обходу средств защиты;

– для аттестации информационной системы по требованиям информационной безопасности.

Опыт работы в области защиты информации показал, что эффективное создание защищенных информационных систем возможно только при использовании принятой методологии защиты, действующей в виде комплекса стандартов предприятия-разработчика.

УДК 007

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЧАСТЬ СОВРЕМЕННОГО ОБЩЕСТВА

А.Н. РЫКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
antonme66@mail.ru

Появление в мире новых рисков, вызовов и угроз, обострение глобальных проблем человечества, проблемы безопасности в политической сфере, насущные потребности по сохранению дальнейшего устойчивого развития Беларуси объективно потребовали поиска новых подходов к комплексному обеспечению национальной безопасности страны. [1]

Ключевые слова: информационная безопасность, информационные технологии, защита.

В сложившейся ситуации одним из важнейших направлений развития информационных технологий в современном обществе является информационная безопасность. В настоящее время в ее функции входит защита таких категорий информации, как научная, коммерческая и стратегическая [1].

Под понятием безопасности автоматизированной информационной системы понимают ее защищенность от преднамеренного и случайного вмешательства в нормальный процесс ее функционирования, а также от попыток модифицировать или разрушить ее компоненты. Это обеспечивает комплекс технологических и административных мер, которые применяются к программам, данным и аппаратным средствам с целью обеспечить доступность, целостность и конфиденциальность защищаемых ресурсов. В табл. 1 приведена систематизация ресурсов защиты информации.

Табл. 1. Основные ресурсы защиты информационной системы

Компьютерная безопасность	Совокупность технологических и административных мер, обеспечивающая доступность, целостность и конфиденциальность ресурсов компьютера
Безопасность данных	Защита данных от несанкционированной модификации, разрушения и раскрытия этих данных.
Безопасность коммуникаций	Предотвращение предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на запрос по каналам связи.
Безопасность программного обеспечения	Программное обеспечение, которое обеспечивает безопасную обработку данных в компьютерной системе, а также дает возможность безопасно использовать ресурсы системы.

Проблемой информационной безопасности начали заниматься, как только появилась угроза раскрытия засекреченной информации. Первым шагом стало распространение знаний об информационной безопасности за пределами правительственных организаций, непосредственно связанных с секретной информацией или отвечающих за режим секретности. Первый опубликованный материал – «Критерии оценки надежных компьютерных систем» («Оранжевая книга») увидела свет в США в 1983 году благодаря Министерству обороны США.

Согласно «Оранжевой книге» безопасной системой называется та система, которая «управляет посредством соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать и удалять информацию». Очевидно, что абсо-

лютно безопасных систем не существует – каждую систему можно «взломать», если иметь достаточное количество времени и материальных ресурсов [1].

Надежная система – «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Сейчас крупные фирмы, банки, организации стараются защитить свою информацию от злоумышленников. Шпионская программа или программа способная разрушить целостность системы может быть замаскирована в любой файл. Стоить заметить, что не существует абсолютно безопасных систем. Каждую систему можно «взломать» если иметь достаточное количество временных и материальных ресурсов.

Для защиты информации существуют программы способные обнаруживать вероятные источники угроз и устранять их (так называемые антивирусы) или защищать информацию другими способами (шифрование, архивирование, или назначение пароля). Антивирусы способны отслеживать абсолютное большинство всех угроз и предотвращать атаки, то есть антивирус объединяет в себе черты средств активной защиты. Шифрование и введение паролей – элементы пассивной защиты информации (они не дают получить доступ к информации). Эти программы не допускают к работе с информацией неавторизованных пользователей или программы, действующие от их лица. Однако справится с такими программами намного легче, чем справится с пользователем, допустившим для системы фатальную ошибку. После него трудно восстановить систему и его почти невозможно обнаружить, если не иметь возможности протоколировать действия пользователей, так или иначе влияющих на безопасность системы. Однако протоколирование будет бесполезно без своевременного и грамотного анализа.

Представляется возможным предотвращение потери информации в хранении ее небольшими частями на разных носителях и в разных местах. Это избавит систему от возможных ошибок, атак или проблем с носителями информации. Подобная система сейчас активно применяется в авиатехнике. Также возможны случаи, когда злоумышленникам удастся собрать все части, тогда необходимо позаботится о безопасности информации. Для таких случаев эти части кодируются. Если все части закодированы одинаково, то безопасность кода значительно уменьшается. Однако если каждую часть кодировать по своему, то весь объем информации будет слишком велик и труднообрабатываем.

Существует множество способов защиты информации, лучший результат они дают при их совмещении. Для каждой угрозы существует своя защита и при правильном использовании они выполняют свои функции. В итоге сам пользователь решает, каким образом защищать важную для него информацию и прибегает к различным методам.

Список литературы

1. Информационно-аналитический центр при Администрации Президента Республики Беларусь: Информационный материал № 6 (90). Обеспечение национальной безопасности Республики Беларусь как важнейший фактор развития государства в современных условиях. [Электронный ресурс]. – Режим доступа: http://iac.gov.by/nfiles/000046_480473.pdf. – Дата доступа: 08.04.12.

УДК 355.58 (07)

ПОДВИЖНЫЕ ПУНКТЫ УПРАВЛЕНИЯ МЧС РЕСПУБЛИКИ БЕЛАРУСЬ

С.Ю. ВОРОБЬЕВ, Д.Б. ХОРОЛЬСКИЙ

Государственное учреждение «Республиканский центр управления и реагирования на чрезвычайные ситуации Министерства по чрезвычайным ситуациям Республики Беларусь»
Логойский тракт, 17, г. Минск, 220090, Республика Беларусь
scorczeni@tut.by

Рассматриваются вопросы применения подвижных пунктов управления гражданской обороны в интересах органов и подразделений по чрезвычайным ситуациям Республики Беларусь, их назначение, состав и тактико-технические характеристики.

Ключевые слова: пункт управления, подвижный пункт управления, радиосвязь, узел связи, гражданская оборона.

Одним из основных элементов систем управления гражданской обороны (ГО) являются пункты управления (ПУ), которые создаются на всех уровнях управления от объекта экономики до районного, областного и республиканского уровней управления.

ПУ ГО называются специально оборудованные или приспособленные и оснащенные техническими средствами сооружения, помещения или их комплексы, или транспортные средства, предназначенные для размещения органов управления ГО и обеспечения их устойчивой работой в особый период, а также при проведении мероприятий по предупреждению и ликвидации чрезвычайных ситуаций (ЧС) природного и техногенного характера [1].

ПУ разделяют на стационарные и подвижные, размещенные на различных транспортных средствах.

Стационарные ПУ можно разделить на:

– повседневные ПУ, предназначенные для обеспечения функционирования органов управления в местах их постоянной дислокации в мирное время;

– запасные ПУ, предназначенные для обеспечения устойчивого управления в особый период и в мирное время в случае невозможности использования повседневных ПУ. По месту своего размещения они могут быть городскими и загородными [2].

Подвижные ПУ (ППУ) создаются заблаговременно, оборудуются на специальных командно-штабных машинах (КШМ) или на специально дооборудованных транспортных средствах и должны быть способны быстро перемещаться, развертываться и свертываться, устойчиво работать круглосуточно, поддерживать связь на стоянке и в движении.

Состав, оборудование и оснащение ППУ на каждом уровне управления различны. На транспортных средствах ППУ оборудуются рабочие места для руководителей исполнительных и распорядительных органов власти (начальников ГО), членов комиссии по ЧС и оперативных рабочих групп органа управления, устанавливаются средства связи.

ППУ могут оборудоваться также на средствах воздушного, морского, речного и железнодорожного транспорта (на практике в Республике Беларусь не применяется).

ППУ должны обеспечивать непосредственное управление подчиненными органами и силами при ликвидации ЧС в любом районе Республики Беларусь, на наиболее ответственных направлениях в военное время, а также выполнять функции дублеров стационарных запасных ПУ.

В зависимости от типа транспортных средств базирования ППУ можно разделить на:

– воздушные ПУ – на базе самолетов или вертолетов;

– мобильные ПУ (МПУ) – на базе автомобильной техники высокой проходимости (с использованием кунгов и прицепов) или автобусов, а также других транспортных средств.

В состав МПУ, как правило, входят несколько автомобилей для размещения личного состава органа управления, штабной автобус для работы смены оперативной группы органа управления, мобильный узел связи, подвижная звукоусилительная станция, машины сопровождения [2].

ППУ должен обеспечивать:

– устойчивое управление подчиненными силами и средствами при ликвидации ЧС;

– надежную связь с вышестоящими органами управления, подчиненными и взаимодействующими силами, привлекаемыми для ликвидации ЧС;

– связь должна быть организована как на месте ЧС, так и в движении автомобильной колоны в район ЧС (в пункт постоянной дислокации);

– автономный режим работы оперативной группы регионального центра до 3-х суток;

– круглосуточную работу оборудования технических, технологических и телекоммуникационных систем.

ППУ считается развернутым и подготовленным к работе, если весь личный состав оперативной группы занял свои рабочие места и готов к работе, с вышестоящими органами управления организована связь, между элементами ППУ (машинами, кунгами, модулями и палатками) организована связь, системы жизнеобеспечения (электропитания, теплоснабжения) включены [3].

В настоящий момент в МЧС Республики Беларусь применяются ППУ на республиканском и областном уровнях.

Список литературы

1. Организация выполнения мероприятий гражданской обороны: методическое руководство. Под общей редакцией Э.Р. Бариева. – Минск, 2009.

2. ОАО «Арсенал Спасения»: Пункты управления. [Электронный ресурс]. – Режим доступа: http://www.arspas.ru/mchs/spravochnik/2/pu.php?print=Y. – Дата доступа: 11.12.2013.

3. Каталог автомобилей ООО «Автомастер»: Передвижной пункт управления (ППУ) на шасси КАМАЗ-43118. [Электронный ресурс]. – Режим доступа: http://www.avto-master.com/catalog/4/174/. – Дата доступа: 15.12.2013.

УДК 681.772.7

ПРИМЕНЕНИЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ И ТЕРРИТОРИЙ

С.Ю. ВОРОБЬЕВ[1], Д.Б. ХОРОЛЬСКИЙ[1], Г.В. МИШНЕВ[2], В.А. РУСАК[3]

[1]Государственное учреждение «Республиканский центр управления и реагирования на чрезвычайные ситуации Министерства по чрезвычайным ситуациям Республики Беларусь»
Логойский тракт, 17, г. Минск, 220090, Республика Беларусь
scorczeni@tut.by

[2]Прокуратура Партизанского района г. Минска
ул. Стахановская, 37, г. Минск, 220009, Республика Беларусь

[3]Учреждение образования «Академия Министерства внутренних дел Республики Беларусь»
пр-т Машерова, 6, г. Минск, 220005, Республика Беларусь

В статье рассмотрены вопросы применения систем видеонаблюдения для предотвращения правонарушений, преступлений и чрезвычайных ситуаций. Представлен обзор применения данной технологии как в странах ближнего и дальнего зарубежья, так и на территории Республики Беларусь.

Ключевые слова: видеонаблюдение, безопасность, безопасный город, правонарушение, пожар, чрезвычайная ситуация.

В настоящее время актуальной является проблема безопасности жителей городов. Противоправные действия, техногенные катастрофы, стихийные бедствия или неконтролируемое развитие ситуаций в местах массового пребывания людей в современном мегаполисе могут иметь самые тяжелые последствия [1].

Как для предотвращения правонарушений, преступлений, чрезвычайных ситуаций, так и в ходе ликвидации их последствий возрастает необходимость оперативного получения объективной информации с места происшествия (чрезвычайной ситуации), координации действий дежурно-диспетчерских служб, других сил и средств, участвующих в пресечении правонарушения или проведении аварийно-спасательных работ.

Системы видеонаблюдения как средство объективной фиксации различных процессов и явлений все шире используются в различных видах практической деятельности. В том числе имеет месте их использование в интересах органов правопорядка и чрезвычайных ситуаций.

Как пример, Лондон считается городом с самой основательной системой видеонаблюдения. Полмиллиона камер осуществляют видеонаблюдение в британской столице. Камеры наблюдения подвешены на каждом углу. На протяжении всего дня среднестатистического лондонца записывает свыше трехсот камер наблюдения. Их кольцо окружает центр города. За секунду каждый номер машины попадает в базу, в которой содержится информация о передвижениях каждого автомобиля. Считается, что эта защита удовлетворительна.

В Российской Федерации получили широкое распространение так называемые системы «Безопасный город» – интегрированные комплексные системы, предназначенные для решения задач обеспечения правопорядка, видеомониторинга чрезвычайных ситуаций, охраны собственности и безопасности граждан в любой точке города [1].

Как правило, технически данные системы представляют собой совокупность множества подсистем, объединенных единой транспортной средой и системой управления.

Начало применения систем видеонаблюдения, использующихся в деятельности по обеспечению общественного порядка и безопасности на улицах городов и дорогах Республики Беларусь, получило широкое распространение в 2002 году.

Развитие и применение систем контроля технологий производства, охранного телевидения, контроля доступа показывают, что видеотехнологии могут успешно решать и задачи обеспечения пожарной безопасности объектов и территорий. Видеодетекторы могут обнаруживать пожар в помещении и на открытых площадках автоматически по специфическим признакам: задымленность, открытое пламя, характерные движения и частоты колебаний объекта на изображении, позволяя, в то же время, при необходимости оператору визуально оценивать ситуацию на объекте.

Видеоматериалы, полученные с использованием систем видеонаблюдения, могут быть использованы как в оперативных целях (при установлении лица, совершившего, либо готовящего преступление), так и в процессе доказывания по конкретному уголовному делу. Они могут быть использованы в оперативно-розыскной деятельности при раскрытии общественно опасных деяний и установления лиц, их совершивших, поскольку содержащиеся в них изображения правонарушителей, их транспортных средств имеют важное ориентирующее значение. Изучение событий, запечатленных с помощью видеозаписи, позволяет установить биологические, социальные и психологические особенности человека, цвет и тип одежды, наличие сопутствующих предметов (очков, зонта, трости и т.п.), вид транспортного средства, тип, цвет его кузова [1].

Среди доступных систем видеомониторинга в настоящий момент присутствует огромное количество оборудования и систем видеонаблюдения. Сами камеры существенно различаются по техническим характеристикам и функциональности, а также по форматам, в которых производится передача и сохранение видеоданных. Это вызывает ряд проблем, требующих решения. Учитывая то, какие средства вкладываются в разработку систем видеонаблюдения (в интересах муниципальных служб, милиции, жилищно-коммунального хозяйства, лесного хозяйства и предупреждения чрезвычайных ситуаций и пожаров) предполагается, что оно должно работать надежно и эффективно, а главное – формировать изображения, отвечающие целям, в которых эти системы внедряются. Соответственно, этим определяются и требования к качеству и надежности подобных систем.

На основе вышеизложенного материала можно сделать вывод о том, что успешное раскрытие и доказывание преступлений, а также предотвращение и ликвидация пожаров и чрезвычайных ситуаций возможны лишь при условии использования систем видеонаблюдения с высокими тактико-техническими характеристиками.

Только масштабная система безопасности на основе фундаментальной программно-аппаратной платформы, объединяющей все области безопасности и жилищно-коммунального хозяйства в единое цифровое пространство, будет эффективно функционировать в условиях современного мегаполиса [1].

Список литературы

1. *Воробьев С.Ю., Мишнев Г.В., Русак В.А.* // Сб. науч. трудов науч.-практ. центра проблем законности и правопорядка Генер. прокуратуры Респ. Беларусь. 2012. № 5. – С. 273–279.

УДК 004.353.2

КОНСТРУКЦИИ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ПЕРЛИТА И ТИТАНОМАГНЕТИТА

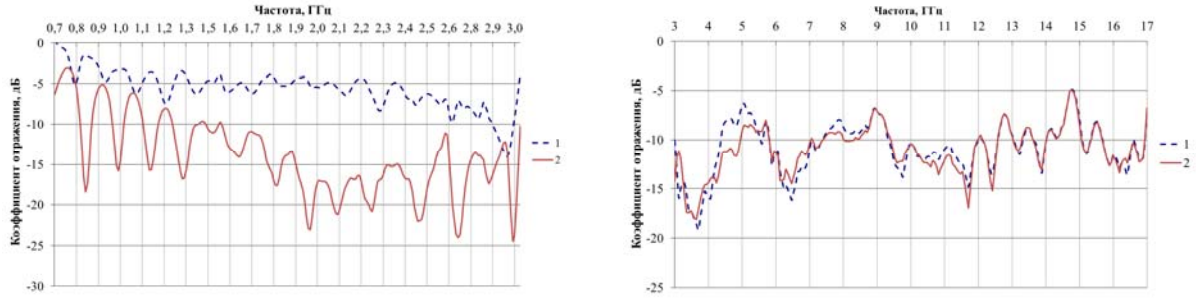
О.В. БОЙПРАВ, Т.В. БОРБОТЬКО, Л.Л. ГАНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
boipravolga@rambler.ru

Проанализированы характеристики отражения и передачи электромагнитного излучения конструкций экранов, изготовленных на основе смеси порошкообразных материалов, характеризирующихся диэлектрическими и магнитными свойствами – перлита и титаномагнетита, соответственно. Разработаны рекомендации по практическому применению таких конструкций.

Ключевые слова: коэффициент отражения электромагнитного излучения, коэффициент передачи электромагнитного излучения, перлит, титаномагнетит.

Для обеспечения электромагнитной совместимости радиоэлектронного оборудования, используемого в системах передачи и обработки данных, применяют конструкции экранов электромагнитного излучения (ЭМИ). В процессе их создания на сегодняшний день широко используются материалы, формируемые на основе порошкообразных компонентов. При этом синтез данных материалов осуществляется путем закрепления их порошкообразных компонентов в связующем веществе либо спекания последних. Основной недостаток таких технологий состоит в том, что в большинстве случаев они характеризуются высокой ресурсоемкостью. Указанного недостатка лишена технология формирования конструкций экранов ЭМИ, формируемых путем заполнения порошкообразным материалом (либо смесью порошкообразных материалов), характеризующимся диэлектрическими, магнитными и/или резистивными свойствами, емкостей определенной формы. При этом управляемо изменять экранирующие характеристики (значения коэффициентов отражения и передачи ЭМИ) таких конструкций возможно путем изменения объема емкости, типа порошкообразных материалов либо соотношений последних в смесях. В рамках настоящей работы на основе перлита марки М150 и титаномагнетита сформированы конструкции экранов ЭМИ и исследованы их характеристики отражения и передачи ЭМИ. Выбор перлита в качестве компонента для формирования конструкций экранов обусловлен его низкой плотностью (для перлита марки М150 – 150 кг/м^3), а значит, и малым весом, титаномагнетита – низкой стоимостью по сравнению с другими ферритами. Исследованные образцы конструкций экранов ЭМИ изготавливались путем заполнения каналов сотового поликарбоната смесью перлита марки М150 (50 об. %) и титаномагнетита (50 об. %). Образец № 1 характеризовался толщиной 10 мм, образцы № 2 и № 3 – 20 мм и 30 мм соответственно. Измерение параметров экранирующих характеристик образцов проводились, согласно методике, описанной в [1]. Установлено, что значения коэффициентов отражения и передачи ЭМИ образца № 1 в диапазоне частот ЭМИ 0,7…17 ГГц равны соответственно –5…–25 дБ (–2…–14 дБ) и –2…–6 дБ, образца № 2 – –5…–20 дБ (–2…–12 дБ) и –4…–14 дБ, образца № 3 – –5…–25 дБ (–4…–18 дБ) и –4…–16 дБ (в скобках указаны значения коэффициентов отражения ЭМИ, измеренные при закреплении исследованных образцов на металлической подложке). На рис. 1 представлены частотные зависимости коэффициентов отражения ЭМИ образца № 3. Кривые 1 соответствуют частотным зависимостям коэффициентов отражения образца, закрепленного на металлической подложке.



а *б*

Рис. 1. Частотные зависимости коэффициентов отражения ЭМИ образца № 3 в диапазоне: *а* – 0,7…3 ГГц, *б* – 3…17 ГГц

Процесс взаимодействия ЭМИ с каждым из исследованных образцов аналогичен их дифракции на мелкой решетке. При взаимодействии ЭМИ с магнитными материалами в них возникают вихревые токи, обуславливающие ослабление энергии ЭМИ.

Магнитная проницаемость ферро- и ферримагнетиков является комплексной величиной и в переменном электромагнитном поле зависит от его частоты. Эта зависимость называется магнитным спектром и может быть условно разделена на 5 областей: 1) низкочастотную, характеризуемую обычно незначительным изменением магнитной проницаемости (диапазон частот 0…0,2 МГц); 2) «инфрарадиочастотную», для которой свойственен магнетомеханический эффект, характеризуемый резонансным всплеском действительной составляющей комплексной магнитной проницаемости; 3) радиочастотную, характеризуемую быстрым спадом вещественной составляющей комплексной магнитной проницаемости ферритов и явно выраженным эффектом поглощения в диапазоне 1…1000 МГц; 4) сверхвысокочастотную, характеризуемую явлением естественного ферромагнитного резонанса, обычно наблюдаемого при частотах 10^3…$5 \cdot 10^4$ МГц, и прецессией электронного спина в эффективном поле анизотропии вещества феррита; 5) «инфракрасную», которая, согласно расчетам, должна характеризоваться незначительным резонансным изменением кривых дисперсии и поглощения ЭМИ при частотах порядка 10^7 МГц [2].

Диапазон частот, в котором проводились измерения значений коэффициентов отражения и передачи ЭМИ изготовленных образцов, принадлежит радиочастотной области (или области естественного ферромагнитного резонанса), в которой располагается резонансная частота, соответствующая наибольшему значению ослабления энергии ЭМИ, взаимодействующего с ферро- и ферримагнетиками.

Исследованные конструкции экранов ЭМИ могут быть применены для облицовки стен помещений, где функционируют системы обработки данных (например, серверных комнат), либо для создания специальных экранирующих перегородок для обеспечения электромагнитной развязки оборудования, располагаемого в пределах таких помещений. Кроме того, использованную в рамках настоящей работы смесь перлита и титаномагнетита допустимо засыпать в стены экранируемых помещений в процессе создания последних. Толщина засыпного слоя в таких случаях будет определяться требованиями к экранирующим характеристикам для данных помещений.

Список литературы

1. *Бойправ О.В.*, *Неамах М.Р.*, *Соколов В.Б.* // Докл. БГУИР. 2012. № 1(63). С. 70–75.

2. *Фоменко Л.А.* Магнитные спектры ферритов // Успехи физических наук. 1958. Т. LXIV, вып. 4. С. 669–731.

УДК 004.056.57:537.531

ВЛИЯНИЕ ПОРОШКООБРАЗНЫХ ВКЛЮЧЕНИЙ В ОГНЕСТОЙКИЕ ПОКРЫТИЯ НА ХАРАКТЕРИСТИКИ ГИБКИХ ЭКРАНОВ ЭМИ

А.А.А. АХМЕД, Я.Т.А. АЛЬ-АДЕМИ, Т.А. ПУЛКО, Л.М. ЛЫНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Исследовалось влияние порошкообразных включений в составе огнестойких покрытий на экранирующие характеристики тканых материалов с вплетенным ферромагнитным микропроводом в частотном диапазоне 8…12 ГГц.

Ключевые слова: экранирование электромагнитного излучения, тканые материалы, мелкодисперсные наполнители, огнестойкие покрытия.

Композиционные материалы на основе тканых полотен отличаются рядом преимуществ, связанных с малой стоимостью, гибкостью, модульностью конструкций. Однако последние тенденции в области данных разработок связаны с расширением частотного диапазона электромагнитных экранов и получением многофункциональных конструкций.

Целью исследования является разработка высокоэффективных экранов электромагнитного излучения для обеспечения комплексной защиты технических средств и обслуживающего персонала в помещениях производственного и бытового назначения от воздействия электромагнитных излучений СВЧ-диапазона, обеспечивающих экологическую безопасность и огнезащиту.

Были сформированы образцы композиционных материалов на основе тканых полотен с вплетенным ферромагнитным микропроводом, покрытых огнестойкой краской с различными наполнителями. Ткань включает нити, выполненные из наноструктурного ферромагнитного микропровода в стеклянной изоляции, которые составляют 1,0–3,2% от поверхностной плотности ткани. В низкочастотном диапазоне 30 МГц–100 МГц ослабление ЭМИ такой тканью составляет 20–40 дБ. Применялась огнезащитная силикатная краска, представляющая собой смесь связующего, пигмента и наполнителя, а также в соответствующих пропорциях огнеупорные наполнители (вермикулит, перлит, тальк, волокна каолиновой ваты, распушенного асбеста), что уменьшает образование дыма, понижает температуру и в конечном итоге приводит к самоугасанию пожара (образец №1). Для увеличения поглощающей способности композиционных материалов в состав огнезащитной краски были добавлены: мелкодисперсный порошок TiO2 в соотношении 1:1 (образец №2) и 2:1 (образец №3), высокодисперсный порошок Ni-Zn(+63-94μm) в соотношении 1:1 (образец №4) и высокодисперсный порошок технического углерода в соотношении 1:1 (образец №5).

Исследование экранирующих характеристик композитных образцов разработанных материалов выполнялось в диапазоне частот 8…12 ГГц по стандартной методике с использованием панорамного измерителя ослабления и КСВН Я2Р-67 с ГКЧ-61 и волноводного тракта. Частотные зависимости экранирующих характеристик исследуемых образцов композитных материалов приведены на рис. 1.

Применение огнезащитного покрытия на поверхности тканых полотен позволяет получить ослабление порядка 5,5…6,5 дБ при коэффициенте отражения в пределах -

1,5…–3,5 дБ. Полученные композиционные материалы с добавлением порошкообразных наполнителей характеризуются улучшением поглощающих свойств при снижении коэффициента отражения в рассматриваемом диапазоне частот.

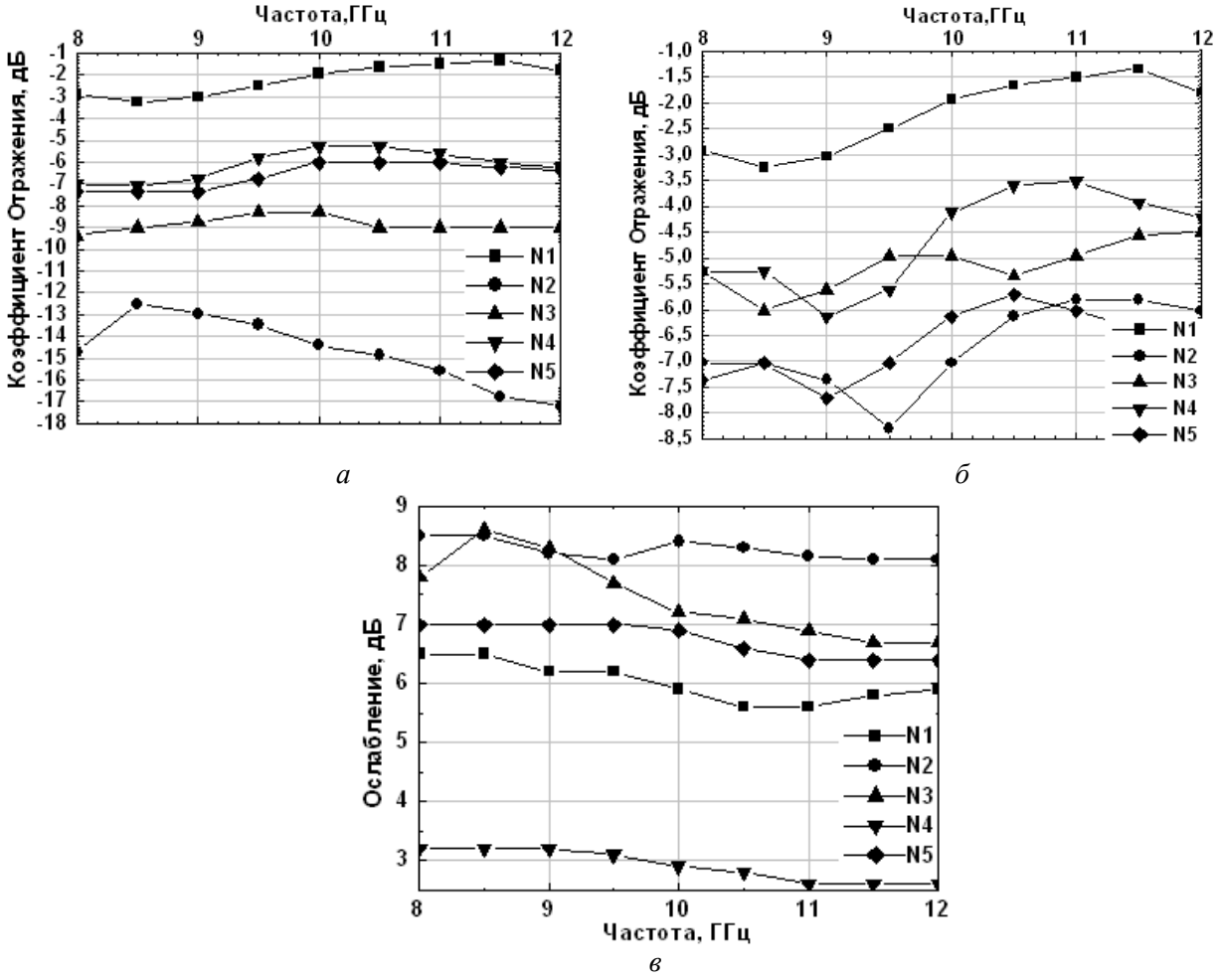


Рис. 1. Частотные зависимости экранирующих характеристик образцов композиционных материалов с наполнением огнезащитного покрытия (1 – без наполнителя; 2 – TiO2 в соотношении 1:1; TiO2 в соотношении 2:1; 3 - Ni-Zn(+63-94μm) в соотношении 1:1; 4 – технический углерод в соотношении 1:1): коэффициент отражения ЭМИ (*а*); коэффициент отражения с металлом (*б*); ослабление (*в*)

При использовании порошкообразных включений в составе огнестойких покрытий наблюдается увеличение ослабления ЭМИ до 5,5…8,5 дБ при коэффициенте отражения –5…–18 дБ. Наилучший результат соответствует образцу гибкого экрана с добавлением в огнезащитное покрытие мелкодисперсного порошка TiO_2 в соотношении 1:1, что позволило увеличить ослабление ЭМИ до 8,5 дБ при коэффициенте отражения –12…–17 дБ (в режиме КЗ изменяется от –6 до –8,5 дБ) в диапазоне 8…12 ГГц. Т.о., исследованные образцы композиционных материалов на основе тканых полотен с применением порошкообразных включений в огнестойком покрытии могут использоваться для обеспечения комплексной защиты различных объектов от воздействия электромагнитных полей, обеспечения экологической безопасности и повышения огнестойкости экранирующих материалов.

УДК 614.841.334.1

ОБЕСПЕЧЕНИЕ ПОЖАРНОЙ БЕЗОПАСНОСТИ ВЫСОТНЫХ ЗДАНИЙ

М.М. КЕМЕЖУК

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
mar.1990@mail.ru

Одним из ключевых направлений развития общества является строительство, в условиях плотной городской застройки целесообразно переходить к возведению высотных зданий. В этой связи необходимо рассмотреть основные положения, которые должны учитываться при строительстве зданий большой этажности, включая правила пожарной безопасности и организации систем оповещения и эвакуации людей при пожарах.

Ключевые слова: пожарная безопасность, высотные здания, система оповещения, эвакуация, чрезвычайная ситуация.

Сегодня популярным становится строительство высотных зданий, которые заметно меняют облик города, делая его более современным и привлекательным. Появление зданий высотой более 75 метров обусловлено и причиной экономии площадей городской застройки.

Однако, несмотря на всю свою привлекательность, высотные здания относятся к объектам повышенной опасности, так как представляют собой технологически сложные сооружения. По этой причине можно говорить о том, что вероятность возникновения чрезвычайных ситуаций, в частности, пожаров на таких объектах выше. Примерами являются пожары в высотных зданиях Каракаса и Мадрида в 2005 году, небоскребе в Астане в 2006 году. Пожары в строениях большой этажности удается потушить не сразу и зачастую выгорает почти все здание. Пожары наносят огромный экономический ущерб, исчисляемый миллионами долларов. Поэтому в условиях масштабного строительства высотных зданий, вопрос обеспечения их противопожарной безопасности становится все более актуальным [1].

Необходимо отметить, что зачастую гибель людей и условия развития пожаров вызваны отсутствием соответствующих инженерных решений, наличием ряда ошибок в проектировании высотных зданий, повышающих их пожарную опасность.

Пожарная безопасность высотных строений осуществляется реализаций комплекса мероприятий, технических и организационных. Большинство мероприятий выполняется на стадии проектирования и строительства зданий. К ним можно отнести:

1. Наличие круговых проездов шириной не менее 6 м с твердым покрытием на расстоянии 8–10 м от наружных стен. Выполнение данной рекомендации позволит спасательной технике беспрепятственно проехать к зданию;

2. На прилегающей к жилому комплексу территории следует предусмотреть площадку для посадки пожарного вертолета либо высадки людей из спасательной кабины;

3. Для теплоизоляции наружных стен следует применять негорючие материалы. Выполнение данного пункта не позволит огню быстро распространиться по зданию;

4. Для отделки потолков, стен и устройства полов на путях эвакуации и в технических этажах обязательно применение негорючих материалов;

5. На техническом этаже необходимо предусмотреть зону коллективной безопасности, которая будет иметь помещения для хранения противопожарного оборудования, средств спасения и индивидуальной защиты;

6. Необходимо обеспечить лестничные клетки естественным освещением, для чего должны быть предусмотрены соответствующие оконные проемы;

7. Предусмотреть систему передачи сигнала установок противопожарной защиты на пульт МЧС РБ;

8. Обеспечить внедрение системы извещения о пожаре путем установки в квартирах пожарных извещателей, систему автоматического пожаротушений – путем установки оросителей, подключенных к водопроводу;

9. Жилые этажи должны быть оборудованы автономным водопроводом, специально предназначенным для пожаротушения;

10. Кабельные электросети в пределах пожарного отсека должны прокладываться в металлических трубах или коробах, за пределами пожарного отсека – в каналах и шахтах;

11. Кабели, прокладываемые по зданию, должны иметь соответствующий класс пожарной опасности [1].

Рассмотренные мероприятия являются основными, но далеко не единственными при проектировании и строительстве высотных зданий, в которых могут располагаться не только жилые, но и офисные помещения, торговые центры и т.д.

Одним из наиболее важных методов противопожарной защиты можно выделить организацию системы оповещения о пожаре, внедрение которой поможет своевременно известить о чрезвычайной ситуации и организовать эвакуацию людей. Одним из основных требований для системы оповещения является принцип зональности многоэтажных зданий и предварительное оповещение персонала здания. Зоной оповещения представляет собой часть здания или сооружения, где проводится одновременное и одинаковое по содержанию оповещение людей о пожаре. Разбиение здания на зоны осуществляется на основе его архитектурных и функциональных особенностей. Для каждого типа системы оповещения оговаривается очередность оповещения, связь с диспетчерской и способы оповещения. Система оповещения должна, прежде всего, оповещать персонал здания, чтобы служащие могли спланировать свои действия по эвакуации людей. Система оповещения о пожаре может функционировать как автономно, так и входить в более сложную систему как одна из ее составных частей. Важной характеристикой системы оповещения является – максимальное количество зон оповещения. Кроме того, системы оповещения различаются по гибкости программирования логики событий и наличию возможности компьютерного управления.

Для того чтобы избежать жертв при пожаре, необходимо не только выполнять основные требования при проектировании и строительстве высотных сооружений, использовать системы оповещения и автоматического пожаротушения, но и отрабатывать основные сценарии возникновения пожаров с целью моделирования их развития динамики развития опасных факторов пожара, а также временных интервалов спасательных работ; распространения поражающих факторов, включая зоны теплового воздействия и обрушения; необходимого резерва средств ликвидации возможных чрезвычайных ситуаций на объекте.

Список литературы

1. AIS.by: Обеспечение пожарной безопасности высотных зданий. [Электронный ресурс]. – Режим доступа: http://ais.by/story/1059. – Дата доступа: 08.01.2014.

УДК 537.876.4, 691.57

ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ОГНЕСТОЙКИХ КРАСОК И АМОРФНОГО УГЛЕРОДА

Е.С. БЕЛОУСОВА, Л.М. ЛЫНЬКОВ,
АБДУЛСАЛАМ МУФТАХ АБУЛЬКАСЕМ МОХАМЕД

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
elena1belousova@gmail.com

Композиционные материалы на основе углерода широко используются для изготовления экранов электромагнитного излучения. Одним из наполнителей композиционных материалов является аморфный углерод (сажа), которая обладает большим спектром свойств, самое важное свойство – высокая электропроводность. В данной работе представлено исследование коэффициента отражения и передачи электромагнитного излучения огнестойкой краски с добавление сажи в диапазоне частот 8–12 ГГц.

Ключевые слова: экраны электромагнитного излучения, огнестойкая краска, аморфный углерод, сажа.

На сегодняшний день перспективным является создание экранирующих отделочных строительных материалов на основе нанопорошкообразных наполнителей, обладающих за счет своей размерности особыми свойствами. Предпочтительно использование электропроводных углеродсодержащих минералов в порошкообразном виде [1].

Использование аморфного углерода в виде саж обусловлено высокой дисперсностью таких углеродных материалов и их большим электросопротивлением. Структура и свойства различных саж оказывают решающее значение на свойства экранирующих и поглощающих электромагнитное излучение материалов. Важнейшими характеристиками сажи являются: дисперсность, малый размер первичной структуры (100–3000 нм), малое количество примесей, формирование вторичных структур, электропроводность.

Целью работы было исследования коэффициента отражения и передачи электромагнитного излучения огнестойких красок при добавлении сажи.

В качестве огнестойкой краски был выбран огнезащитный состав марки «АгниТерм М», который представляет собой суспензию пигментов, реактивных и инертных наполнителей в стабилизированной водной дисперсии синтетических полимеров с модифицирующими добавками. Огнестойкое покрытие «АгниТерм М» обеспечивает пассивную противопожарную защиту путем образования под воздействием высокой температуры трудногорючего пенообразного термоизолирующего слоя (кокса) [2]. В огнестойкую краску было добавлено 10 мас. % строительной сажи (технический углерод П-803), полученная смесь наносилась равномерным слоем толщиной 0,7 мм на прессованное целлюлозное основание толщиной 1,8 мм.

Для исследования экранирующих характеристик огнестойкой краски с добавлением сажи использовались панорамный измеритель ослабления и КСВН Я2Р-67 с ГКЧ-61 и волноводным трактом, который обеспечивает выделение и детектирование уровней падающей и отраженной волн электромагнитного излучения, прошедших и отраженных от образца. Измерения проводились в диапазоне 8…12 ГГц, т.к. этот диапазон используется в военной отрасли. На рис. 1, 2 представлены частотные зависимости коэффициента отражения и передачи исследуемой огнестойкой краски и краски с добавлением сажи.

Коэффициент передачи электромагнитной энергии (рис. 1) огнестойкой краски составляет −3,8… −5,3 дБ в диапазоне частот 8…12 ГГц, при добавлении сажи в состав краски частотная характеристика коэффициента передачи существенно не изменяется. Коэффициент отражения электромагнитного излучения от поверхности огнестойкой краски составляет –4,2… –4,7 дБ, добавка сажи в состав краски уменьшает коэффициент отражения на 1… 1,4 дБ (рис. 2, *а*).

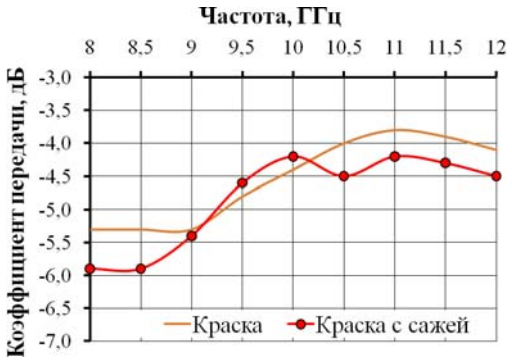
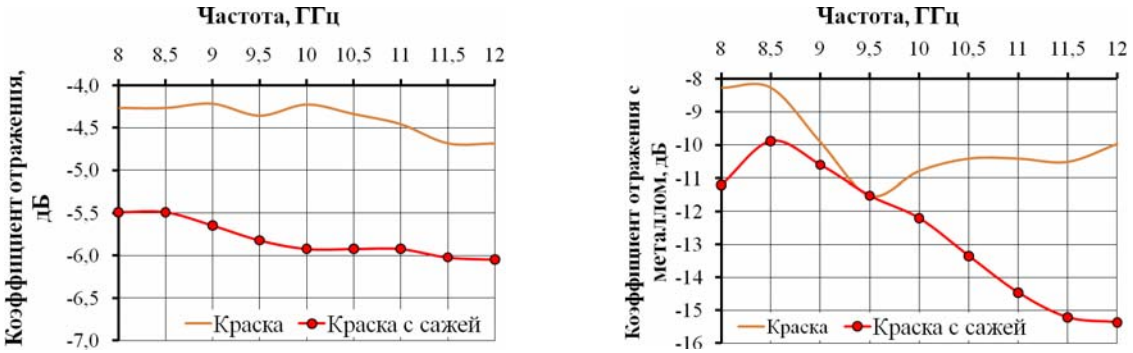


Рис. 1. Частотные зависимости коэффициента передачи огнестойкой краски



а *б*

Рис. 2 Частотные зависимости коэффициента отражения огнестойкой краски:
а – без металлического отражателя; *б* – с металлическим отражателем

При нанесении огнестойкой краски на металлическую поверхность коэффициент отражения электромагнитного излучения составляет –8,2… –11 дБ, при добавлении сажи: –9,8… –15,4 дБ (рис. 2, *б*). Коэффициент отражения огнестойкой краской объясняется высоким содержанием в ее составе пигментов, реактивных и инертных наполнителей в стабилизированной водной дисперсии, добавление электропроводного углеродного порошка сажи увеличивает диэлектрические свойства краски и обеспечивает низкий коэффициент отражения. Огнестойкую краску «АгниТерм М» с добавлением 10 мас. % сажи можно использовать для нанесения на металлические поверхности высокочастотного оборудования.

Список литературы

1 *Белоусова Е.С.* // Матер. II Респ. научн. конф. «Актуальные вопросы физики и техники». Гомель, 18 апреля 2013 г. С. 15–18.

2 АгниТерм М – пенящаяся защита для металла [Электронный ресурс]. – Режим доступа: http://lablimen.com/Catalog/view_10. – Дата доступа: 11.01.2014.

УДК 537.876.4, 691.588

ШУНГИТСОДЕРЖАЩИЕ ЭПОКСИДНЫЕ СМЕСИ ДЛЯ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Е.С. БЕЛОУСОВА, ИДЖИ МОБОЛАДЖИ МИКАЭЛЬ ОЛАКУНЛЕ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
elena1belousova@gmail.com

В настоящее время актуальным является направление, связанное с созданием новых шунгитонаполненных композиционных материалов на основе различных связующих для экранирования электромагнитного излучения в диапазоне сверхвысоких частот. В данной работе представлено исследование коэффициента отражения и передачи электромагнитного излучения шунгитсодержащей эпоксидной смеси в диапазоне частот 0,7–17 ГГц.

Ключевые слова: экраны электромагнитного излучения, шунгит, эпоксидный клей.

Одним из наиболее активно используемых материалов для формирования экранов электромагнитного излучения является углерод в форме порошка или волокон. Шунгитовый углерод образует матрицу, в которой довольно равномерно распределены высоко дисперсные силикаты. Уникальные особенности шунгитовых пород определяются в первую очередь структурой и свойствами шунгитового углерода, а также его взаимоотношениями с силикатными компонентами породы. В целом это определяет перспективы практического использования шунгита. В работе [1] представлены результаты исследования смеси эпоксидного клея (массовая доля – 40 %) с порошками шунгита (20 %), титаномагнетита (20 %), диоксида титана (20 %) и установлено, что коэффициентом отражения составляет –12… –14,5 дБ. Поэтому в данной работе ставиться цель исследовать коэффициент отражения шунгитсодержащей эпоксидной смеси в диапазоне частот 0,7–17 ГГц при помощи панорамного измерителя коэффициентов передачи и отражения SNA 0,01–18.

Для проведения измерений изготовлено 2 образца с массовой долей эпоксидного клея – 40 %, шунгита – 20 %, титаномагнетита – 20 %, диоксида титана – 20 %, данная смесь наносилась слоем толщиной 3,5 мм и 7 мм на целлюлозное основание, размер образцов составлял 30×40 см. Масса образцов составила 0,5 кг и 1,56 кг соответственно. На рис. 1, 2 представлены частотные зависимости коэффициентов отражения и передачи электромагнитной энергии для образцов из эпоксидного клея с разными толщинами. Коэффициент отражения образца из эпоксидного клея с толщиной 3,5 мм составил –1,7… –10 дБ. На частотах 7–8,5 ГГц происходит полное отражение электромагнитной волны. Для образца из эпоксидного клея толщиной 7 мм коэффициент отражения составляет –1,8… –10,4 дБ с резонансом –10,4 дБ на частоте 6 ГГц (рис. 1, *а*). Измерения коэффициента отражения образца из шунгитсодержащей эпоксидной смеси с толщиной 3,5 мм и установленным за ним металлическим отражателем показали, что его значения изменяются в пределах 0… –11,2 дБ с резонансом –11,2 дБ на частоте 5 ГГц. Для образца толщиной 7 мм коэффициент отражения с металлическим отражателем изменяется в пределах 0… –12,2 дБ с резонансом на частоте 8–9 ГГц (рис. 1, *б*). Коэффициент передачи электромагнитной энергии (рис. 2) для образца толщиной 3,5 мм составляет 0… –6,5 дБ, для образца толщиной: –1,6… –11 дБ, однако у обоих образцов имеется резонанс на частоте 6 ГГц со значениями коэффициента передачи 0 дБ (для образца толщиной 3,5 мм) и –3 дБ (для образца толщиной 7 мм).

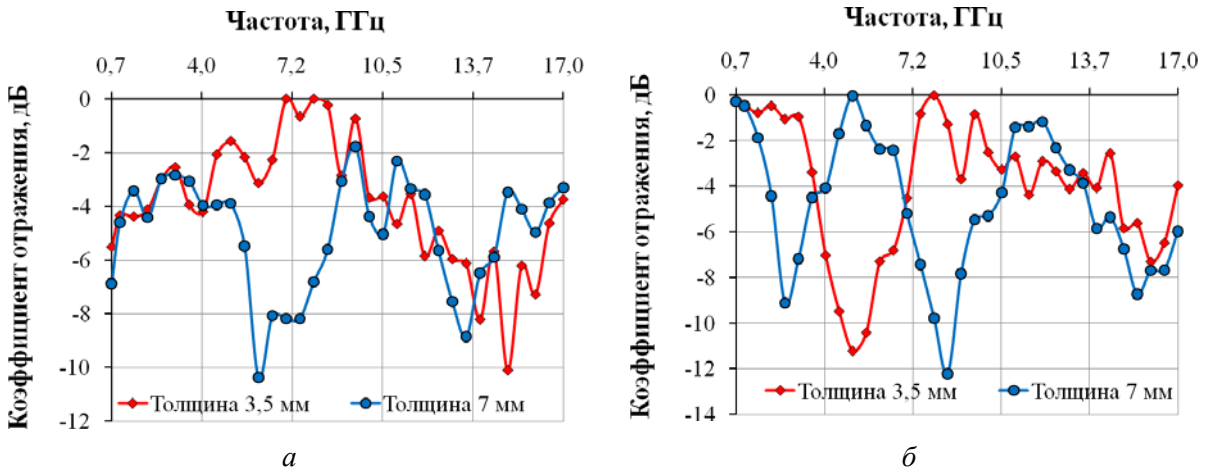


Рис. 1. Частотные зависимости коэффициента отражения шунгитсодержащей эпоксидной смеси толщиной 3,5 см и 7 см: *а* – без металлического отражателя; *б* – с металлическим отражателем

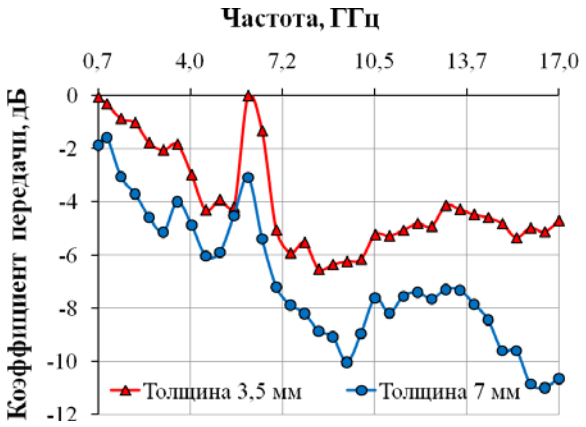


Рис. 2. Частотные зависимости коэффициента передачи шунгитсодержащей эпоксидной смеси толщиной 3,5 см и 7 см

На основе анализа частотных характеристик коэффициента отражения и передачи электромагнитного излучения шунгитсодержащей эпоксидной смеси, можно сделать следующие выводы:

– коэффициент отражения электромагнитного излучения имеет минимальные значения при установке за исследуемыми образцами шунгитсодержащей эпоксидной смеси металлического листа, поэтому данная смесь эффективнее наносить на металлические поверхности;

– частотная характеристика коэффициента отражения для образцов разной толщины имеет резонансы на разных частотах, поэтому в зависимости от типа защищаемой информации, изменяя толщину слоя можно добиваться уменьшения коэффициента отражения на определенных частотах до –11… –12 дБ.

Список литературы

1 *Белоусова Е.С.* // Сб. матер. IV междунар. науч.-техн. молодежной конф. «Научные стремления». Минск, 3–6 декабря 2013 г. С. 271–274.

УДК 535.24

ОПТИЧЕСКИЕ СВОЙСТВА СЕТЧАТЫХ МАТЕРИАЛОВ ТРЕХ ВИДОВ ОКРАСКИ ДЛЯ СКРЫТИЯ ОБЪЕКТОВ В ДИАПАЗОНЕ ИЗЛУЧЕНИЯ 0,4 – 2,5 мкм

Е.С. БЕЛОУСОВА, А. ОМЕР ДЖАМАЛЬ СААД, ТИКА АБДУЛЬБАСИТ АЛИ, Ю.В. БЕЛЯЕВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
elena1belousova@gmail.com

В оптическом диапазоне от 0,4 до 2,5 мкм эффект маскировки достигается созданием имитаторов спектрального распределения (отраженного и рассеянного от различных фонов) внешнего излучения. В данной работе представлены результаты лабораторных и натурных исследований определения коэффициента спектральной яркости и степени линейной поляризации сетчатого материала трех видов окраски.

Ключевые слова: оптический канал утечки информации, коэффициент спектральной яркости, степень поляризации, маскировочные сетки.

При скрытии местоположения охраняемого объекта от средств наблюдения важнейшим техническим каналом утечки информации является оптический канал. Он эффективен вследствие применения различных оптических приборов дистанционного зондирования, позволяющих увеличить контраст объекта на окружающем фоне. Подбор образцов, позволяющих надежно скрывать различного рода объекты, является сложной и трудоемкой задачей. Лабораторные исследования с использованием установки на базе гониометра Г-5 и спектрорадиометра ПСР-02 с поляризационной насадкой [1] позволяют оперативно измерять отражательные спектральные и спектрально-поляризационные параметры маскировочных материалов в области длин волн 0,35 – 2,5 мкм и вносить корректировки при выборе необходимой окраски и структуры маскировочных образцов для их минимального яркостного и поляризационного контраста с различными природными фонами.

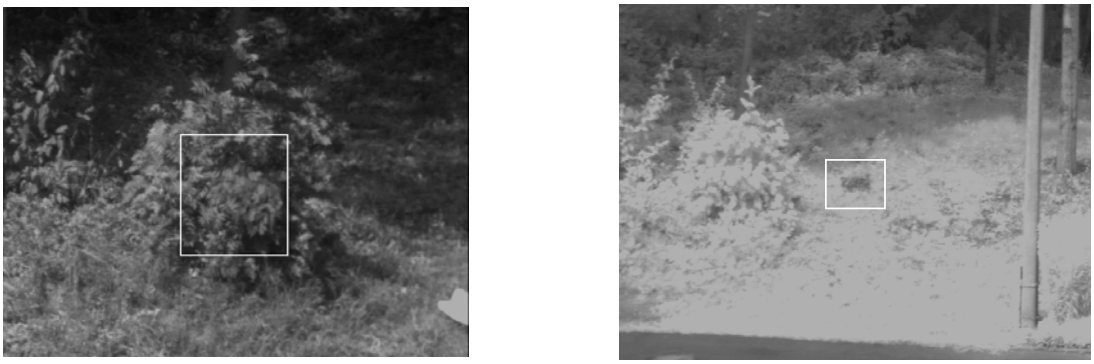
Для проведения лабораторных исследований образцов маскировочных сеток использовалась установка на базе гониометра Г-5 и спектрорадиометра ПСР-02 с поляризационной насадкой. В качестве образцов сетчатых материалов различной окраски, помещаемых на рабочий столик, были выбраны лепестки, составляющие комбинированный маскировочный материал (рис. 1). Для верификации результатов лабораторных измерений проводились натурные съемки исследуемого комбинированного сетчатого материала на фоне растительности спектрозональным видеополяриметром СВП.

Результаты определения коэффициента спектральной яркости (КСЯ) образцов сетчатого материала трех видов окраски, составляющих лепестки комбинированной маскировочной ткани и КСЯ листа комнатного растения показали, что на зависимостях КСЯ от длины волны излучения для листа растения выделяются характерные полосы поглощения хлорофилла в видимой области спектра и полосы поглощения воды в ИК-диапазоне (1400 нм и 1900 нм). Ход КСЯ лепестков ткани светло-зеленой окраски ближе всего к ходу КСЯ листа растительности в полосах поглощения хлорофилла и на «плато отражения» растительности в ближней ИК-области спектра 850 – 1000 нм. Лепестки светло-коричневые и темно-зеленые в этой области имеют низкие значения КСЯ,

отличающиеся от значений КСЯ листа растительности в области 850 – 1000 нм более чем в два раза.

Рис. 1. Комбинированный сетчатый материал, состоящий из лепестков различной окраски: 1 – светло-зеленые; 2 – темно-зеленые; 3 – светло-коричневые

На изображении, полученном с помощью СВП с центральной длиной волны пропускания λ_1= 565 нм, исследуемый маскировочный образец практически не виден, поскольку величина контраста меньше 0,1 (рис. 2, *а*).



а *б*

Рис. 2. Изображения комбинированного сетчатого материала на фоне куста растительности, зарегистрированные СВП в различных спектральных диапазонах

Степень линейной поляризации листа растительности практически во всем спектральном диапазоне превышает значения поляризации лепестков маскировочной сетки. Соответственно, контраст степени линейной поляризации «сетка – лист растительности» за исключением двух небольших участков отрицательный, т.е. при прямом солнечном освещении при определенном положении поляризатора маскировочный образец должен выглядеть темнее аналогично расположенного лиственного покрова, что и подтверждается спектрально-поляризационными изображениями, зарегистрированными с помощью СВП во всем диапазоне чувствительности камеры 400 – 950 нм (рис. 2*б*). Натурные эксперименты по верификации лабораторных исследований с помощью спектровидеополяриметра СВП подтверждают адекватность методики лабораторных исследований.

Список литературы

1. *Беляев, Б.И.* // Тез. докл. 11-й науч.-техн. конф. «Фотометрия и её метрологическое обеспечение». Москва, 17 – 19 декабря 1996 г. С. 55.

УДК 534.833.522.4

ПРОЕКТИРОВАНИЕ СТЕНДОВОЙ УСТАНОВКИ ДЛЯ ОПРЕДЕЛЕНИЯ РАЗБОРЧИВОСТИ РЕЧИ ПРИ ВОЗДЕЙСТВИИ НА НЕЕ ПОМЕХОВОГО СИГНАЛА

О.Б. ЗЕЛЬМАНСКИЙ, С.Н. ПЕТРОВ, Д.Э. ОКОДЖИ, Т.В. БОРБОТЬКО

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
7650772@rambler.ru, petrov@bsuir.by

В работе предложена экспериментальная стендовая установка, позволяющая определять разборчивость речи, в том числе проходящей через элементы ограждающих конструкций, при воздействии на нее помехового сигнала. Данная установка представляет собой аналог малой заглушенной звукомерной камеры.

Ключевые слова: разборчивость речи, звукоизоляция, акустика.

Экспериментальная установка изготовлена из двух частей металлической трубы с толщиной стенок 6 мм (внутренний диаметр – 0,26 м, длина частей – 0,8 и 0,4 м), каждая из которых заварена наглухо с внешних торцов, а с внутренних – наварены круговые фланцы с резиновыми прокладками для фиксации образцов элементов ограждающих конструкций (рис. 1).

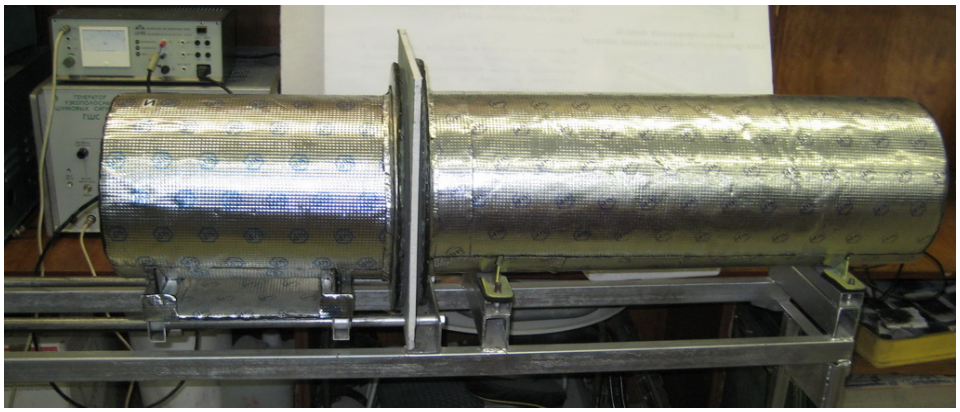


Рис. 1. Стендовая установка для определения разборчивости речи

Установка закреплена на металлической станине. Неподвижная часть – стационарно на виброизолирующих прокладках из резины, подвижная часть передвигается с помощью червячной передачи. В неподвижной части трубы установлен микрофон марки М–101 с микрофонным предусилителем ВПМ–101. Микрофон подвешен на резиновых нитях для снижения воздействия на него вибрации корпуса установки. В подвижной части трубы установлен двухдиффузорный динамик JUMP пиковой/номинальной мощностью 130/65 Вт. Для снижения косвенной передачи звука в камеру низкого уровня через металлическую станину на внутреннюю и внешнюю поверхности установки нанесен виброизоляционный материал STP Bimast-Bomb толщиной 4 мм и удельным весом 6,0 кг/м^2 на основе битумной и мастичной композиций с добавлением антиадгезионной бумаги и алюминиевой фольги. Данный материал является вибропоглотителем (вибродемпфером). На внутренней поверхности установки в качестве второго слоя на-

несен шумопоглощающий материал на основе вспененной резины «Комфорт S-Max» толщиной 6 мм, обладающий эффективностью звукопоглощения в диапазоне частот 500 – 6 000 Гц до 32 дБ. Для исключения передачи вибраций с пола на металлическую станину были использованы виброизоляционные опоры, конструктивно выполненные на основе материалов из натурального каучука. Для получения равномерной АЧХ излучающей части установки было применено акустическое оформление типа «закрытый ящик» (герметично закрытый корпус акустической системы). Акустическая система в таком оформлении отличается простотой конструкции и приемлемыми переходными характеристиками, которые обусловлены высокой упругостью колебательной системы диффузор – внутренний объем корпуса. Рассчитав параметры Тиля-Смола [1] используемого динамика, был подобран такой внутренний объем корпуса установки за динамиком, при котором резонансная частота акустической системы составила 95 Гц и не входит в исследуемый диапазон частот (200 – 7000 Гц).

Принцип работы стендовой установки заключается в следующем. Заранее записанные тестовые акустические сигналы, представляющие собой тестовые фразы из СТБ ГОСТ Р 50840-2000 [2] воспроизводятся с помощью ноутбука, подключенного через усилитель мощности LV-103 к динамику установки.

Для определения разборчивости речи, проходящей через элементы ограждающих конструкций, при воздействии на нее помехового сигнала между фланцами установки размещается элемент конструкции, на котором со стороны подвижной части установки закрепляется виброизлучатель помехового сигнала, подключенный к генератору шума через усилитель мощности (рис. 2). В случае исследования прямого акустического канала, элементы ограждающих конструкций не применяются, акустические сигналы распространяются непосредственно из подвижной части трубы в неподвижную. При этом в качестве источника помехового сигнала выступает акустический преобразователь (динамик), размещенный в подвижной части трубы.

Далее сигнал, представляющий собой смесь тестового и помехового сигналов, записывается на ноутбук с использованием микрофона, установленного в неподвижной части трубы, и анализируется группой аудиторов.

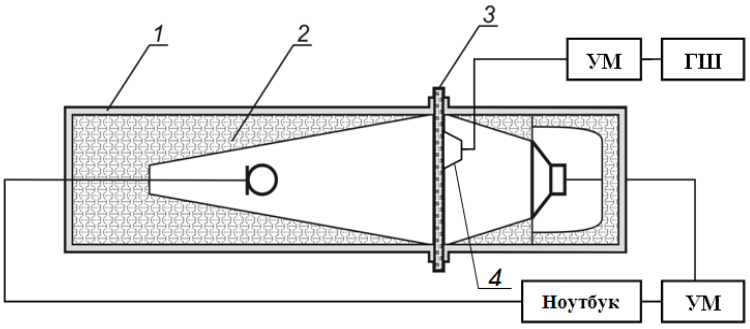


Рис. 2. Схематическое изображение экспериментальной установки (исследование виброакустического канала): 1 – металлическая труба; 2 – звукопоглощающий материал; 3 – элемент ограждающей конструкции; 4 – виброизлучатель; ГШ – генератор шума; УМ – усилитель мощности

Список литературы

1. *Dan Ferguson* Проектирование и построение автомобильных акустических систем. McGraw-Hill, 2000.

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

УДК 003.23: 004.522

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ ЗАКОНОМЕРНОСТЕЙ КАЗАХСКОГО ЯЗЫКА ДЛЯ СИНТЕЗА РЕЧЕПОДОБНЫХ ПОМЕХ

О.Б. ЗЕЛЬМАНСКИЙ, Х.С. АБИШЕВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
7650772@rambler.ru

На сегодняшний день статистические закономерности казахского языка не достаточно изучены. В настоящей работе представлены результаты исследования частоты употребления букв казахского алфавита и слов казахского языка на примере анализа казахско-русского словаря, технических и газетных текстов и их сравнительный анализ.

Ключевые слова: статистика казахского языка, частота употребления букв казахского алфавита, встречаемость слов казахского языка, речеподобные сигналы.

Компиляция участков естественной речи широко используется в системах синтеза речи, а также речеподобных сигналов, формируемых по случайному закону и по своим основным временным, спектральным характеристикам и восприятию на слух, максимально подобных речевым сигналам, но не содержащих смысловой информации. Один из предлагаемых способов синтеза речеподобных сигналов заключается в преобразовании формируемого с учетом статистических закономерностей выбранного языка орфографического псевдотекста в акустические колебания звукового диапазона частот. Таким образом, для реализации подобных систем необходимо формирование речевых баз дикторов, представляющих собой набор отрезков естественной речевой волны, соответствующих фонетическим единицам речи диктора. При этом необходим учет статистических закономерностей языка. Для русского, английского и арабского языков такие системы достаточно подробно изучены. Однако для казахского языка сведения о подобных системах не опубликованы.

Таким образом, с целью создания речевых баз, учитывающих основные статистические, фонетические, лексические и грамматические особенности современного казахского языка, был проведен статистический анализ употребления букв и слов казахского языка.

Казахский кириллический алфавит, разработанный С.А. Аманжоловым и принятый в 1940 году, содержит 42 буквы: 33 буквы русского алфавита и 9 специфических букв казахского языка Ә, Ғ, Қ, Ң, Ө, Ұ, Ү, Һ, І.

Для создания баз данных и возможной сегментации речевых сигналов на казахском языке предложена методика статистического учета употребления букв казахского алфавита. За основу методики оценки употребления той или иной буквы принимали их количество, использованное в казахско-русском словаре. При этом подсчитывалось количество слов, начинающихся с определенной буквы. В табл. 1 представлены результаты статистической обработки казахско-русского словаря на 50000 казахских слов, выборки из технических текстов, а так же статей средств массовой информации (СМИ) различной тематики.

Анализ табл. 1 показывает, что полученные статистические закономерности очень схожи между собой. Так, наиболее используемой буквой казахского алфавита является буква «Қ», за которой следует буква «Т», а наименее употребляемыми

являются буквы В, Ғ, Ц, Ч, Щ, Ю, Я. В казахском языке нет слов начинающихся с букв Ё, Ң, Й, Һ, Ъ, Ь.

Табл. 1. Результаты статистического анализа употребления букв казахского алфавита

№	Буква	Частота употребления (%)			№	Буква	Частота употребления (%)		
		Словарь	Технический текст	СМИ			Словарь	Технический текст	СМИ
1	Қ	14,5	12	11	22	Ф	1	0,01	0,1
2	Т	10,6	10	9,4	23	І	0,8	0,8	0,8
3	Ж	9,6	10	9,3	24	Г	0,6	0,1	0,1
4	Б	8,7	10,6	12,3	25	Л	0,6	0,3	0,3
5	А	8,5	8,5	8,2	26	Р	0,6	0,9	0,9
6	К	7,4	6,3	7,3	27	Х	0,6	1,3	1,1
7	С	6,4	8	7,5	28	Э	0,6	0,6	0,6
8	Ш	4,8	1,5	2,3	29	У	0,6	0,6	0,5
9	М	3,7	5	4,4	30	В	0,3	0,1	0,1
10	Е	3,5	5	4,8	31	Ғ	0,3	0,5	0,3
11	Д	3,2	3,7	4,3	32	Ц	0,1	0,03	0,04
12	О	1,9	3,5	3,8	33	Ч	0,04	0,01	0,04
13	Ұ	1,6	1,7	1,6	34	Щ	0,02	0,01	0,04
14	Ө	1,3	2,6	2,5	35	Ю	0,02	0,01	0,02
15	Ү	1,2	1,6	1,4	36	Я	0,02	0,03	0,06
16	Ә	1,2	1,3	1	37	Ё	0	0	0
17	П	1,2	0,8	1	38	Ң	0	0	0
18	И	1,2	0,7	0,8	39	Й	0	0	0
19	Н	1,2	1	1	40	Һ	0	0	0
20	Ы	1,1	0,2	0,3	41	Ъ	0	0	0
21	З	1	0,7	0,8	42	Ь	0	0	0

Поскольку системы синтеза речеподобных сигналов ориентированы на повседневный светский казахский язык, то для них больше подходит распределение вероятности появления букв алфавита, полученное в ходе анализа статей СМИ. Данное распределение вероятности является основанием для выбора набора слов и словаря для создания речевых баз казахского языка. Речевая база будет содержать минимальное количество слов, начинающихся с наименее употребимой буквы Я и максимальное количество слов, начинающихся с буквы Қ. Таким образом, текст, содержащий, например, 10 слов, начинающихся с буквы «Я», потребует около 1833 слов, начинающихся с буквы Қ.

На основании анализа современных текстов на казахском языке (статей СМИ объемом 20000 слов) была определена относительная встречаемость казахских слов различной длины (табл. 2).

Табл. 2. Частота употребления в казахской речи слов различной длины

Число слогов в слове	1	2	3	4	5	6
Вероятность появления слова, %	19	23,1	30,3	17,7	6,3	3,6

Анализ табл. 2 указывает на преимущественное использование в казахском языке трехсложных слов (до 30,3 %) и двухсложных слов (до 23,1 %). Ударение в казахском языке всегда падает на последний слог. Если слово склоняется и к нему прибавляется окончание, то ударным становится прибавленное окончание.

УДК 004.934

SYNTHESIS OF SPEECHLIKE NOISE FOR DECREASING THE INTELLIGIBILITY OF THE MASKING SPEECH

FIRAS NAZIYAH MAHMOOD AL-MASHHADANI, O.B. ZELMANSKI

Belarusian State University of Informatics and Radioelectronics
6, Brovka Str., Minsk, 220013, Republic of Belarus
alyikotston@yahoo.com

Information security system is discussed. The system is used for active masking of the secret conversation by the speechlike noise formed from this conversation but with no any semantic load. The main aim of the systems is to decrease the intelligibility of the speech that can be intercepted. Proposed system is based on the compilation of parts of the speech of the participants of the secret conversation in real time according to phonemic text that is generated on the base of statistical characteristics of a language in order to get a speechlike signal that will be mixed with the speech of the conversation participants.

Key words: speechlike signal, information security, speech information, acoustic channels, speech intelligibility.

The task of information protection from a leakage via acoustic channels occupies one of the main obstacles in the sphere of information security. In fact that it is the key element in the life of modern world and the substantial part of the threats realizes through it. The protection of speech information is the most important task since the speech is the most natural form of the interaction for the man. There are many methods of interception of speech information with the use of the directed or laser microphones, miniature Dictaphones and so on. The protection of speech information from all possible threats is a complex and expensive task.

One of the approaches to its solution is active masking of conversation, which is based on the creation of acoustic noise on the perimeter of the protected accommodations or directly in the accommodation itself, where a secret conversation is conducted in order to reduce the speech intelligibility for interception means. Analysis of the existing systems for active acoustic masking revealed the fact that in the majority of such systems «white» or «painted» noise is used. However, it should be noted that with the use of «white» noise the signal level necessary for the reliable protection of accommodation can exceed comfortable level and sometimes can reach permissible sanitary standards. On this basis it is possible to make a conclusion about the expedience of applying speechlike noise. This form of noise is oriented not to the creation of random signal but to change real speech signal in such a way that its sense would become incomprehensible.

In this work we examined questions of synthesis of speechlike signals for the protection of speech from a leakage via technical channels. The possibility of forming speechlike signals for the protection of negotiations simultaneously for several languages is discussed, which makes it possible to substantially hinder the interception of the speech of participants in the international negotiations.

The synthesis of speechlike signals for the protection of negotiations in different languages is based on the compilation of the sections of the records of the speech of announcers according to the phonemic text, generated by probabilistic methods taking into account the statistics of language. The proposed synthesis uses allophones as the sections of the records of the speech of announcers, which either previously are separated from the speech of arbitrary announcers and form the data bases, or they are separated directly from the speech of partici-

pants of the negotiations. Phonemic text is formed from the phonemes on the basis of the probabilities of their appearance in the text in accordance with the statistics of the language.

The realization of speechlike signals synthesis system for the protection of acoustic information from a leakage via technical channels deserves attention in following tasks:

1. Automatic switching on the system at the moment of the beginning of the protected conversation on the basis of the analysis of the surrounding acoustic situation for the presence of speech.

2. Forming the phonemic text in accordance with the statistical special features of the language that carries no semantic load.

4. Segmentation of the speech of participants of the conversation per phonetic units in real time.

5. Classification of the chosen phonetic units.

6. Synthesis of speechlike signals according to the phonemic text directly on the basis of the voices of participants of the private talk.

The proposed synthesis of speechlike signals must ensure generation of the noise on the basis of the voices of participants in the negotiations in such a way that it is not possible to divide their speech and generated noise. This noise is formed from the sections of the spoken speech. This process realizes in the modules of the segmentation of speech, classification of speech and synthesis of speech.

Segmentation is the process of the partition of speech in the sections of homogeneous fluctuations, which correspond to the different types of the phonemes: nasal, fricative, occlusive.

After speech is segmented into the phonetic elements it is necessary to separate them into the classes. This is achieved in the module of the classification of speech. The task of classification requires for its solution special classifying characteristics. Each obtained segment is characterized by specific spectral-temporary parameters, which can be divided beside the classes on the form of spectrum, change in the energy, on the periodicity and other conducted investigations. But there is no any parameter which makes it possible to accurately recognize all types of segments. Each type possesses its specific special features, which distinguish it, for example, from the second type, but not distinguishing it from the third type, for which it is necessary to use other special features. Thus, it is necessary to use a set of the parameters and to solve the problem of classification separately for each type of segments. However, since the problem of classification are included into the generation of signal, on its fundamental temporary, spectral characteristics and perception that is similar to speech, the high accuracy of the recognition of phonemes is not required.

Direct synthesis of speechlike signal formed by the random law and with all formal signs (splash nature, the presence of words, spaces between the words, frequency range), maximally similar to real speech, but not containing semantic information, is achieved by a module of the synthesis of speech. It is formed taking into account statistical laws of the selected language of phonemic text beside the acoustic fluctuations of sonic frequency band. The allophone model of the synthesizer of the speech and the bases of the allophones of announcers are used for this process.

Thus, the developed system for the active protection of speech information is automatically switched on with the beginning of secret conversation, provides protection of the secret conversation, since the disguising signal is formed on the basis of the voices of participants of the conversation and does not bear any semantic load, and therefore it makes it possible to substantially hinder interception of speech information be reducing the speech intelligibility. This system can be used when it is not possible to guarantee the complete safety of accommodation, including the cases of negotiating in the car and on the street.

УДК [004.934+004.056.5]:811.411.21

МЕТОД ФОРМИРОВАНИЯ КОМБИНИРОВАННЫХ МАСКИРУЮЩИХ РЕЧЬ СИГНАЛОВ

Г.В. ДАВЫДОВ[1], А.В. ПОТАПОВИЧ[1], Е.Н. СЕЙТКУЛОВ[2]

[1]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
nil53@bsuir.edu.by

[2]Евразийский национальный университет им. Л.Н. Гумилева
ул. Мирзояна, 2, г. Астана, Республика Казахстан
seitkulov_y@enu.kz

Обосновывается метод формирования комбинированных маскирующих сигналов для систем защиты речевой информации от утечки по акустическим каналам. Комбинированные маскирующие сигналы включают «белый» шум в диапазоне 125 – 6500 Гц и сигналы всплескового характера (речеподобные сигналы). Соотношения между указанными видами сигналов выбирается исходя из языка речевого сигнала, требующего защиты.

Ключевые слова: комбинированные маскирующие сигналы, «белый» шум, речеподобные сигналы, разборчивость речи, восприятие речи.

Формирование маскирующих речь сигналов необходимо выполнять с учетом следующих основных акустических характеристик речевых сигналов: среднего уровня звукового давления речи, темпа речи, уровней звукового давления в октавных и 1/3 октавных полосах частот. Технические аспекты решения указанной задачи и анализ существующих методов активной и пассивной защиты речевой информации рассмотрены в работах [1, 2]. Однако, остается открытым вопрос выбора маскирующих сигналов для активной защиты речевой информации от утечки по акустическим каналам. Наиболее часто для защиты речевой информации используются маскирующие сигналы в виде «белого» или «розового» шумов, речеподобные сигналы, музыка или так называемые сигналы «речевой» коктейль.

Для математического описания речевого сигнала наиболее часто используемых следующие математические модели: модель с волновыми уравнениями, описывающими распространение акустических колебаний в речевом тракте; гармоническая модель речевого сигнала, состоящей из сигналов синусоидальной формы плюс шум; модель речевого сигнала в виде набора отрезков функций на основе вейвлет - коэффициентов; модель, основанная на теории модуляции и модель, основанная на аппроксимации спектра набором постоянных составляющих в полосах частот [3]. Наиболее перспективной для решения задачи выбора маскирующих речь сигналов представляется гармоническая модель речевого сигнала. Речевой сигнал моделируется набором гармонических составляющих и шумом, что можно записать в виде уравнения

$$S(t) = R(t) + \sum_{k=1}^{N} A_k \cos\left(2\pi \cdot f \cdot t + \varphi_k\right),$$

где $R(t)$ – шумовая компонента; $A_к$ – амплитуда $к$-ой гармонической составляющей; f – частота $к$-ой гармонической составляющей; $\varphi_к$ - фаза $к$-ой гармонической составляющей; t – время.

В зависимости от вида фонемы в речевом сигнале может преобладать гармоническая составляющая сигнала или шумовая. Для вокализованных фонем преобладает гармоническая составляющая сигнала. При этом амплитуда гармонической составляющей превышает амплитуды шумовой составляющей.

Экспериментальные исследования показали, что при маскировании речевого сигнала «белым» шумом при соотношении сигнал/шум минус 20 дБ на реализации суммарного сигнала во временной области можно выделить временные участки, когда в суммарном сигнале присутствует речевой сигнал (компоненты, содержащие гармонические составляющие). Это может выступать в качестве признака демаскирующего конфиденциальную речь при защите ее маскирующими сигналами типа «белый» шум. Выделение речевой составляющей из шума в этом случае может выполняться с использованием набора узкополосых фильтров, настроенных на формантные составляющие вокализованных звуков, с перестройкой соотношений между формантными составляющими, или уже известными соотношениями присущие определенному диктору.

Для исключения такой возможности в маскирующие речь сигналы необходимо ввести сигналы со свойствами характерными для речевых сигналов. Таким требованиям удовлетворяют речеподобные сигналы, сформированные по базе аллофонов определенного диктора или ряда дикторов, для получения речеподобных сигналов в виде диалога. При формировании диалоговой формы речеподобных сигналов могут быть использованы и различные языки (например, русский, белорусский, украинский и др.). Маскирующие речеподобные сигналы следует формировать с учетом вероятностных характеристик появления определенных фонем в данном языке, а также длины слов, предложений, синтагм и фоноабзацев, характерных для данного языка и с учетом индивидуальных особенностей произношения для определенного диктора.

Таким образом, комбинированные маскирующие сигналы должны включать шумовую компоненту (например, «белый» шум) и составляющую, содержащие ярко выраженные вокализованные участки – речеподобные сигналы. При этом сигнал, который может быть принят средствами разведки нарушителя, будет иметь следующий вид

$$S_c(t) = R(t) + \sum_{k=1}^{N} A_k \cos\left(2\pi \cdot f_k \cdot t + \varphi_k\right) + R_s(t) + R_n(t) + \sum_{l=1}^{M} A_l \cos(2\pi \cdot f_l \cdot t + \varphi_l),$$

где $R_n(t)$ – шумовая компонента маскирующего шума; $R_s(t)$ – шумовая компонента речеподобного сигнала; A_l – амплитуда l-ой гармонической составляющей речеподобного сигнала; φ_l – фаза l-ой гармонической составляющей речеподобного сигнала.

Эффективность защиты речевой информации комбинированными маскирующими сигналами следует определять по параметрам разборчивости и слышимости речи, как предлагается в работе [4]. В отличие от известных формантных методов оценки разборчивости речи и методов, основанных на индексе артикуляции, дополнительно следует использовать вероятностные характеристики

Так как речеподобные сигналы, уровень шума и защищаемая речь варьируются от момента к моменту, фактически конфиденциальность речь будет изменяться с течением времени.

Список литературы

1. *Давыдов Г., Попов В., Потапович А.* // Наука и инновации. 2013. №6(124). С. 15–19.

2. *Давыдов Г.В., Каван Д.М., Попов В.А. и др.* // Доклады БГУИР. 2009 № 4. С. 49–54.

3. *Голубинский А.Н.* //Безопасность информационных технологий. 2009. № 2. С. 12–18.

4. Bradley, J.S. ; Gover, B.N. Designing and Assessing the Architectural Speech Security of Meeting Rooms and Offices. Canada. 2006.

УДК 004.056:65.012.8

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ И СРЕДСТВ ДЛЯ УПРАВЛЯЕМОГО ВОЗДЕЙСТВИЯ НА НАСЕЛЕНИЕ В АУДИО-ВИДЕО ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

ЭБИМОГХАН ТАРИЕБИ МАРШАЛЛ, Л.М. ЛЫНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
leonid@bsuir.by

Изложена концепция использования несмертельного оружия в региональных конфликтах в современном мире. Показано, что использование информационных средств воздействия на ЭВМ и системы передачи данных противника, акустических и электромагнитных воздействий позволяют выводить из строя электронную аппаратуру, людские ресурсы, что, свою очередь, вызывает необходимость разработки методов и средств противодействия и создания систем защиты.

Ключевые слова: оружия несмертельного действия, информационные угрозы.

Несмертельное оружие включает в себя широкий диапазон средств, многие из которых давно известны и широко применяются. Их можно разделить на две категории: обычные и использующие высокие технологии. К обычным средствам относятся, например, дубинки, аэрозольные баллончики, резиновые пули. Основным их преимуществом является простота использования, а недостатком – ограниченная область применения (в основном непосредственное столкновение с враждебно настроенным населением и подавление массовых беспорядков) [1]. К высокотехнологическому несмертельному оружию относятся такие средства, как, например, акустические и электронные системы. Однако при этом следует учитывать, что НСО должно быть функциональным, т.е. стоимость его разработки, внедрения и использования должна оправдывать ожидаемый эффект от его применения. Высокотехнологические НСО должны отвечать следующим требованиям.

Основными принципами разработки различных видов несмертельного оружия должны быть следующие:

– совместимость с обычным вооружением;

– дополнение имеющихся и разрабатываемых систем;

– необходимость разработки ОНД с учетом минимальных дополнительных организационных мер (обучение личного состава, поддержка и сопровождение систем и др.);

– легкость интеграции в существующие оперативные сценарии.

Проанализированы информационные угрозы ОНД. Описаны их виды:

– заблаговременное включение в программное обеспечение систем оружия, управления и связи соответствующих элементов (они активизируются по истечении определенного промежутка времени, по специальному сигналу или иным способом), выводящих обслуживаемые ЭВМ из строя. При этом отказ может восприниматься в качестве естественного сбоя аппаратуры;

– внесение агентурным путем, по каналам связи или другими способами компьютерных вирусов, разрушающих информацию в банках данных и программное обеспечение боевых систем;

– вхождение в каналы связи между ЭВМ и внесение в них ложной информации;

– выведение из строя ЭВМ и стирание информации с помощью мощного СВЧ-излучения, электромагнитного импульса или иным путем;

– синтез речи для использования в целях пропаганды.

Показано поражающее воздействие психотронного оружия и проанализированы принципы действия информационного оружия и ведения информационной войны. Отмечено, что за последние 6–7 лет произошло качественное изменение отношения научных и правительственных кругов за рубежом к проблеме, которая ушла в закрытую область. Исследования по проблеме ведут зарубежные государственные и частные учреждения и инженерно-прикладные организации в штатах Техас (Остин), Нью-Йорк, Вирджиния, Филадельфия (Сент-Джозеф), Нью-Джерси (Принстон), Калифорния (Пало-Альто), по меньшей мере, пятнадцать американских университетов. Широкие научные изыскания по самым различным проблемам биополей и психофизического воздействия осуществляются в странах НАТО, в частности, в университетах Бонна и Фрайбурта (Германия), в лондонском, кембриджском, бристольском университетах (Англия), во Франции, Италии, Дании, а также в Австрии, Аргентине, Бразилии, Голландии. В Китае, Японии, Израиле, ЮАР развернут поиск новых приемов, способов, форм и методов воздействия на сознание и психику больших масс людей и армейских подразделений.

Описаны принципы энергоинформационных воздействий на организм человека и биологические последствия такого рода воздействий. Сделан вывод, что реакция клеток человеческого организма на воздействие СВЧ- и КВЧ-излучений начинается при уровнях воздействия не более 10^{11} Вт/Гц. Это подтверждается, в частности, тем, например, что в технологиях КВЧ-терапии используются сверхнизкие интенсивности электромагнитных излучений порядка $10^{-20}…10^{-21}$ Вт/Гц·см^2, или $3·10^{-10}$ Вт/см^2.

Описано психоэкологическое воздействие мобильной радиотелефонии и ее возможные последствия. Сформулированы основные и опциональные требования к зонам «радиомолчания».

Основные требования:

1. Оперативная организация зон, в которых было бы гарантированно невозможно воспользоваться терминалами сотовой связи.

2. Реализация обеспечения без использования постоянного генератора электромагнитных помех, негативно воздействующих на людей и высокоточную технику (медицинские учреждения, научно-технические центры).

3. Возможность организации таких зон в любых населенных пунктах, вне населенных пунктов, как в зданиях и сооружениях, так и на открытых площадках.

4. Отсутствие зависимости от сетевой инфраструктуры, функциональных особенностей сетей сотовой связи осуществляющих покрытие в зоне блокирования, типа терминала, его производителя.

5. Скрытность воздействия.

В результате проведенных исследований проанализированы основные технические и социально-экономические требования к безопасности информационных систем и сформированы основные требования к безопасности информационных систем в аудио- и видео- системах телекоммуникаций. Показана необходимость формирования защищенных информационных систем на принципах достоверности, конфиденциальности открытости и масштабируемости.

Список литературы

1. *Каторин Ю.Ф., Волковский Н.Л., Тарнавский В.В.* Уникальная и парадоксальная военная техника. М., 2004.

УДК 004.056:65.012.8

ДОКУМЕНТИРОВАНИЕ НА ЭТАПАХ РАЗРАБОТКИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.В. БЕЛОУС, Р.В. ПАРШУКОВА, А.М. ПРУДНИК

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
aleksander.prudnik@bsuir.by

Приводится обоснование разработки, а также практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) для государственных учреждений в соответствии со стандартом СТБ ISO/IEC 27001:2011 «Системы менеджмента информационной безопасности. Требования».

Ключевые слова: информационная безопасность, СМИБ, ISO 27000, оценка рисков, аудит.

СМИБ является частью общей системы управления организации, которая основана на оценке рисков, и предназначена для реализации, эксплуатации, мониторинга и совершенствования ИБ. Реализация СМИБ предполагает использование в качестве руководства для разработки стандартов Международной организации по стандартизации серии ISO 27000 [1], которая в настоящее время насчитывает более 50 стандартов (с учетом стандартов, находящихся на стадии разработки).

Методология реализации СМИБ, как и прочих систем менеджмента (качества, окружающей среды и др.), основана на цикле PDCA (Plan-Do-Check-Act — четырехэтапный итерационный метод решения проблем, используемый для улучшения бизнес-процессов).

К основным достоинствам разработки и внедрения СМИБ принято относить [2]:

– способность организации соответствовать различным требованиям по защите данных, особенно, если данная организация является государственным учреждением, финансовой организацией или учреждением здравоохранения;

– преимущество перед конкурентами;

– снижение расходов, вызванных инцидентами ИБ;

– оптимизация ведения бизнеса — четко определяются обязанности и ответственность сотрудников, а также права доступа к информационным активам.

Перед разработкой СМИБ должны быть выполнены следующие этапы (здесь и далее после наименований этапов в скобках приводятся основные документы, которые должны быть разработаны на данном этапе):

– получение одобрения руководства для реализации СМИБ (описание стандартов, применяемых к организации, описание предварительной области действия СМИБ, определение ролей и сфер ответственности в области СМИБ);

– разработка плана проекта, которая предполагает определение области применения СМИБ (описание производственных процессов и сфер ответственности в области действия СМИБ и за ее пределами; описание информационных систем и телекоммуникационных сетей в области применения СМИБ и за ее пределами);

– определение требований, которым должна соответствовать СМИБ, определение информационных активов организации и получение данных по текущему состоянию ИБ в рамках области применения СМИБ (список основных процессов, функций, объектов, информационных систем, коммуникационных сетей; требования организации, касающиеся конфиденциальности, доступности и целостности; перечень уязвимостей в организации; классификация процессов и активов);

– определение методологии оценки рисков, оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими (перечень целей и средств управления рисками; документированная оценка риска высокого уровня; утвержденная методология оценки риска, совмещенная с контекстом стратегического менеджмента риска в организации).

Непосредственно разработка СМИБ предполагает:

– разработку конечной структуры организации с описанием ролей и сфер ответственности (структура организации, роли и сферы ответственности);

– разработка основы для документации СМИБ (обобщенная база записей и документации по СМИБ, хранилища и шаблоны записей);

– разработку политик ИБ (политики ИБ);

– разработку процедур обеспечения ИБ (процедуры ИБ);

– разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления (план внедрения средств управления, связанных с безопасностью ИКТ и физических объектов);

– разработку средств управления;

– план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, включая аспекты аудита, мониторинга и измерения (список исходных данных для осуществления проверки руководством, процедуры проверки руководством, включая аспекты аудита, мониторинга и измерения);

– разработка 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 (материалы для обучения в области ИБ; формирование обучения в области ИБ, включая должностные обязанности и ответственность; планы обучения, образования и информирования в области ИБ; документирование результатов обучения и образования в области ИБ);

– разработка 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, проверка соответствия СМИБ по контрольной таблице стандарта ISO 27003[1] и проведение внешнего аудита СМИБ [3].

Список литературы

1. ISO – ISO Standards – ISO/IEC JTC 1/SC 27 – IT Security techniques — Режим доступа http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306. Дата доступа 11.01.2014.

2. Four key benefits of ISO 27001 implementation [Электронный ресурс]. — Режим доступа http://blog.iso27001standard.com/2010/07/21/four-key-benefits-of-iso-27001-implementation/. Дата доступа 11.01.2014.

3. СТБ ISO/IEC 27001:2011. Системы менеджмента информационной безопасности. Требования. Введ. 2012-01-01. Минск: БелГИСС, 2012. 36 с.

[1] В настоящее время СТБ ISO/IEC 27003 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности» находится на стадии завершения рассмотрения.

УДК 004.56

ШИРОКОПОЛОСНЫЙ ГЕНЕРАТОР ЭЛЕКТРОМАГНИТНОГО ШУМА

А.В. СИДОРЕНКО[1], М.В. ЖАЛКОВСКИЙ[2]

[1]Белорусский государственный университет
пр-т Независимости, 4, г. Минск, 220030, Республика Беларусь
sidorenkoA@yandex.ru

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
xxl2501@tut.by

Использование вычислительной техники для обработки информации ограниченного распространения требует принятия специальных мер по предотвращению утечки информации по каналам побочных излучений. Достаточно эффективным способом защиты является использование генераторов электромагнитного шума. В связи с этим, интерес представляют широкополосные генераторы шума, обеспечивающие нормативное отношение сигнал/шум в диапазоне частот более 2 ГГц.

Ключевые слова: генераторы шума, побочные электромагнитные излучения и наводки, ПЭМИ.

Применение цифровых технологий в средствах вычислительной техники (СВТ) значительно упрощает решение ряда задач в повседневной жизни, науке и технике. Практически во всей цифровой технике используется двоичная система исчисления: логическая единица передается прямоугольным электрическим импульсом заданной длительности, логический ноль – отсутствием импульса. Резкие изменения напряжения или тока, при помощи которых передается информация в интерфейсах СВТ, приводят к нежелательному излучению в окружающее пространство электромагнитных волн. Данное явление принято называть побочными электромагнитными излучениями (ПЭМИ). Наибольшую опасность представляют ПЭМИ от последовательных интерфейсов, таких как RS-232, USB, Serial ATA, VGA. В отдельных случаях, применение специальной высокочувствительно аппаратуры позволяет восстановить по ПЭМИ передаваемую информацию [1].

Принято выделять три метода защиты от ПЭМИ: *активный, пассивный,* а также *комбинированный*. Последний из указанных методов включает основные мероприятия двух предыдущих [2].

Пассивный метод заключается в экранировании источника излучения, размещении СВТ в экранированном шкафу или в экранировании помещения в целом.

Активный метод защиты предполагает применение специальных постановщиков помех, которые обеспечивают маскировку ПЭМИ от СВТ путем формирования и излучения электромагнитного поля шума в широком диапазоне частот.

Применение генераторов электромагнитного шума становится особенно актуальным при необходимости защиты информации на переносных СВТ (ноутбуках), когда практически невозможно применение пассивных методов защиты.

В зависимости от физического источника шума генераторы шума подразделяются на следующие группы [3]:

– генераторы шума на элементах с высокой рабочей температурой (генераторы на лампах накаливания);

– генераторы шума на специальном электровакуумном шумовом диоде;

– генераторы шума на полупроводниковом стабилитроне (диоде);

– генераторы шума на биполярных транзисторах;

– генераторы шума на интегральных микросхемах и микросборках.

Наилучшими параметрами из вышеперечисленных генераторов шума обладают генераторы на биполярных транзисторах. Основными элементами при построении указанных генераторов являются колебательная система нерезонансного типа и широкополосная цепь обратной связи, что обеспечивает условия для возбуждения ряда колебаний основного вида, а также их гармонических составляющих высших порядков и унтертонов [4].

Разработанный генератор шума состоит из системы связанных генераторов с идентичными параметрами. Структурная схема генератора представлена на рис. 1.

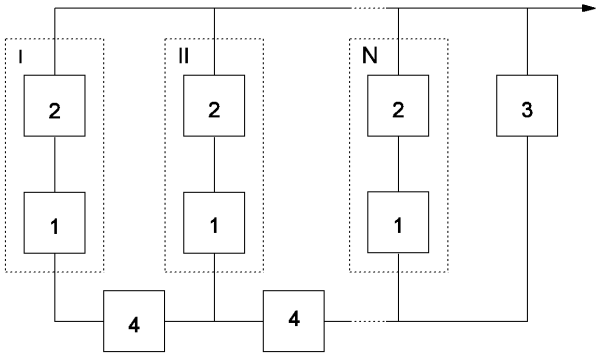


Рис. 1. Структурная схема генератора шума: 1 – активный элемент, 2 – колебательный контур, 3 – цепь запаздывающей обратной связи, 4 – элемент связи

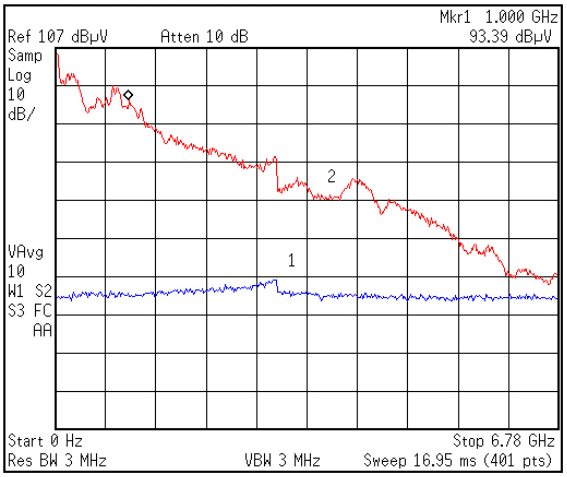


Рис. 2 Спектрограмма выходного сигнала генератора шума: 1 – на нагрузке 50 Ом, 2 – спектрограмма собственных шумов анализатора спектра

Основу генератора составляет многотранзисторная конструкция (генераторы с идентичными параметрами I, II … *N*), состоящая из: активных элементов одного типа (1), колебательных контуров (2), общей цепи запаздывающей обратной связи (ЗОС) с постоянной времени *T* (3), емкостные элементы связи (4), с помощью которых осуществляется связь между генераторами. Положение генераторов на плате, относительно цепи ЗОС определяется собственными рабочими частотами.

Спектрограмма выходного сигнала генератора представлена на рис. 2. В зависимости от излучающей системы и требований по отношению сигнал/шум, рабочий диапазон частот генератора может составлять до 4–5 ГГц.

Таким образом, созданный генератор шума может быть основой активной системы защиты информации от утечки по каналам ПЭМИ.

Список литературы

1. *Wim van Eck* // Computers & Security – Elsevier Advanced Technology Publications, 1985. – В. 4. – Т. 4. – P. 269–286.

2. *Домарев, В.В.* Безопасность информационных технологий. Системный подход. Киев, 2004.

3. *Ван дер Зил А.* Шумы при измерениях. М., 1979.

4. *Иванов, В.П.* // Успехи современной радиоэлектроники, 2008, № 1, с. 37-45.

УДК 004.056.5

МАСКИРОВАНИЕ ИНФОРМАЦИИ ИЗОБРАЖЕНИЕМ И НИЗКОСКОРОСТНЫМ КОДОМ

А.И. МИТЮХИН

Институт информационных технологий БГУИР
ул. Козлова 28, г. Минск, 220037, Республика Беларусь
mityuhin@bsuir.by

Рассматривается метод защиты информации от несанкционированного доступа путем скрытия факта ее передачи и введения структурной избыточности в информацию. Предлагается способ маскирования посредством реализации дисперсионной фильтрации коэффициентов линейного преобразования Хартли. Представлены экспериментальные данные, характеризующие эффективность такого метода защиты информации.

Ключевые слова: помехоустойчивое кодирование, сжатие изображения, дисперсионная фильтрация, коэффициенты преобразования Хартли, ошибка восстановления.

Возможность эффективной защиты информации от несанкционированного доступа за счет использования алгоритмов маскирования и структурной избыточности или помехоустойчивого низкоскоростного кодирования обуславливается следующими двумя основными особенностями изображения и кода сравнительно большой значности $n \geq 100$:

1. Наличием в изображении текстурных областей, имеющих шумовую структуру. Если величина отношения $q = \frac{S}{N} < 0{,}1$, где S – мощность скрываемого сигнала, N – мощность шума, то обеспечивается определенный уровень энергетической скрытности. Следует также учитывать низкую чувствительность человеческого глаза к незначительным изменениям яркости, контрастности, цветов изображения, которые могут возникнуть при внедрении информации.

2. Использование низкоскоростного кода позволяет получить малую спектральную плотность мощности информационной составляющей передаваемого сигнала, усложнить решение задачи обнаружения и дешифрации закодированной информации.

Большинство реальных изображений характеризуется кодовой, межэлементной и визуальной избыточностью данных. Алгоритмы устранения, уменьшения избыточных данных изображения основаны на применении пороговой или дисперсионной (зональной) фильтрации коэффициентов ортогональных преобразований (трансформант). Исходя из теоремы Парсеваля и принципов теории информации, трансформанты с максимальными дисперсиями содержат максимум информации и, следовательно, должны сохраняться в процессе кодирования. Малоинформативные спектральные коэффициенты можно приравнять к нулю. Маскирующая функция коэффициентов преобразования, удовлетворяющая заданной зоне фильтрации коэффициентов, определяется как

$$\gamma_{u,v} = \begin{cases} 0, \hat{g}_{u,v} < l \\ 1 \text{ в остальных случаях} \end{cases}, \forall u, v \in \mathbb{Z}^+, 0 \leq u, v \leq N-1,$$

где – $\hat{g}_{u,v}$ функция двумерного преобразования изображения размерностью $N \times N$. Индексы u, v обозначают значения нормированных частот трансформант в направлениях пространственных переменных y, x. Пространственная зона с соответствующими коор-

динатами, в которую вводится дополнительная кодированная информации в преобразованный фрагмент, определяется двумерной функцией $dtag[\sigma^2]$ распределения дисперсий коэффициентов дискретного преобразования Хартли (ДПХ). Матрицы C_v, C_u дискретного множества функций ДПХ соответственно размером $N \times N$ и $M \times M$ задаются набором ортонормированных базисных векторов c_v, c_u [1]:

$$c_v = \left[c(0v\varphi),\ \ c(1v\varphi),\ \ c(2v\varphi),\ \ \ldots,\ \ c\left((N-1)v\varphi\right)\right]^T, v = 0,1,\ldots,N-1;$$
$$c_u = \left[c(0u\varphi),\ \ c(1u\varphi),\ \ c(2u\varphi),\ \ \ldots,\ \ c\left((N-1)u\varphi\right)\right], u = 0,1,\ldots,M-1,$$

где $c(v\varphi) = \cos\frac{v2\pi}{N} \equiv \cos v\frac{2\pi}{N} + \sin v\frac{2\pi}{N}$, $c(u\varphi) = \cos\frac{u2\pi}{M} \equiv \cos u\frac{2\pi}{M} + \sin u\frac{2\pi}{M}$.

Функция, задающая зону внедрения дополнительной информации, вычисляется по формуле

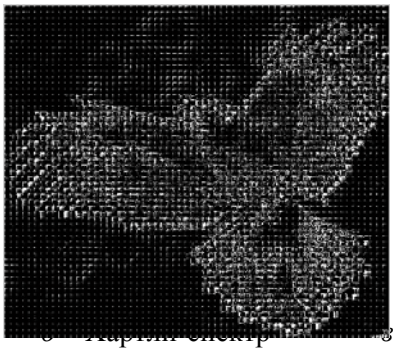
$$dtag[\sigma^2] = dtag[\bar{K}_C] \otimes dtag[\bar{K}_R],$$

где $dtag[\bar{K}_C]$ и $dtag[\bar{K}_R]$ ковариационные матрицы соответственно столбцов и строк ДПХ.

Полученная в результате пространственная зона с соответствующими априорными значениями координат позволяет на приемной стороне выделять дополнительную информацию.

Ниже представлены некоторые экспериментальные результаты. На рис. 1, *а* показано исходное полутоновое изображение размером 512 × 512 пикселей. Изображение разбивалось на блоки размером 8 × 8, которые затем подвергались ДПХ. В центре, рис. 1, *б* представлено изображение ДПХ-спектров блоков. Яркие точки спектров соответствуют коэффициентам ДПХ с максимальными значениями дисперсий. Скрытно передавалось два кодовых слова кода значностью n = 255 и скоростью $R = \frac{k}{n} = 0{,}031$.

В процессе эксперимента в зону фильтрации было внедрено два 8-битовых информационных слова. На рис. 1, *в* показано восстановленное изображение после обратного ДПХ. Как видно, изменение спектрального образа маскирующего изображения практически не внесло искажений в исходное изображение.



а – исходное изображение

Рис. 1. Преобразование маскирующего изображения

Список литературы

1. *Mitsiukhin A*. Segmentation of Dynamical Images by Means of Discrete Hartley Transform / Proceedings 56. International Scientific Colloquium, DE, Ilmenau, 12–16 September 2011 / TU Ilmenau, 2011. – URN (Paper): urn: nbn: de: gbv: ilm1-2011iwk-011:5, id 1100. – P. 1– 4.

УДК 004.056.57:537.531

ВЗАИМОДЕЙСТВИЕ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ С КОМПОЗИТНЫМИ МАТЕРИАЛАМИ НА ОСНОВЕ ТОРФЯНОГО ОРГАНИЧЕСКОГО НАПОЛНИТЕЛЯ И ГИДРОГЕЛЯ

Д.В. СТОЛЕР, Т.А. ПУЛКО, Н.В. НАСОНОВА, Л.М. ЛЫНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Исследовано влияние торфогрунта и различных концентраций порошкообразного торфа в составе полимера на характеристики отражения электромагнитных излучений частотного диапазона 8,0…12,0 ГГц.

Ключевые слова: коэффициент отражения электромагнитного излучения, композитные материалы, торфогрунт, полимеры.

В настоящее время актуальной задачей в системах защиты информации и различных объектов от негативного воздействия электромагнитных излучений (ЭМИ) является формирование композитных материалов для создания высокоэффективных, широкополосных, технологичных и удобных в эксплуатации экранирующих конструкций ЭМИ.

Целью настоящей работы является исследование зависимостей коэффициента отражения ЭМИ композитных материалов на основе органических наполнителей от различных концентраций применяемого наполнителя и связующих его компонентов, позволяющих стабилизировать экранирующие и эксплуатационные свойства.

Синтезировались образцы композитных материалов на основе органического материала и полимерного связующего в определенных пропорциях до образования однородной массы с последующей сушкой при комнатной температуре. В качестве органического наполнителя использовался торф с соответствующими физико-химическими свойствами: низинный торф №1 (рабочая влажность (ω_p) 58%, зольность (A^c) 15%); низинный торф №2 (ω_p = 45%, A^c=30%); верховой торф №3 (ω_p=25%, A^c=23%). В качестве полимерного связующего использовался полиэлектролитный гидрогель. Композитные материалы изготавливались с объемным содержанием порошкообразного наполнителя 20%, 30% и 40%. Для проведения сравнительного анализа влияния полимерного связующего на экранирующие характеристики органического наполнителя синтезировались образцы на основе торфогрунта.

Исследование экранирующих характеристик композитных образцов разработанных материалов выполнялось в диапазоне частот 8,0…12,0 ГГц. Для этой цели был использован панорамный измеритель ослабления и КСВН Я2Р-67 с ГКЧ-61 и волноводным трактом, которые обеспечивают выделение и детектирование уровней падающей и отраженной волн электромагнитного излучения, прошедших и отраженных от образца. Калибровка оборудования перед началом измерений экранирующих характеристик производилась по стандартной методике.

Частотные зависимости коэффициента отражения (*S11*) ЭМИ для исследуемых образцов композитных материалов приведены на рис. 1.

Полученные композитные материалы с увеличением объемного содержания порошкообразного наполнителя характеризуются улучшением свойств, способствующих понижению коэффициента отражения в рассматриваемом диапазоне частот. Так для композитных

материалов на основе низинного торфа №1, рис. 1, *а*, на частоте 10 ГГц коэффициент отражения изменяется с –2,1 дБ до –6,5 дБ, на основе низинного торфа №2, рис. 1, *б* – с –1,9 дБ до –6,0 дБ, на основе верхового торфа, рис. 1, *в* – с –2,2 дБ до –7,3 дБ.

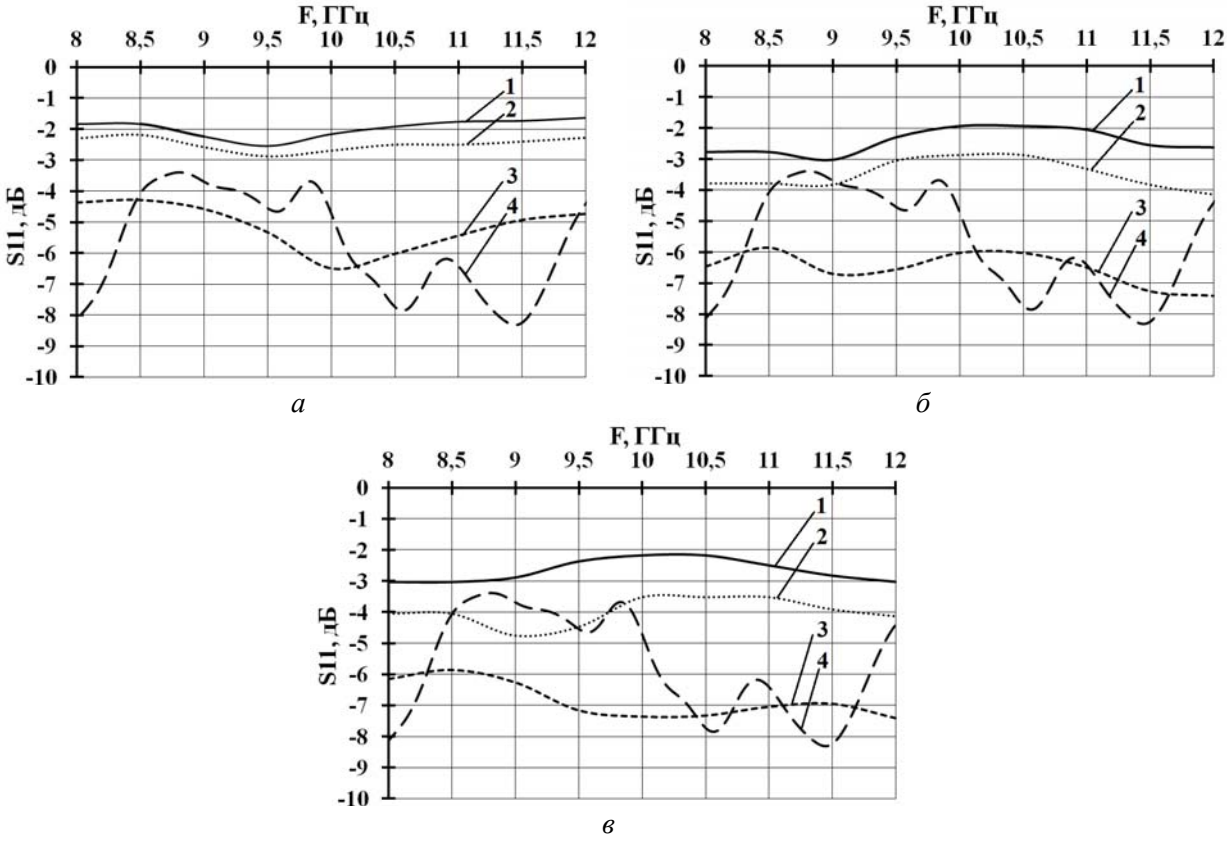


Рис. 1. Частотные зависимости коэффициента отражения образцов композитных материалов на основе: *а* – низинного торфа №1, *б* – низинного торфа №2, *в* – верхового торфа №3 в частотном диапазоне 8,0…12,0 ГГц, где:
1 – объемное содержание органического материала 20 %;
2 – объемное содержание органического материала 30 %;
3 – объемное содержание органического материала 40 %; 4 – торфогрунт

Для торфогрунта наблюдается изменение коэффициента отражения в пределах –3,4…–8,3 дБ, причём различные физико-химические свойства исследованных органических наполнителей существенно не отражаются на экранирующих характеристиках. Формирование композитного материала с применением полимерного связующего при различном объёмном соотношении органического наполнителя позволило получить коэффициент отражения ЭМИ в пределах –1,9…–7,3 дБ в диапазоне частот 8,0…12,0 ГГц.

Таким образом, использование в составе композитного материала на основе торфа полимерного связующего позволяет увеличить коэффициент отражения ЭМИ в диапазоне частот 8,0…12,0 ГГц за счёт стабильного влагосодержания композита, а изменение объемного содержания органического материала в составе композита позволяет управляемо изменять коэффициент отражения в зависимости от требований эксплуатации.

УДК 681.3.06

ОЦЕНКА КАЧЕСТВА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СТАТИСТИЧЕСКИМИ ТЕСТАМИ

Г.В. ДАВЫДОВ, А.И КУХАРЕНКО

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
nil53@bsuir.edu.by

Описывается метод оценки случайности последовательности чисел статистическими методами. Рассматриваются пакет тестов NIST, определяется роль каждого теста, входящего в него. Тесты используются при оценке и проверке генераторов случайных чисел.

Ключевые слова: генератор случайных чисел, статистические тесты, случайная последовательность, вероятность, программа.

Современные информационные технологии широко используют случайные числа в самых разных приложениях — от имитационного моделирования до криптографии. Случайность чисел в заданных последовательностях оценивается статистическими методами. Для этого используются семейства статистических тестов, например, тесты Д. Кнута, тесты Дж. Марсальи, Национального института стандартов США (тесты NIST) и др. В состав тестов NIST входят 15 статистических тестов, основные требования которых заключаются в следующем.

Частотный побитовый тест (Frequency Test) определяет соотношения между нулями и единицами во всей двоичной последовательности. В этом тесте определяется P-value, являющейся оценкой вероятности того, что вычисленное значение нормированной кумулятивной суммы не превышает заданного порога. Выполнение неравенства P-value < 0,01 (рекомендованное значение), указывает на несоответствие входной последовательности гипотезе о нормальном распределении вероятности. Все последующие тесты проводятся при условии прохождения этого теста.

Частотный блочный тест (Frequency Test within a Block) определяет количество единиц внутри блока длиной k бит. В тесте выясняется, действительно ли частота повторения единиц в блоке длиной k бит приблизительно равна k/2 , как можно было бы предположить в случае абсолютно случайной последовательности.

Тест на последовательность одинаковых бит (Runs Test). Тест на самую длинную последовательность единиц в блоке (Test for the Longest Run of Ones in a Block). Первый тест подсчитывает полное число серий в исходной последовательности, где под серией подразумевается непрерывная подпоследовательность одинаковых бит. Второй определяет самую длинную серию единиц внутри блока. Цель данных тестов – сделать вывод о том, действительно ли серии, соответствуют по числу и по длинам сериям, наблюдаемым в абсолютно случайной последовательности.

Тест рангов бинарных матриц (Binary Matrix Rank Test) рассчитывает ранги непересекающихся подматриц, построенных из исходной двоичной последовательности. Целью этого теста является проверка на линейную зависимость подстрок фиксированной длины, составляющих первоначальную последовательность.

Спектральный тест (Discrete Fourier Transform Test). В данном тесте оценивается высота пиков дискретного преобразования Фурье исходной последовательности. Тест выявляет периодические свойства последовательности, например, наличие повторяющихся участков.

Тест на совпадение неперекрывающихся шаблонов (Non-overlapping Template Matching Test). Тест на совпадение перекрывающихся шаблонов (Overlapping Template Matching Test). Эти 2 теста подсчитывают количество заранее определенных шаблонов, найденных в исходной последовательности. Цель – выявить ГСЧ, формирующие слишком часто заданные непериодические шаблоны.

Универсальный статистический тест Маурера (Maurer's "Universal Statistical" Test) определяет, может ли данная последовательность быть значительно сжата без потерь информации.

Тест на периодичность (Serial Test) подсчитывает частоты всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов. Целью является определение, действительно ли количество появлений 2m перекрывающихся шаблонов длиной m бит приблизительно такое же, как в случае абсолютно случайной входной последовательности бит.

Тест приблизительной энтропии (Approximate Entropy Test). Как и в тесте на периодичность, в данном тесте акцент делается на подсчете частоты всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов. Цель теста – сравнить частоты перекрывания двух последовательных блоков исходной последовательности с длинами m и m+1 с частотами перекрывания аналогичных блоков в абсолютно случайной последовательности.

Тест кумулятивных сумм (Cumulative Sums Test). Тест на произвольные отклонения (Random Excursions Test). Тест на произвольные отклонения состояний последовательности (Random Excursions Variant Test). Эти 3 теста объединяет преобразование последовательности (0,1) в соответствующую последовательность (-1, +1) и подсчет кумулятивных сумм. Первый тест определяет максимальное отклонение от нуля кумулятивной суммы при произвольном обходе и определяет, является ли сумма слишком большой или слишком маленькой по сравнению с ожидаемым поведением такой суммы у абсолютно случайной входной последовательности, для которой отклонение должно быть вблизи нуля. Второй тест подсчитывает число циклов, имеющих строго k посещений при произвольном обходе кумулятивной суммы. Третий тест подсчитывает общее число посещений определенного состояния при произвольном обходе кумулятивной суммы. Определяется, отличаются ли результаты от аналогичных результатов в случае абсолютно случайной последовательности.

Тесты NIST, ввиду наличия подробной документации и открытых исходных кодов программной реализации тестов, получили широкое распространение. Чтобы воспользоваться этими тестами, необходимо скомпилировать исходный код в исполняемый EXE файл. Программа представляет собой консольное приложение, в котором задается тестируемый файл, указывается количество бит в последовательности (рекомендуется не менее 1000000 бит), выбираются необходимые тесты и настройки по каждому тесту. После выполнения расчетов, программа сохраняет результаты тестирования в текстовый файл. Далее необходимо произвести обработку результатов тестов, например, построить гистограмму распределения P-value, которая должна иметь равномерное распределение, и, в конечном итоге, определить качество тестируемой случайной последовательности.

Список литературы

1. *Rukhin A.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications// NIST. 2010. P.131.

2. *Juan Soto*. Statistical Testing of Random Number Generators// National Institute of Standards and Technology. P. 12.

УДК [004.934+004.056.5]:811.411.21

ВОЗБУЖДЕНИЕ ВИБРАЦИЙ ОГРАЖДАЮЩИХ КОНСТРУКЦИЙ ПОМЕЩЕНИЙ ДЛЯ МАСКИРОВАНИЯ РЕЧИ

Г.В. ДАВЫДОВ[1], А.В. ПОТАПОВИЧ[1], Е.Н. СЕЙТКУЛОВ[2]

[1]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
nil53@bsuir.edu.by

[2]Евразийский национальный университет им. Л.Н. Гумилева
ул. Мирзояна, 2, г. Астана, Республика Казахстан
seitkulov_y@enu.kz

Рассматриваются механизмы возбуждения маскирующих речь вибраций ограждающих конструкций помещений для защиты речевой информации от утечки по акустическим каналам. Обосновывается требования к вибрационным преобразователям и методы измерения их характеристик для обеспечения защиты речевой информации в помещениях.

Ключевые слова: вибрационные преобразователи, комбинированные маскирующие сигналы, спектр колебаний, разборчивость речи.

Одним из методов защиты речевой информации от утечки по акустическим каналам является активный метод маскирования речевых сигналов в ограждающих строительных конструкциях помещений. Суть метода заключается в создании в ограждающих конструкциях вибраций, маскирующих речевой сигнал.

Системы активной защиты речевой информации включают генератор маскирующих сигналов и преобразователи электрических сигналов в акустические сигналы или механические перемещения.

В качестве преобразователей широко применяются электромагнитные и пьезоэлектрические. Недостатком электромагнитных преобразователей является низкая эффективность в области высоких частот (от 2000 до 8000 Гц). Пьезоэлектрические преобразователи не развивают необходимых усилий для возбуждения вибраций ограждающих элементов конструкций в диапазоне частот от 100 до 500 Гц.

При установке таких преобразователей на ограждающие элементы конструкций в местах их установки создаются силовые воздействия на ограждающие элементы конструкций помещений, вызывающие вибрацию.

Для оценки эффективности преобразователей необходимо измерять их параметры в частотном диапазоне речевых сигналов от 160 до 5600 Гц, чтобы иметь гарантию того, что преобразователи обеспечивают формирование маскирующих вибраций во всем диапазоне частот. В работах [1,2] указывается на необходимость проверки выталкивающей силы преобразователей, а не контроля ускорений или амплитуд вибраций самих преобразователей. Амплитуды вибраций преобразователей не являются однозначно определяемой величиной характеризующей взаимодействие преобразователя с ограждающей конструкцией, на которой он установлен. В данном взаимодействии важной характеристикой является масса преобразователя.

Так как механизм взаимодействия преобразователя с ограждающей конструкцией носит инерционный характер, то с увеличением массы преобразователя при одной и той же амплитуде колебаний преобразователя силовые воздействия на ограждающую конструкцию будут увеличиваться.

Силовое воздействие на ограждающую конструкцию определится из выражения

$$F = m \cdot A \cdot \omega^2 Sin(\omega \cdot t),$$

где A – амплитуда вибраций; ω – частота вибраций: t – время; m – масса преобразователя.

Структурная схема установки для контроля выталкивающей силы преобразователей показана на рис. 1.

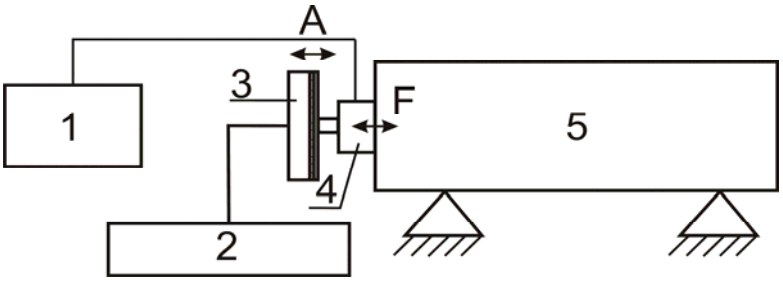


Рис. 1. Структурная схема установки для контроля выталкивающей силы:
1 – измеритель силы, 2 – генератор шума в 1/3 октавных полосах, 3 – вибрационный преобразователь, 4 – датчик силы, 5 – инерционная масса

Масса, на которую устанавливается датчик силы, представляет собой цилиндрическую массу диаметром 120 мм и длиной 350 мм и массой 16 кг.

Установка позволяет проверять амплитудно-частотную характеристику преобразователей и сравнивать характеристики преобразователей различных типов.

Эффективность работы преобразователей во многом определяется правильным выбором мест установки и способов крепления преобразователя, к ограждающим конструкциям.

Требуемое количество преобразователей определяется исходя из мест их расположения, конструкции и материалов ограждающих поверхностей, оконных проемов и инженерных коммуникаций, а также эффективного радиуса маскирования речевых сигналов преобразователями.

Под эффективным радиусом маскирования речевых сигналов преобразователями понимается максимальное расстояние по поверхности от места его установки до места, где уровни вибраций превышают маскируемый речевой сигнал в заданное количество раз.

Эффективный радиус маскирование речевых сигналов зависит не только от характеристик самого преобразователя, но и во многом – от характеристик ограждающих конструкций помещений поверхностей и поэтому определяется экспериментально. При удалении от места установки преобразователя на 1 м, уровень создаваемых им маскирующих вибраций уменьшается примерно на 3 – 6 дБ.

Список литературы

1. *Воробьев В.И., Давыдов Г.В.* // Доклады БГУИР. 2005 № 5 (17 мая 2005 г.). С. 32.

2. *Готовко М.А., Корунос П.С., Потапович А.В.* // Тезисы докладов X Белорусско-российской научно-технической конференции «Технические средства защиты информации» Минск, 29-30 мая 2012 г. С. 12.

3. *Готовко М.А., Корунос П.С., Потапович А.В.* // Тезисы докладов X Белорусско-российской научно-технической конференции «Технические средства защиты информации» Минск, 29-30 мая 2012 г. С. 12.

УДК. 004.3

К ВОПРОСУ ПОВЫШЕНИЯ ОБОСНОВАННОСТИ ПЛАНИРОВАНИЯ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л.Л. УТИН, М.А. САБЕРИАН

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
ullktn@mail.ru, maryam.saberian@yandex.ru

Разработка программно-аппаратных систем поддержки принятия решений в области информационной безопасности является одним из приоритетных направлений научных исследований Республики Беларусь. Одной из составных задач, решаемых данными системами является повышение качества планирования применения средств защиты информации. В докладе предлагается к обсуждению направления повышения качества решения данной задачи.

Ключевые слова: планирование применения средств защиты, моделирование радиоизлучений средств вычислительной техники, поддержка принятия решений.

В настоящее время выбор организационных и технических мер защиты информации от утечки по каналам побочных электромагнитных излучений и наводок осуществляется, как правило, путем привлечения экспертов в области обеспечения информационной безопасности [1]. Такой подход позволяет наиболее полно учесть требования отечественного законодательства, однако обладает множеством недостатков, одним из которых является недостаточное внимание к исследованиям условий функционирования средств вычислительной техники внутри объектов информатизации типа «защищаемое помещение». В результате требования, предъявляемые к защите информации, как правило, являются завышенными. Основной причиной сложившегося положения дел является отсутствие в Республике Беларусь сертифицированных средств поддержки принятия решений в области обеспечения информационной безопасности. Разработка подобных средств является важной актуальной научной и практической задачей.

Проведенный анализ диссертационных работ, защищенных в Республике Беларусь за прошедшие годы, показал, что в данном направлении отдельными авторами предлагаются достаточно оригинальные решения позволяющие повысить обоснованность применения активных и пассивных средств защиты информации. Например, в работе [2] предложено на этапе планирования применения средств защиты информации, использовать разработанный программный комплекс имитационного моделирования зон радиоизлучений ЭВМ, размещаемых в защищаемых помещениях. Основу данного комплекса составляет методика оптимизации размещения ЭВМ в защищаемом помещении, позволяющая минимизировать уровень радиоизлучений ЭВМ за пределы контролируемой зоны.

Разработанный программный продукт позволяет [3]:

– отображать суммарную зону электромагнитных излучений ЭВМ и других электронных устройств, находящихся в помещении;

– определять расстояние до точки, в которой еще возможен перехват информативных излучений ЭВМ радиоприемной аппаратурой злоумышленников с учетом затухания электромагнитного поля при прохождении его через различные препятствия;

– находить место для размещения ЭВМ в защищаемом помещении, на котором ее излучения за пределы контролируемой зоны будут минимальны;

– отображать потенциально опасные направления распространения излучений за пределы контролируемой зоны;

– отображать зону помех активных средств защиты информации, планируемых к применению в помещении, а также визуализировать степень маскирования информативных излучений ЭВМ;

– осуществлять подбор места расположения генераторов шума для минимизации мощности излучаемых помех, при максимизации удаления средств защиты от рабочих мест персонала;

– подбирать минимальные размеры пассивных средств защиты информации, визуализировать эффективность их применения.

В целом применение данного программного продукта позволяет уже на этапе планирования оценить целесообразность применения тех или иных средств защиты и сократить финансовые затраты на их приобретение за счет оптимизации размещения ЭВМ в защищаемом помещении по критерию минимизации зоны ее радиоизлучений. Однако, в ходе анализа предложенного программного комплекса, был выявлен ряд недостатков, которые могут лечь в основу для дальнейшего совершенствования процесса планирования применения средств защиты информации. Основные недостатки и пути их решения предлагаются к обсуждению.

Список литературы

1. *Утин Л.Л., Кред Х.М.* Особенности оценки утечек информации через побочные электромагнитные излучения и наводки // Инженерный вестник. 2010. №2(30). С.27–31.

2. *Кред, Х.М.* Программный комплекс имитационного моделирования зон радиоизлучений средств вычислительной техники в защищаемых помещениях. Дис... канд. техн. наук. Минск, 2013.

3. *Утин Л. Л., Григорьев В. Л. , Кред Х. М.* Усовершенствованная методика построения зоны излучения персональных электронных вычислительных машин // Доклады БГУИР. 2010. №7(53). С.53–58.

УДК 539.2

СПЕКТРЫ ОТРАЖЕНИЯ И ПРОХОЖДЕНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СЛОИСТЫХ СТРУКТУР С ТОНКОЙ ПЛЕНКОЙ МЕТАЛЛА

АХМЕД АЛИ АБДУЛЛАХ АЛЬ-ДИЛАМИ, И.А. ВРУБЛЕВСКИЙ,
К.В. ЧЕРНЯКОВА, Г.А. ПУХИР, И.А. ЗАБЕЛИНА

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
vrublevsky@bsuir.edu.by

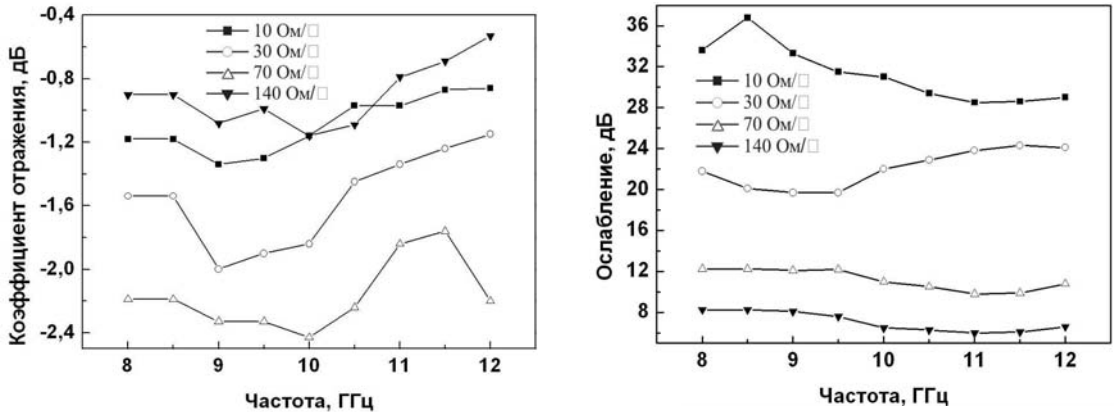
Для решения задачи согласования волновых сопротивлений двух сред в процессах поглощения электромагнитного излучения используются слоистые структур с пленкой металла толщиной 10 – 100 нм. В данной работе изучались вопросы влияния толщины диэлектрика на взаимодействие электромагнитного излучения со структурой диэлектрик – тонкая пленка металла. В качестве образцов использовались мембраны анодного оксида алюминия с пленками нихрома поверхностным сопротивлением от 140 до 10 Ом/□.

Ключевые слова: слоистая структура, электромагнитное излучение, пленка нихрома, анодный оксид алюминия.

Для процессов экранирования электромагнитного излучения (ЭМИ) используются особенности распространения волн, связанные с поглощением электромагнитной энергии в материалах и отражением электромагнитной волны от границы раздела двух сред. При распространении ЭМИ на границе раздела сред с различными волновыми сопротивлениями, часть электромагнитной энергии проходит через нее, а часть отражается от нее. Причем коэффициент отражения зависит от соотношения волновых сопротивлений двух сред. Одним из путей для решения задачи согласования волновых сопротивлений является использование слоистых структур с тонкой пленкой металла толщиной 10–100 нм для поглощения электромагнитного излучения [1].

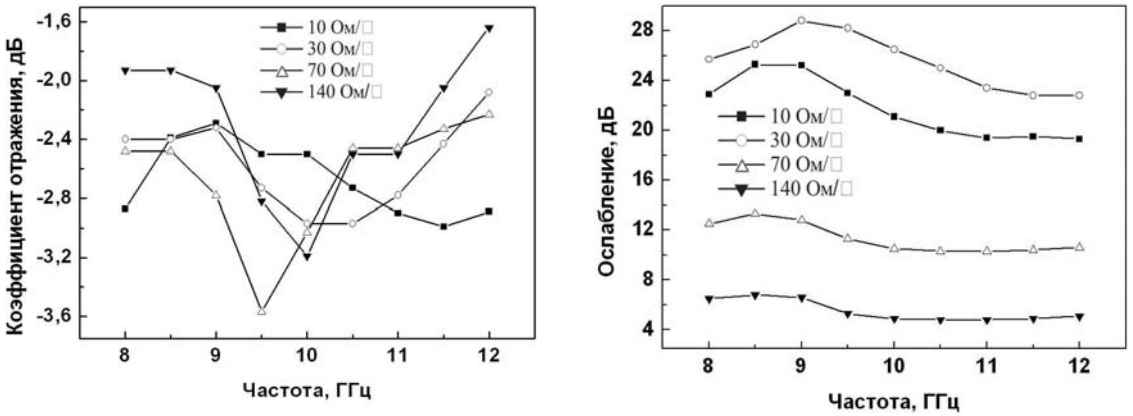
В работе исследовались вопросы влияния толщины диэлектрика на взаимодействие электромагнитного излучения со структурой диэлектрик – тонкая пленка металла. Для анодного оксида алюминия толщиной 70 мкм минимальный коэффициент отражения на уровне –2,5 дБ имела структура с пленкой нихрома поверхностным сопротивлением 70 Ом/□. Коэффициент ослабления такой структуры был относительно низким, около 8 дБ. Более высокий коэффициент ослабления имели структуры с пленкой поверхностным сопротивлением 30 и 10 Ом/□, в среднем 24 и 30 дБ, соответственно. В тоже время коэффициенты отражения таких структур оставались высоким –1,9 дБ (30 Ом/□) и – 1,2 дБ (10 Ом/□). Для процессов взаимодействия электромагнитного излучения со слоистой структурой с анодным оксидом алюминия толщиной 70 мкм и тонкой пленкой нихрома можно выделить следующие закономерности. Увеличение толщины пленки нихрома (уменьшение поверхностного сопротивления) приводило к заметному росту коэффициента ослабления и к увеличению коэффициента отражения. Исключение было только для образца с пленкой нихрома поверхностным сопротивлением 140 Ом/□. Это, по нашему мнению, было связано с островковой структурой пленки. Увеличение толщины слоя диэлектрика в два раза за счет размещения впереди дополнительной мембраны анодного оксида алюминия с толщиной равной исходной мембране приводило к заметному улучшению характеристик ослабления и отражения. Так для образцов с пленками нихрома поверхностным сопротивлением 30 Ом/□ ослабление увеличивалось с 22 до 26 дБ и коэффициент отражения уменьшался с –1,9 дБ до –2,9 дБ. В тоже время ослабление в структурах с пленкой нихрома поверхностным со-

противлением 10, 70 и 140 Ом/□ оставалось приблизительно на таком же уровне. Наиболее сильное уменьшение коэффициента отражения до –3,6 дБ наблюдалось для структуры с пленкой нихрома 70 Ом/□. Особенность слоистых структур с анодным оксидом алюминия толщиной 140 мкм – это появление в спектрах образцов с пленками нихрома эффекта резонансного отражения.



а *б*

Рис. 1. Спектры отражения (*а*) и ослабления (*б*) слоистых структур с анодным оксидом алюминия толщиной 70 мкм и пленками нихрома с различным поверхностным сопротивлением



а *б*

Рис. 2. Спектры отражения (*а*) и ослабления (*б*) слоистых структур с анодным оксидом алюминия толщиной 140 мкм и пленками нихрома с различным поверхностным сопротивлением

Таким образом, увеличение толщины анодного оксида алюминия с 70 до 140 мкм приводило к снижению отражения слоистых структур. Следовательно, толщина диэлектрического слоя в слоистой структуре оказывает заметное влияние на уменьшение коэффициента отражения электромагнитного излучения и создание условий для возникновения эффекта резонансного отражения.

Список литературы

1.*Усанов Д.А., Скрипаль А.В., Абрамов А.В. и др*. Измерение электропроводности нанометровых металлических пленок в слоистых структурах по спектрам отражения электромагнитного излучения – Саратов: Изд-во Сарат. университета, 2007. – 84 с.

УДК 539.2

ИССЛЕДОВАНИЕ РЕЗОНАНСНОГО ОТРАЖЕНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СТРУКТУРАМИ АНОДНЫЙ ОКСИД АЛЮМИНИЯ – ТОНКАЯ ПЛЕНКА МЕТАЛЛА

АХМЕД АЛИ АБДУЛЛАХ АЛЬ-ДИЛАМИ[1], И.А. ВРУБЛЕВСКИЙ[1], К.В. ЧЕРНЯКОВА[1], Г.А. ПУХИР[1], В.Х. ВИДЕКОВ[2]

[1]*Белорусский государственный университет информатики и радиоэлектроники*
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
vrublevsky@bsuir.edu.by

[2]*Технический университет – София*
бул. К. Охридски, 8, г. София, 1000, Болгария
videkov@tu-sofia.bg

Одним из эффективных и простых способов уменьшения отражения является использование резонансного отражения электромагнитного излучения. В данной работе изучалось влияние толщины пленки металла в области четвертьволнового резонанса на коэффициент отражения электромагнитного излучения структур диэлектрик – пленка металла. В качестве образцов использовались мембраны анодного оксида алюминия с пленками нихрома поверхностным сопротивлением от 140 до 10 Ом/□.

Ключевые слова: резонансное отражение, электромагнитное излучение, пленка нихрома, анодный оксид алюминия.

Для достижения эффективного поглощения электромагнитного излучения необходимо использовать материалы, имеющие высокие значения мнимой части диэлектрической или магнитной проницаемости. Такому условию полностью отвечают только идеальные проводники – металлы. Однако при использовании металлов возникает проблема согласования бесконечно малого волнового сопротивления металла с конечным волновым сопротивлением свободного пространства. Одним из путей решения такой задачи является использование тонких пленок металла толщиной 10 – 100 нм для поглощения электромагнитного излучения. Существует несколько способов позволяющих значительно снизить отражение электромагнитных волн от проводящей поверхности. Одним из наиболее эффективных и простых способов уменьшения отражения является использование резонансного отражения электромагнитных волн. В этом случае тонкая пленка металла наносится на непоглощающий диэлектрический материал, толщина которого кратна четверти длины волны. Такая слоистая структура имеет узкополосную характеристику отражения и может использоваться в конструкциях фильтров поглощения электромагнитных волн.

Целью данной работы являлось изучить влияние толщины металлического слоя в области четвертьволнового резонанса на коэффициент отражения электромагнитного излучения структур диэлектрик – пленка металла. В работе исследовался спектр отражения электромагнитной волны, формируемый при взаимодействии ее со структурой анодный оксид алюминия – пленка нихрома. Мембраны анодного оксида алюминия получали электрохимическим окислением алюминиевой фольги. Процесс проводили в двухэлектродной ячейке в 0,3 М водном растворе щавелевой кислоты при постоянном напряжении анодирования 60 В. В качестве катода использовалась сетка из платиновой проволоки. Остаточный слой алюминия удаляли с помощью селективного травителя на основе $CuCl_2$ и HCl. Полученные мембраны пористого оксида алюминия имели толщину 140 мкм (значение диэлектрической проницаемости 8). На одну из сторон мембран по-

ристого оксида алюминия методом ионно-лучевого испарения наносились тонкие пленки нихрома различной толщины с поверхностным сопротивлением 140, 70, 30 и 10 Ом/□. Поверхностное сопротивление пленок нихрома измерялось на установке ИУС–2М. Для исследования экранирующих характеристик образцов использовался генератор качающей частоты и индикатор коэффициента стоячей волны по напряжению (КСВН) и ослабления Я2Р-67. Измерения проводились в частотном диапазоне от 8 до 12 ГГц. Излучателем и приемником сигнала служили концы прямоугольных волноводов.

На рис. 1, *а* приведены экспериментальные зависимости коэффициентов отражения для структур анодный оксид алюминия – нихром с различной толщиной пленки нихрома. Как видно из рис. 1, *а*, в исследуемых структурах при отражении электромагнитного излучения имел место четвертьволновой резонанс. Наиболее сильно резонансное отражение проявлялось в структуре с пленкой нихрома поверхностным сопротивлением 70 Ом/□. Резонансный минимум коэффициента отражения на частоте 9,5 ГГц достигал –3,6 дБ. В случае образцов с более тонкой пленкой нихрома (140 Ом /□) или с более толстой пленкой (30 Ом/□) наблюдалось уменьшение коэффициента резонансного отражения. Для образцов с пленкой нихрома поверхностным сопротивлением 10 Ом/□ коэффициент отражения приближался к насыщению и был равен –2,5 дБ.

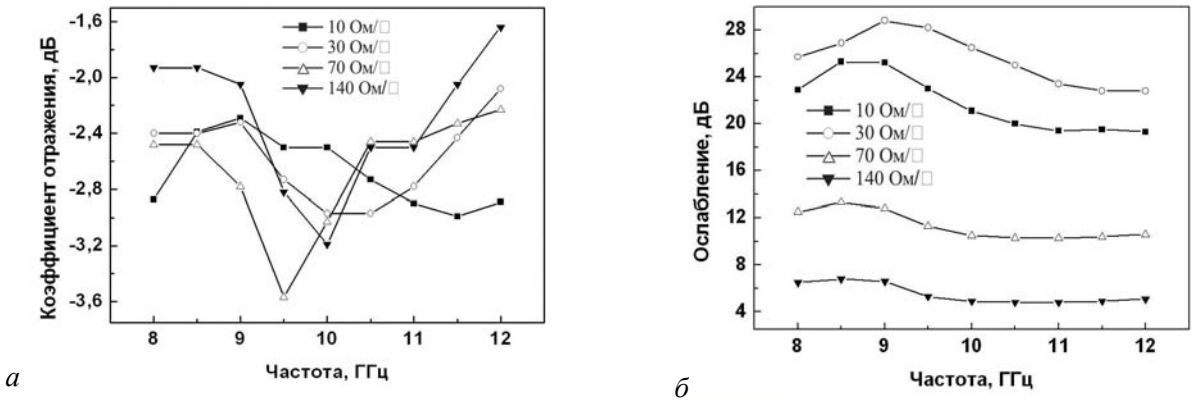


Рис.1 Спектры отражения (*а*) и ослабления (б) слоистых структур анодный оксид алюминия – нихром с поверхностным сопротивлением пленок нихрома

На рис. 1, *б* показано влияние толщины пленки нихрома на ослабление электромагнитного излучения слоистой структурой. Как видно из рис. 1, *б*, максимальное ослабление имели структуры с пленкой нихрома поверхностным сопротивлением 10 Ом/□ и 30 Ом/□, коэффициент ослабления для которых достигал значений 24 и 28 дБ соответственно. Ослабление на уровне 7 дБ показала структура с пленкой нихрома поверхностным сопротивлением 140 Ом/□. Образец с более толстой пленкой нихрома поверхностным сопротивлением 70 Ом/□ имел ослабление на уровне 13 дБ.

По результатам исследований можно сделать вывод, что наиболее сильно эффект резонансного отражения электромагнитного излучения проявлялся в структуре анодный оксид алюминия – нихром с пленкой нихрома поверхностным сопротивлением 70 Ом /□.

Список литературы

1. *Усанов Д.А., Скрипаль А.В., Абрамов А.В., Боголюбов А.С.* Резонансное отражение электромагнитного излучения от структур с нанометровыми металлическими слоями // Физика волновых процессов и радиотехнические системы. 2006, № 3, с. 59–63.

УДК. 004.3

ОБОСНОВАНИЕ ВЫБОРА ПРОГРАММНОГО СРЕДСТВА ДЛЯ ПОСТРОЕНИЯ ТРЕХМЕРНОЙ ЗОНЫ РАДИОИЗЛУЧЕНИЙ ЭВМ В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ

Л.Л. УТИН, М.А. САБЕРИАН, А.А. СУДАКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
ullktn@mail.ru

Построение трехмерной зоны радиоизлучений средств вычислительной техники позволяет получить представление об особенностях функционирования ЭВМ в защищаемом помещении, определить наиболее опасные направления утечки информации по каналу побочных электромагнитных излучений и наводок и повысить обоснованность принятия решений по применению средств активной и пассивной защиты информации. В настоящее время трехмерные объекты могут быть построены с помощью различных 3D редакторов, результаты обзора которых представлены в докладе.

Ключевые слова: трехмерное моделирование, 3D редакторы, планирование применения средств защиты, моделирование радиоизлучений средств вычислительной техники.

В настоящее время моделирование все глубже внедряется в различные сферы деятельности, будь то производство, медицина, наука, искусство, защита информации. Это обусловлено возросшими вычислительными возможностями современных ЭВМ, а также доступностью на рынке разнообразных средств имитационного моделирования, которые позволяют научным сотрудникам при проведении разнообразных исследований учитывать большее количество факторов, а также решать новые задачи. Одной из таких задач является построение трехмерной зоны радиоизлучений средств вычислительной техники для последующего определения опасности влияния излучений на персонал, постоянно работающий в защищаемом помещении, а также выявление потенциально опасных направлений излучений, выходящих за пределы контролируемой зоны [1, 2].

Вместе с тем, выбор редактора для решения конкретной прикладной задачи сопряжено с определенными трудностями. Производители компьютерных приложений, как правило, не акцентируют внимание будущих пользователей на недостатках их продуктов. В результате довольно часто распространены ситуации, когда выбрав определенный продукт для моделирования, исследователи вынуждены в последующем отказаться от его использования по различным причинам. Временные затраты на изучение особенностей использования того или иного программного обеспечения для решения научных и практических задач, как правило, не оплачиваются, и в ряде случаев создают предпосылки для прекращения исследований.

Авторами были проанализированы отдельные наиболее распространенные 3D-редакторы. В результате анализа было выявлено, что с точки зрения доступности программное обеспечение можно разделить на две основных категории: проприетарное (платное), бесплатное. Проприетарные продукты обычно отличаются наличием исчерпывающего набора встроенных инструментов. Такое программное обеспечение чаще используют профессиональные разработчики. Однако, стоит отметить, что подобные решения обычно работают лишь под управлением операционных систем семейства Windows и реже Mac.

В противоположность проприетарным продуктам выступает свободное программное обеспечение, распространяемое бесплатно и часто с открытым исходным ко-

дом, что позволяет провести их анализ на предмет наличия недекларируемых возможностей, а также использовать их под управлением широкого круга операционных систем. В табл. 1 представлены основные достоинства и недостатки наиболее распространенных редакторов [3, 4, 5].

Табл. 1. Достоинства и недостатки распространенных 3D редакторов

Программный продукт	Достоинства	Недостатки
Autodesk 3ds Max	1. Широкий набор встроенных инструментов и расширений для профессиональных разработчиков	1. поддерживаются только операционные системы семейства Windows 2. высокая стоимость
FreeCAD	1. Поддержка расширений с использованием Python API 2. Поддержка операционных систем семейства Linux, Mac, Windows 3. простота	
BRL-CAD	1. Поддержка операционных систем семейства Linux, Mac, BSD, Irix, Solaris, Windows	

Из таблицы видно, что для решения задачи построения трехмерной зоны радиоизлучений средств вычислительной техники целесообразно использовать редактор FreeCAD. Поддержка Python API позволяет расширять встроенную функциональность редактора и производить необходимые вычисления при решении задачи оптимизации благодаря популярному в научной среде модулю NumPy. Также немаловажным преимуществом данного программного продукта является поддержка открытых операционных систем семейства Linux и простота освоения, что, в свою очередь, существенно расширяет аудиторию пользователей.

Список литературы

1. *Кред Х.М.* Программный комплекс имитационного моделирования зон радиоизлучений средств вычислительной техники в защищаемых помещениях. Дис... канд. техн. наук. Минск, 2013.

2. *Утин Л.Л., Григорьев В.Л., Кред Х.М.* Усовершенствованная методика построения зоны излучения персональных электронных вычислительных машин // Доклады БГУИР. 2010. №7(53). С.53–58.

3. FreeCAD : an Open Source parametric 3D CAD modeler : features [Электронный ресурс] – Режим доступа : http://www.freecadweb.org/wiki/index.php?title=Feature_list.

4. BRL-CAD : Open Source Solid Modeling : documentation [Электронный ресурс] – Режим доступа : http://brlcad.org/wiki/Documentation.

5. Autodesk 3ds Max : 3D Modeling and rendering software : features [Электронный ресурс] – Режим доступа : http://www.autodesk.com/products/autodesk-3ds-max/features/all/gallery-view.

УДК 004.056

О НЕКОТОРЫХ МЕТОДАХ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВЫХ УЧРЕЖДЕНИЯХ

Л.В. МИХАЙЛОВСКАЯ, Е.В. ВАЛАХАНОВИЧ

Военная Академия Республики Беларусь,
пр-т Независимости, 220, г. Минск, 220057, Республика Беларусь
ludmila_mi@mail.ru

Применение методов оценки рисков информационной безопасности в финансовых учреждениях позволяет выполнить мероприятия по обеспечению защиты информации при условии минимизации затрат на их проведение.

Ключевые слова: информационная безопасность, оценка рисков, защита автоматизированных систем обработки информации.

В настоящее время информация – это один из самых ценных ресурсов. Жизненно важные интересы финансовых учреждений (ФУ), участвующих в процессе автоматизированной обработки и передачи информации, а также предоставления информационных услуг заключаются в том, чтобы определенная часть информации с одной стороны была бы легко доступна, с другой стороны – надежно защищена от неправомерного ее использования.

По этой причине проблема защиты автоматизированных систем обработки информации (АСОИ) в ФУ является достаточно актуальной. Это связано, во-первых, с тем, чтобы обеспечить режим защиты коммерческой тайны и персональных данных клиентов и служащих, во-вторых, чтобы затраты на выполнение данных мероприятий не превышали необходимого ресурса. В целях формирования стратегии по управлению рисками и планированию расходов на проведение мероприятий по защите информации необходимо проводить оценку рисков информационной безопасности.

Под риском в ФУ понимаются возможные потери вследствие воздействия угроз на основные активы (ресурсы): непосредственно информацию, инфраструктуру, персонал, имидж и репутацию. Количество информационных активов может быть очень велико. Поэтому первоочередной задачей управления рисками становится определение наиболее значимых активов и их ценности.

В ходе анализа ценности активов применяются следующие методы оценки риска: в денежном выражении, вероятностный и балльный, которые позволяют определить соответствующий уровень уязвимости для каждой комбинации информационного актива и угрозы ФУ и степень потенциальной опасности угроз.

Для оценки стоимости потерь в денежном выражении используется так называемая «аддитивная модель» [1] ценности информации, когда информация представляется в виде конечного множества элементов и осуществляется экспертная оценка компонент. Отдельные компоненты сравнивают по ценности относительно друг друга. Оценка возможных потерь (оценка риска) строится на основе полученных стоимостей компонент, исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

При использовании метода вероятностной оценки риска оценивается риск вероятности обхода системы защиты. С этой целью задается формальное описание структуры системы защиты и связности для множества элементов системы защиты и для множества элементов информационных угроз. Математическое описание связности построено на использовании теории графов и алгебраической топологии. Результаты анализа риска представляются как в качественной, так и в количественной формах.

Существует много предложений по оценке риска, основанных на балльном методе, например, в [2, 3]. В то же время, они не учитывают влияния уровней уязвимости системы при действии на нее определенной угрозы. При оценке рисков для ФУ целесообразно определенным категориям угроз присваивать различные значения баллов в зависимости от уровня воздействия угроз. Также присваивается соответствующий балл и уровням уязвимости системы при действии на нее определенной угрозы. Затем производится перемножение баллов воздействия на баллы уязвимости и по результату оценивается уровень риска для системы при воздействии на нее угрозы определенных категории и типа.

Задачами о принятии решений в условиях неопределенности (наиболее непредсказуемые элементы для систем защиты информации – люди: персонал, партнеры, клиенты) занимается теория игр. С помощью теории игр ФУ получает возможность предусмотреть ходы своих партнеров и конкурентов в соответствии с концепцией приемлемого риска. Особенностью такого подхода является использование качественных критериев и характеристик риска, включая оценку влияния на него лиц, принимающих решение (ЛПР). Причем учитывается влияние как ЛПР данного ФУ, так и ЛПР конкурентов. Между ЛПР в составе ФУ и у его конкурентов возникает ситуация игры с противоположными интересами, в рамках которой применяются как вполне законные действия, так и «на грани закона». Наиболее рациональным представляется расчет риска, связанного с однократными событиями, каждое из которых имеет свою вероятность появления и достаточно высокую «стоимость». Сложный инструментарий данной теории следует использовать только при принятии принципиально важных стратегических решений.

Применение приведенных методов по оценке рисков информационной безопасности для ФУ позволяет определить проблемные области обеспечения информационной безопасности и определить оптимальный комплекс мероприятий по защите информации. Если в процессе анализа будет выяснено, что меры по снижению риска малоэффективны и дороги одновременно, то может оказаться экономически более целесообразно застраховать свои действия. При этом будет ставится задача не предотвращения, а возмещения ущерба.

Список литературы

1. *Маслов О.Н.* // Inside. Защита информации. 2011. №4 (40). С. 16–22.

2. *Удалов Н.П.* Методика оценки риска инвестиционного проекта для различных уровней неопределенности проектной информации: Дис. … канд. экон. наук. Москва, 2007.

3. *Макоско А.В., Перемышленников Н.А.* // BIS Journal – Информационная безопасность банков. 2013. №1(8). С. 25–31.

УДК 681.5:004(07)

НАПРАВЛЕНИЕ ИНТЕЛЛЕКТУАЛЬНОСТИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. АПАНАСЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
mjdel@tut.by

В последнее время в области информационной безопасности начали активна развиваться интеллектуальные средства защиты информации. Такие как интеллектуальные агенты, искусственные нейронные сети, искусственные иммунные системы. Это обусловлено тем, что за последнее десятилетий прогрессивна, развиваются различные способы атак и вторжений в информационные системы, а с учетом их большое разнообразие невозможно оперативно и адекватно реагировать на эти атаки. Но интеллектуальные системы защиты информации могут изменить эту ситуацию.

Ключевые слова: интеллектуальные агенты, искусственные нейронные сети, искусственные иммунные системы, аномалии, атаки.

В последнее время большой проблемой стало увеличившееся количество вирусов, и хакерских атак на информационные ресурсы, банковские систему и т.д.

С каждым днем появляются новые виды атак на информационные ресурсы. В связи с этим возникает большая проблема: пока будет распознан данная атака, проанализирована, приняты адекватные меры по ее отражению, выпущены соответствующие обновления для ПО, проходит приличное количество времени, на протяжении которого информационные ресурсы не защищены и подвержены угрозам. По этому в сфере информационной безопасности нужно переходить к интеллектуальным средствам защиты информации.

Под интеллектуальными средствами защиты информации понимают такие средства, которые на основе своего опыта или имеющихся знаний, могут самостоятельно принять решение является ли данная ситуация аномальной или нет.

К ним относятся интеллектуальные агенты, нейронные сети, искусственные иммунные системы и др. Одни из них применятся на этапе обнаружения угрозы, другие на этапах анализа и нейтрализации угрозы. Поэтому эти средства нужно применять комплексно.

В отличие от статических средств защиты интеллектуальные, способны принимать самостоятельно решение, есть ли сейчас угроза, и если она есть находить тут же адекватные меры.

Любой интеллектуальный агент представляет собой открытую систему, помещенную в некоторую среду, причем эта система обладает собственным поведением, удовлетворяющим некоторым экстремальным принципам. Таким образом, интеллектуальный агент считается способным воспринимать информацию из внешней среды с ограниченным разрешением, обрабатывать ее на основе собственных ресурсов, взаимодействовать с другими агентами и действовать на среду в течение некоторого времени, преследуя свои собственные цели. Другими словами интеллектуальных агентов можно представить как сеть, в которой каждый агент отвечает за свою «территорию», при это при обнаружении аномалии, сообщает о ней другим агентам сети. Что позволяет оперативно и адекватно реагировать всей системе на атаки злоумышленников или вирусов.

Нейронные сети – класс аналитических методов, построенных на (гипотетических) принципах обучения мыслящих существ и функционирования мозга и позволяющих прогнозировать значения некоторых переменных в новых наблюдениях по данным других наблюдений (для этих же или других переменных) после прохождения этапа, так называемого обучения на имеющихся данных.

Основные преимущества и достоинства нейронных сетей перед традиционными вычислительными системами.

1. Решение задач при неизвестных закономерностях
2. Устойчивость к шумам во входных данных
3. Адаптированные к изменениям окружающей среды
4. Потенциальное сверхвысокое быстродействие
5. Отказоустойчивость при аппаратной реализации нейронной сети

Основным недостатком нейронных сетей является узкий диапазон применения, она может, эффективна, работать только после прохождения обучения нахождения определённого класса атак. Нейронные сити лучше всего использовать на этапах обнаружения, квалификации аномалий и нахождения способов ее нейтрализации.

Искусственная иммунная система (ИИС) – это адаптивная вычислительная система, использующая модели, принципы, механизмы и функции, описанные в теоретической иммунологии, которые применяются для решения прикладных задач.

Иммунная система представляет большой интерес как система, способная эффективно обрабатывать значительные объемы данных. В частности, она выполняет большой объем сложных высокопараллельных распределенных вычислений. Поведение иммунной системы в целом определяется всей совокупностью локальных взаимодействий.

Основные достоинства ИИС:

1. Наличие большого числа детекторов приводит к отказоустойчивости и надежности системы. Отсутствие единой точки отказа.
2. При увеличении количества узлов среды распределенных вычислений в предложенной системе повышается уровень защищенности.
3. Все столкновения детекторов с вредоносными объектами заносятся в память. Это позволяет проводить обучение детекторов.

Основные недостатки:

1. Возможна аутоиммунная реакция.
2. Возможен иммунодефицит, особенно при малом количестве узлов среды распределенных вычислений.

ИИС эффективна, использовать на этапе обнаружения и выявления аномалий и атак злоумышленников. Таким образом, можно сделать вывод, что в современном мире нужно создавать глубоко эшелонирование, интеллектуальные системы защиты информации, которые смогут адекватна реагировать и защищать информационные ресурсы от несанкционированного доступа, атак злоумышленников, а так же вредоносного ПО и вирусов.

Список литературы

1. *Васильев В.И.* Интеллектуальные системы защиты информации. «Машиностроение». М., 2013.

2 Гвозденко А. Искусственные иммунные системы как средства сетевой самозащиты [Электронный ресурс]. – Режим доступа: http://itc.ua/node/4270/

3. *Рутковский Л.* Методы и технологии искусственного интеллекта: пер. с польск. – М.: Горячая Линя-Телеком, 2010.

УДК 621:658.382

ОРГАНИЗАЦИЯ ПЛАНИРОВАНИЯ СПОСОБОВ ЗАЩИТЫ ОРГАНИЗМА ЧЕЛОВЕКА ОТ УЛЬТРАФИОЛЕТОВОГО ИЗЛУЧЕНИЯ

Т.М. ПЕЧЕНЬ, УКАТУ АРИНЗЕЧУКВУ ЧУКВУНОНСО

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
tanya.7p@gmail.com

Создание безопасных условий труда всегда является приоритетным направлением, т.к. от этого зависит здоровье каждого работника. В настоящее время хорошо развита автоматизация технологических процессов, однако есть такие процессы, в которых нельзя исключить участие человека. Работа с источниками ультрафиолетового излучения относится к данным технологическим процессам.

Ключевые слова: ультрафиолетовое излучение, интенсивность, длина волны, защитные средства.

Ультрафиолетовое излучение (УФИ) – это электромагнитные волны оптического диапазона с длинами волн от 200 нм до 400 нм. Международная Комиссия по Освещению (МКО) в 1963 году предложила разделить УФИ на три области со следующими границами между ними: УФ-А длинноволновое (ближнее) излучение с длинной волны от 315 до 400 нм; УФ-В средневолновое (эритемное) излучение с длинной волны от 280 до 315 нм; УФ-С коротковолновое (бактерицидное) излучение с длинной волны от 200 до 280 нм.

Известно, что это излучение оказывает на организм человека в зависимости от интенсивности и продолжительности, как положительное воздействие, так и отрицательное. Ультрафиолетовые лучи являются важным стимулятором основных биологических процессов, в том числе процесс синтеза некоторых биологически активных веществ.

Основными способами защиты организма человека от воздействия УФИ являются следующие:

1) защита «расстоянием» – это способ, при котором обслуживающий персонал удален на безопасное расстояние от источников УФИ, причем величина которого определяется только экспериментальным путем в каждом конкретном случае в зависимости от условий работы, состава производственной атмосферы, вида источника излучения, отражающих свойств конструкций помещения и оборудования и т.д. [1].

2) экранирование источников излучения – один из наиболее рациональных методов защиты, в качестве материалов для изготовления экранов могут применяться различные материалы и светофильтры, не пропускающие или снижающие интенсивность излучений;

3) экранирование рабочих мест – это способ, при котором рабочие места ограждают ширмами, щитками или изготавливаются специальные кабины;

4) применение средств индивидуальной защиты, к которым принято относить спецодежду (куртки, брюки и т.п.), рукавицы, фартуки из специальных тканей, щитки со светофильтром;

5) использование специальной окраски помещений – это способ заключается в окрашивании помещений светлыми тонами (серый, желтый, голубой) красок, в которые, как правило, добавляют оксид цинка или титана;

6) рациональное размещение рабочих мест, что позволяет организационным способом снизить интенсивность УФИ.

Важное гигиеническое значение имеет способность УФИ производственных источников изменять газовый состав атмосферного воздуха вследствие его ионизации. При этом в воздухе образуются озон и оксиды азота. Эти газы, как известно, обладают высокой токсичностью и могут представлять большую опасность, особенно при выполнении сварочных работ, сопровождающихся УФИ, в ограниченных, плохо проветриваемых помещениях или в замкнутых пространствах.

С целью профилактики отравлений окислами азота и озоном соответствующие помещения должны быть оборудованы местной или общеобменной вентиляцией, а при сварочных работах в замкнутых объемах необходимо подавать свежий воздух непосредственно под щиток или шлем.

Интенсивность УФИ на промышленных предприятиях установлена «Санитарными нормами ультрафиолетового излучения в производственных помещениях» № 2.2.4.13-45–2005. Допустимая интенсивность облучения работников при наличии незащищенных участков поверхности кожи не более 0,2 м^2, периода облучения до 5 минут, длительности пауз между ними не менее 30 минут и общей продолжительности воздействия за смену до 60 минут не должна превышать 50,0 Вт/м^2 – для области УФ-А; 0,05 Вт/м^2 – для области УФ-В; 0,001 Вт/м^2 – для области УФ-С. Допустимая интенсивность ультрафиолетового облучения работающих при наличии незащищенных участков поверхности кожи не более 0,2 м^2 (лицо, шея, кисти рук и др.), общей продолжительности воздействия излучения 50 % рабочей смены и длительности однократного облучения свыше 5 минут и более не должно превышать 10,0 Вт/м^2 – для области УФ-А; 0,01 Вт/м^2 – для области УФ-В. Излучение в области УФ-С при указанной продолжительности не допускается [2].

Защитная одежда из поплина или других тканей должна иметь длинные рукава и капюшон. Глаза защищают специальными очками со стеклами, содержащими оксид свинца, но даже обычные стекла не пропускают УФ-лучи с длиной волны короче 315 нм. При проведении электросварочных работ необходимо использовать защитную одежду из материалов, не пропускающих УФИ, к ним относятся спилк, кожа, ткани с пленочным покрытием. Известно, что суммарно допустимая интенсивность излучения в областях УФ-В и УФ-С не должна превышать 1,0 Вт/м^2.

Таким образом, при организации планирования способов защиты организма человека от УФИ необходимо учитывать следующие основные факторы:

– тип источника УФИ,
– время работы (продолжительность),
– интенсивность излучения,
– особенности проведения работ,
– применение средств коллективной и индивидуальной защиты.

Нельзя пренебрегать при планировании каким-либо фактором, т.к. это может негативно отразится на здоровье работников. Профессиональное воздействие повышенных уровней УФИ может быть причиной ряда заболеваний органов зрения и кожных покровов, ослабления иммунной системы.

Список литературы

1. *Михнюк Т. Ф.* Охрана труда и основы экологии : учебник для студентов ВУЗ. Минск : Высшая школа, 2007.

2. Санитарные нормы ультрафиолетового излучения производственных источников: СН 2.2.4-13-45-2005: утв. 16.12.2005 г. – Минск, 2005.

УДК 004.056.5

AN ADAPTIVE STEGANOGRAPHY BASED ON PARTITIONING APPROACH

S.A. SEYYEDI, N.N. IVANOV

Belarusian State University of Informatics and Radioelectronics
6, P. Brovki Str., Minsk, 220013, Republic of Belarus
amseyyedi@gmail.com, ivanovnn@bsuir.by

Steganography is a branch of information hiding. A tradeoff between the hiding payload and quality of digital image steganographic schemes is major challenge of steganographic methods. This article presents high payload and imperceptible steganography technique based on integer wavelet transform. The cover image is partitioned into 8×8 non overlapping blocks, then each transformed block divided into two subsets and secret message is embedded into the proper one. Experimental results indicate low degrading the quality of stego image by hidden high volume of secret message.

Keywords: Steganography, Integer Wavelet Transform, Embeddable Subset, Rounding Method and LSB.

Nowadays the digital communication channels and Internet play important role in data transmission and sharing, hence there is a great need for security of information to prevent unauthorized access. Steganography is technique of hiding confidential data in any form of media in such a way that no one, except the intended recipient knows the existence of secret data [1]. The main difference between steganography and cryptography is the suspicion factor. The digital images, videos, audios and other digital files can be used as a carrier to embed the information. The important requirements of such steganographic method are payload, security and fidelity. Payload refers to the amount of information that can be hidden in the cover image. Security refers to impossibility of successful attack to detect hidden information. Fidelity (imperceptibility) refers to inability of human eyes to distinguish between cover image and stego-image. Increasing payload rate is in conflict with fidelity and security. The major goal of steganographic techniques is to enhance communication security by increasing embedding rate [2].

An adaptive steganography technique based on integer wavelet transform (IWT) for hiding a large volume of data is proposed. The cover image is partitioned into 8×8 non overlapping blocks and 2D IWT applied to each block. The coefficients in each block divided into embeddable (E) and unused (U) subsets. The subset partition is based on local threshold (T2) where:

$$T_0 = 2^{\lfloor \log_2 \max(temp) \rfloor} \tag{1}$$

$$T_1 = \frac{T_0}{2}, \tag{2}$$

max (temp) denotes as maximum value of coefficients in a block.

The embeddable subset E for each block is undergone for embedding a secret message. The data hiding length (L) is computed based on absolute value of coefficient in E with the aid of following decision factor:

$$L = \begin{cases} 1 & \text{if } E_i = 0,1 \\ \lfloor \log_2 E_i \rfloor & \text{otherwise} \end{cases} \tag{3}$$

The embedding method is determined based on L value. If L=1 then use LSB to embed secret message bits else use rounding method. Rounding method is one a way for embedding secret message bits in cover image. The pixel value is modifying into the nearest integer with the last LSB bits equal to the input bits. The mathematical representation of rounding method is [3]:

$$y = x + A \times (A \le B) - B \times (B < A), \tag{4}$$

$$A = \mathrm{mod}(m - x, 2^c), \tag{5}$$

$$B = \mathrm{mod}(x - m, 2^c), \tag{6}$$

Where y, x, m, and c denote the output value, input value, secret message and capacity respectively.

In order to evaluate the performance of the proposed steganographic method, experimental results simulated using Matlab platform. Various experiments are carried out to access the performance of proposed method in the terms of Payload and fidelity (by measuring several quality metrics peak signal to noise ratio, mean square error and cross correlation). The secret message is generated randomly and four well know 512×512 gray scale image «Lena», «Baboon», «peppers», «Jet» used as cover image. Tab. 1 is shown the results in term of payload and imperceptibility.

Tab. 1. Comparison of maximum payload and fidelity metrics

Image	***Max Payload (bit)***	***Metrics***	***Length of embedding message(Byte)***		
			20000	**30000**	**50000**
Lena	***406040***	**PNSR**	43.35	41.29	39.96
		MSE	3.006	4.835	6.568
		CC	0.9993	0.9990	0.9986
Baboon	***616365***	**PNSR**	39.21	37.8964	36.978
		MSE	7.805	10.554	13.0381
		CC	0.9978	0.9971	0.9964
Peppers	***418187***	**PNSR**	42.77	41.16	40.18
		MSE	3.436	4.979	6.238
		CC	0.9994	0.9992	0.9990
Jet	***386830***	**PNSR**	43.54	40.52	N/A
		MSE	2.877	5.763	N/A
		CC	0.9993	0.9986	N/A

An adaptive and secure steganography scheme has been proposed. Proposed method has integrated blocking approach, wavelet transform, rounding method and LSB into steganography scheme. The main advantage of proposed method is high hiding payload with acceptable level of perceptual quality of stego-image. Also there are several parameters which have an impact in aspect of proposed method such as level of decomposition, level of thresholds. This parameters lead to change the number of elements in subset E. With increasing the elements of E, payload increased. The sender must make the best tradeoff between requirements.

References

1. *Cheddad A., Condell J., Curran K. and Kevitt P.M.* // Digital Signal Processing. 2010. No.3 (90), pp.727-752.

2. *Chandramouli R. and Memon N.D.* // SPIE Security Watermarking Multimedia Contents. 2003. Vol.5020, pp.173–177.

3. *Sarreshtedari S., Ghobi M. and Ghaemmeghami S.* // the 7th annual IEEE consumer communications and networking conference. USA, January 9-12 2010. pp.1-5.

УДК 331.103.244

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ГРУППОВОЙ ОПЕРАТОРСКОЙ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИЕРАРХИЧЕСКИХ СИСТЕМАХ УПРАВЛЕНИЯ

Н.В. ПУШКАРЕВА, В.А. ГУЩО

Военная академия Республики Беларусь
пр-т Независимости, 220, г. Минск, 220057, Республика Беларусь
n.guscho@gmail.com

Защищать компоненты автоматизированных систем необходимо от всех видов воздействий: стихийных бедствий и аварий, ошибок персонала и пользователей и т.п. Имеется широчайший спектр вариантов преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена. Правильно построенная модель групповой операторской деятельности, в которой отражаются индивидуально-личностные характеристики операторов, их практические и теоретические возможности – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Ключевые слова: групповая деятельность операторов, индивидуально-личностные характеристики операторов, регрессионная модель, математическая теория эксперимента.

Для проведения математического моделирования необходимо изучить связь между эффективностью совместной деятельности малой группы операторов и некоторой совокупностью индивидуально-личностных характеристик партнеров. Поскольку какой-либо априорной (начальной, реальной) информации по сути поставленной задачи у исследователя нет, то объект исследования - малую группу – представим моделью «черного ящика» (рис. 1). Это означает практически полное отсутствие знаний о возникающих внутригрупповых процессах и характере основных механизмов взаимодействия операторов. Затем необходимо организовать наблюдение за поведением показателей эффективности групповой деятельности при различных значениях индивидуально-личностных характеристик операторов, влияющих на защиту информации. Для этого необходимо, во-первых, определить ограниченный набор совокупности значимых индивидуально-личностных характеристик операторов $X=\{x_i\}$; во-вторых, «заморозить» условия, в которых осуществляются наблюдения $Z=\{z_i\}$; в-третьих, показатель эффективности групповой операторской деятельности Y должен быть количественно измеримым; в-четвертых, нельзя исключать случайные воздействия ε.

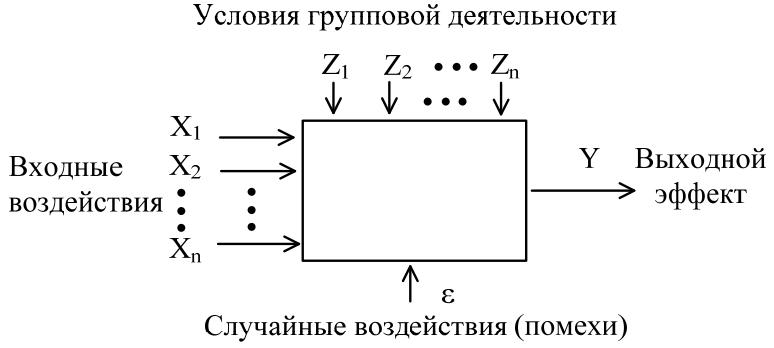


Рис. 1. Модель исследования – «черный ящик»

Изменение входных воздействий можно производить по-разному. Во-первых, поочередно изменять каждое из входных воздействий x_i, «заморозив» остальные на каких-то уровнях; во-вторых, все входные воздействия задавать по случайному закону; в-третьих, изменять одновременно все входные воздействия по какой-то программе [1].

Первый вариант организации наблюдений связан с большим количеством наблюдений и с потерей больших объемов полезной информации, которая заключена в эффектах совместного влияния входных воздействий на выход. Она теряется, так как реакция объекта изучается по изменению каждого в отдельности входного воздействия.

Второй вариант подразумевает фиксацию в какой-то момент времени значений отдельных параметров одновременно для всех входных воздействий x_i и сопоставлении их со значениями выходного эффекта Y [2]. По этим данным строится так называемая регрессионная модель вида

$$y = b_0 + \sum_{i=1}^{n} b_i \cdot x_i + \sum_{\substack{i=1 \\ j=1}}^{n} b_{ij} \cdot x_i \cdot x_j + ..., \qquad (1)$$

где b_i, b_{ij} - коэффициенты регрессии (i = 1, 2, …, n; j=1,2,…n), определяемые с помощью аппарата классического регрессионного анализа.

Эта схема организации наблюдений и соответствующий ей способ обработки результатов однако, не обеспечивают коэффициентам регрессии весовых свойств. Величина коэффициента не свидетельствует о степени влияния на выходной эффект Y того входного воздействия x_i, перед которым он стоит в модели, а знак – о направлении влияния, что резко ограничивает круг задач, решаемых с помощью модели. Ее можно использовать только для решения задач параметрического прогноза, и то лишь в пределах области изменений параметров входных воздействий x_i, т.е. задачи интерполяции [3].

Третий вариант предполагает активное участие исследователя на всех стадиях моделирования, его целенаправленное проведение с хорошо развитой функцией управления всеми наблюдаемыми процессами [4]. Этим требованиям отвечает математическая теория эксперимента или теория планирования эксперимента. Она предлагает большое число вариантов выбора логики одновременного варьирования параметров входных воздействий. Все они не универсальны и не взаимозаменяемы. Результаты наблюдений представляются в виде регрессионной модели (1). Объективность полученной математической модели проверяется путем оценки достоверности как промежуточных, так и конечных результатов. Анализ математической модели основывается на весовых свойствах ее коэффициентов.

Список литературы

1. *Козубовский В.М.* К вопросу о применении математической теории экстремального эксперимента к синтезу оптимальных эргатических систем. Минск: ВИРТУ, 1968.

2. *Козубовский В.М.* Групповая готовность операторов к сложным видам совместной деятельности. Автореф. дис. доктора психологических наук. Киев, 1990.

3. *Пустыльник Е.И.* Статистические методы анализа и обработки наблюдений.- М.: Наука, 1968.

4. Угрозы информационной безопасности в АС. [Электронный ресурс]. – Режим доступа: http://asher.ru/security/book/its/05. Дата доступа: 21.01.2014.

УДК 004.056.55

МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В АУДИОФАЙЛАХ ФОРМАТА MIDI И WAV

В.В. МИРОНЧИК, Е.С. ШЕЛЕСТ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
Violet-88@tut.by

Передача скрытой информации в аудиофайлах является актуальной в контексте защиты авторских прав от несанкционированного использования мультимедийной продукции. Рассмотрены методы скрытой передачи информации в аудиофайлах формата MIDI и WAV.

Ключевые слова: формат MIDI, формат WAV, аудиофайлы, скрытие информации.

В современном мире человек постоянно находится в окружении различных звуков. Развитие и распространение сетевых методов общения привело к появлению новых методов передачи скрытой информации в аудиофайлах. Эффективным решением для передачи скрытой информации в аудиофайлах является объединение методов компьютерной стеганографии и криптографии [1]. При использовании криптографии информация модифицируется по определенному алгоритму, в результате преобразований скрывается смысл сообщения. Стеганография скрывает сам факт передачи или хранения информации путем внедрения ее в различные мультимедийные объекты, которые не теряют от этого своих потребительских свойств. Не смотря на большое разнообразие форматов аудиофайлов, одними из наиболее распространенными являются MIDI и WAV.

Формат MIDI является распространенным форматом хранения и передачи музыки, который используют композиторы, музыканты и обычные пользователи ЭВМ. Известен метод внедрения информации в MIDI-файлы путем использования разности времени между записанными в файл событиями, которые не изменяют характеристики (настройки) устройства воспроизведения [2]. Это происходит, например, когда подряд следуют несколько одинаковых управляющих событий. Суть данного метода заключается в кодировке скрытого сообщения временем между изменением уровня громкости аудиосигнала. Недостатком в данном случае является отсутствие секретного ключа, который предотвращал бы возможность чтения внедренной информации любым пользователем.

Существует также метод внедрения скрытой информации в MIDI-фа йлы с помощью кодирования информации двоичным кодом, а двоичный код, в свою очередь управляет громкостью звучания нот, следующих друг за другом. В данном случае используется следующий алгоритм: если скрывается логическая единица, то значение громкости должно быть нечетным числом, а если скрывается логический нуль – четным. Обнаружить сделанное вложение на слух невозможно, так как, во-первых, изменения громкости незначительны, а во-вторых, изменение громкости на одну единицу невозможно зарегистрировать на слух, однако можно использовать для скрытой передачи информации. Кроме того, запись секретной информации может быть осуществлена в партию лишь одного инструмента (например, контрабаса), что при звучании целого оркестра (или ансамбля) еще больше акустически маскирует скрытое сообщение [3].

Таким образом, формат MIDI может быть успешно использован для передачи или хранения конфиденциальной информации. При этом для сокрытия информации следует использовать большое число различных событий, которые управляют процессом воспроизведения музыкальной композиции.

Файл формата WAV содержит в себе квантованные цифровые значения амплитуды сигнала, измеренные в дискретные моменты времени (так называемые отсчеты). Для файла формата WAV наиболее известным и распространенным методом сокрытия секретной информации является метод замены наименьшего значащего бита (НЗБ) [4].

При внедрении информации в звуковые файлы формата WAV методом НЗБ приходится решать задачу выбора номера разряда отсчета, в который можно поместить скрываемую информацию, с учетом двух конфликтующих требований. С одной стороны, необходимо увеличивать объем скрываемой информации в одном файле (увеличивать пропускную способность канала), а с другой стороны, нужно обеспечить высокую степень скрытности вложенной информации. На данный момент разработано программное обеспечение, позволяющее решать поставленные задачи.

Программа Crypto предназначена для скрытой передачи информации в аудиофайлах, с использованием принципов стеганографии. Для повышения скрытности внедренной информации в программе использован модифицированный метод замены наименьшего значащего бита. Информация разделяется на фрагменты и распределяется по нескольким звуковым файлам. Ключом для извлечения сообщения служит последовательность файлов, в которых были скрыты фрагменты сообщения.

Программа WaveCrypto позволяет внедрять информацию в один звуковой файл с использованием ключа, распределяющего внедряемую информацию по всему контейнеру. Ключ распределения генерируется в зависимости от размера файла и требующегося соотношения между наполняемостью и скрытностью. Если в контейнере содержится «полная тишина» (отсчеты с малой амплитудой), то программа пропускает их, внедряя информацию на других участках фонограммы. Программы Crypto и WaveCrypto создают несколько уровней защиты информации: шифруют открытый текст одним из криптографических методов, внедряют зашифрованный текст в звуковые файлы, распыляя скрываемые биты не только внутри одного файла, но и среди нескольких звуковых файлов [5].

Передача скрытой информации в аудиофайлах позволяет решить проблему защиты авторских прав на мультимедийную продукцию. Но в тоже время, скрытая информация в аудиоформате может оказать негативное влияние на психоэмоциональное состояние человека, так как различные звуки могут воздействовать на мысли и эмоции людей. При прослушивании аудиофайла, содержащего в себе скрытую информацию в виде формулы внушения, человек может на подсознательном уровне подвергаться воздействию. Обнаружение скрытой передачи информации с целью защиты человека от негативного воздействия на его подсознание является на данный момент актуальной задачей.

Список литературы

1. *Андрианова О.С., Губенко Н.Е.* // Моделирование и компьютерная графика. Материалы третьей международной научно-технической конференции Донецк 7 – 9 октября 2009 г. С.389 – 392.

2. *Walter J.M.* Method and apparatus for encoding security information in a MIDI datastream United States Patent US 6798885 B1 Sep. 28, 2004.

3. *Алексеев А.П., Аленин А.А.* Методы внедрения информации в звуковые файлы формата MIDI // Инфокоммуникационные технологии. 2011. Т. 9. № 1. С. 84 – 89.

4. *Алексеев А.П., Орлов В.В.* Стеганографические и криптографические методы защиты информации: учебное пособие. Самара: ИУНЛ ПГУТИ, 2010.

5. *Аленин А.А., Алексеев А.П.* Исследование методов обнаружения вложений в звуковых файлах формата WAV // Безопасность информационных технологий. 2011. Т. 9. №1. С. 51 – 56.

УДК 004.059

ЗАЩИТА ЗААРХИВИРОВАННОЙ ИНФОРМАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ ИНДИВИДУАЛЬНОСТИ

Т.Г. ТАБОЛИЧ[1], Г.В. СЕЧКО[2], А.А. ГИВОЙНО[3]

[1]Высший государственный колледж связи
ул. Ф. Скорины, 8/2, г. Минск, 220014, Республика Беларусь
tabolichtatiana@mail.ru

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
georg.sechko@gmail.com

[3]ОАО «Белэнергоремналадка»
ул. Академическая, 18, г. Минск, 220024, Республика Беларусь
givojno@gmail.com

Статья посвящена разработке уникального программного продукта, сочетающего в себе функции программы-архиватора и идентификации личности пользования по биометрическим характеристикам. Определен метод биометрической идентификации и показан общий алгоритм идентификации личности пользователя по радужной оболочке глаза.

Ключевые слова: программа-архиватор, идентификация личности пользователя, программное средство, идентификация по радужной оболочке глаза.

Согласно исследованиям, опубликованным в журнале «Science», глобальный потенциал телекоммуникационных возможностей на душу населения удваивается каждые 34 месяца; количество внесённой информации в мире на душу населения удваивается каждые 40 месяцев (то есть каждые три года), а трансляция информации на душу населения имеет тенденцию удвоения примерно каждые 12,3 года [1].

Популярной формой передачи и хранения данных стали архивы. Достоинством заархивированной информации в компьютере является общеизвестное её свойство устойчивости к целому ряду компьютерных вирусов, в частности, к руткитам EXPLOIT и BACKDOOR [2], Autorun-вирусам и ряду других (полная информация об этих и аналогичных по своему действию вирусах приведена на сайте SECURELIST.COM).

Несанкционированный доступ к секретным заархивированным файлам может привести к огромному ущербу, поэтому при выборе надёжных методов защиты от несанкционированного доступа целесообразно сравнить по надёжности и стоимости все возможные варианты обеспечения информационной безопасности. Поэтому в настоящей статье рассматривается проблема создания программы-архиватора, которая распознаёт пользователя с помощью его уникальной биометрики.

Традиционные системы идентификации пользователя требуют знания пароля, наличия ключа, идентификационной карточки, либо иного идентифицирующего предмета, который можно забыть или потерять. Биометрический контроль доступа – автоматизированный метод, с помощью которого путем проверки (исследования) уникальных физиологических особенностей или поведенческих характеристик человека осуществляется идентификация личности. Физиологические особенности, например, такие как папиллярный узор пальца, геометрия ладони или рисунок радужной оболочки глаза (РОГ), являются постоянными физическими характеристиками человека. Основным преимуществом биометрической характеристики от персонального идентификационно-

го номера (ПИН), является неизменность первоначальной информации и постоянное ее наличие у идентифицируемой личности [1].

Проведенный сравнительный анализ использования различных биометрических методов идентификации пользователя при создании программы-архиватора позволил остановиться на методах идентификации пользователя по РОГ. Преимущество методов идентификации по РОГ состоит в том, что образец отличительного рисунка радужной оболочки находится на поверхности глаза. Видеоизображение глаза может быть отсканировано на расстоянии метра, что делает возможным использование сканеров для радужной оболочки в банкоматах и других объектах.

Еще одно преимущество связано с физиологическими особенностями человеческого глаза: сетчатка глаза человека может меняться со временем, в то время как радужная оболочка глаза остается неизменной; невозможно найти два абсолютно идентичных рисунка радужной оболочки глаза; очки и контактные линзы, даже цветные, не воздействуют на качество аутентификации [3].

Для реализации процесса распознавания личности требуется выделить изображение радужки человеческого глаза и отделить его от шума – ресниц, век. Методы идентификации и верификации личности по радужной оболочке построены по принципу выделения частотных или статических характеристик по текстуре и рисунку кровеносных сосудов и радужки глаза из изображения и сохранения этой информации в виде шаблона [4].

На данный момент задача разработки программного продукта, совмещающего в себе функции программы-архиватора с идентификацией пользователя по представленной схеме, реализована в полном объеме и апробирована на ряде предприятий энергетической отрасли для передачи технико-экономических показателей теплоэлектроцентралей в Республике Беларусь. Ведется работа по регистрации и модернизации программного продукта.

Список литературы

1. *Hilbert M, López P*. The World’s Technological Capacity to Store, Communicate, and Compute Information // Science. – 2011, № 332 (6025). – P. 60-65.

2. Popular Science Magazine. – February 1950. – P. 96.[Электронный ресурс]. Режим доступа: http://www.prweb.com/releases/2007/04/prweb516626.htm. Дата доступа: 22.12.2013.

3. *Гивойно А.А., Николаенко В.Л., Сечко Г.В, Таболич Т.Г*. Программное средство для защиты информации с помощью архивирования // Материалы 16-й МНТК «Современные средства связи» 27–29 сентября 2011 года, Минск, Респ. Беларусь / редкол.: А.О.Зеневич и [др.] – Мн.: УО ВГКС, 2011. – 182 с – С. 90.

4. Security News: Информационно-аналитическое издание по техническим средствам и системам безопасности. [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.secnews.ru. – Дата доступа: 30.12.2013.

УДК 004.42

КРОССПЛАТФОРМЕННОЕ ПРОГРАММНОЕ СРЕДСТВО С ОТКРЫТЫМ КОДОМ ДЛЯ РАБОТЫ С ПРОТОКОЛОМ SSH

И.А. КОРНЕЕВ[1], Е.В. НИКОЛАЕНКО[2], Т.Г. ТАБОЛИЧ[3]

[1]СООО Интетикс Бел
ул. Тимирязева, 9, г. Минск, 220004, Республика Беларусь
korneev.box@gmail.com

[2]Белорусский государственный университет информатики и радиоэлектроники
Институт информационных технологий
ул. Козлова, 28, г. Минск, 220013, Республика Беларусь
e.nikolaenko@butb.by

[3]Высший государственный колледж связи
ул. Ф. Скорины, 8/2, г. Минск, 220114, Республика Беларусь
tabolichtatiana@mail.ru

Рассматривается новое кроссплатформенное бесплатное программное средство для работы с протоколом SSH, свободное от ряда недостатков существующих аналогов. Программный код этого средства будет опубликован на хостинге с использованием GPL лицензии, вследствие чего получит свободное распространение.

Ключевые слова: информационная безопасность, кроссплатформенное бесплатное программное средство, мультиплатформенность, сервер, протокол SSH.

Популярность организации аппаратной части сетевого оборудования в виде серверов – устройств, выделенных и/или специализированных для выполнения с их помощью сервисного программного обеспечения, ни у кого не вызывает сомнений. Сервера служат для большого диапазона задач начиная от маршрутизации-фильтрации данных, заканчивая хранением активных приложений. В большинстве случаев физически сервер находится удаленно, и совершать над ним какие либо манипуляции крайне проблематично. Поэтому в большинстве серверов для решения данной проблемы используется протокол SSH (Secure SHell), который является протоколом для удаленного безопасного входа и других сетевых сервисов безопасности в недостаточно надежно защищенной сети.

Программные средства SSH представляют собой огромный набор вариантов реализации протокола (OpenSSH, WinSSHD и другие), малая часть которых распространяется бесплатно, а остальные – за деньги. На наш взгляд, недостатками платных вариантов являются:

– слабо развитый интерфейс;

– закрытость программного кода и высокая стоимость;

– платформоориентированность (под этим термином будем понимать возможность работы сервиса только в определённой операционной системе и невозможность работы в других системах;

– выполнение скриптов пользователя в назначенное время;

– отсутствие возможности автономной работы (без участия пользователя).

В докладе рассматривается новое кроссплатформенное бесплатное программное средство для работы с протоколом SSH, свободное от указанных недостатков. Программный код этого средства будет опубликован на хостинге с использованием GPL

лицензии, вследствие чего получит свободное распространение. Средство поддерживает следующие функции:

- возможность передачи команд удаленной системе;
- возможность хранения истории ввода команд;
- совместимость с протоколом SSH версии 2.0;
- использование шифрования (для SSH2-клиент) с помощью алгоритмов: 3DES, Blowfish, CAST128, ARCFOUR, AES128, AES192, AES256-CBC;
- использование пароля при идентификации;
- идентификация по протоколу RSA;
- поддержка сжатия данных;
- авторизация при помощи открытого ключа;
- свободный доступ к коду программы;
- возможность работы приложения на большинстве операционных систем (мультиплатформенность);
- возможность выполнения набора команд из файла (файл-скриптов);
- возможность запуска файла скриптов по расписанию;
- возможность осуществлять CRUD-манипуляции над файлами из контекстного и основного меню программы;
- осуществление функций навигации по локальной файловой системе;
- осуществление функций навигации по удаленной файловой системе;
- чтение и сохранение настроек программы;
- поддержка несколько языков интерфейса;
- защита программы от сбоев при работе с удаленным севером;
- обработка ошибки при работе с удаленным севером;
- возможность восстановления сеанса после сбоя;
- возможность работы с файлами при помощи технологии Drag&Drop;
- возможность работы с «горячими клавишами»;
- поддержка кодировки Unicode.

Для успешного запуска программы необходимо наличие в системе JVM (java virtual machine версия 7 обновление 44), графического адаптера и монитора. Входной информацией программы являются файлы или папки, которые пользователь может отправлять на файловую систему стороннего сервера при помощи главного меню или технологии Drag& Drop либо передавать команды операционной системе посредством командной строки или использовать файлы скриптов, для запуска их на сторонней системе. Выходной информацией является текстовый ответ удаленной системы на команды и скрипты пользователя, а также файлы, перенесенные в локальную систему из удаленной.

В качестве инструментов разработки были выбраны самые передовые и перспективные инструменты и технологии. Ими являются:

- язык программирования - java;
- язык разметки - YAML;
- Apache maven - фреймворк для автоматизации сборки проектов;
- распределенная система контроля версий - git;
- GitHub - самый крупный веб-сервис для хостинга IT-проектов;
- среда разработки – IntelliJ IDEA.

Программа оттестирована и полностью пригодна к использованию.

УДК 004.056.5:654.924.3

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В АВТОСИГНАЛИЗАЦИИ МОБИЛЬНЫХ ОБЪЕКТОВ

С.С. ДУБИНА[1], К.С. КОЗЛОВ[2], Г.В. СЕЧКО[3], А.М. ЧЕРНЕЦКИЙ[4]

[1]ОАО Жабинковский сахарный завод
г. Жабинка, Брестская обл., 225100, Республика Беларусь
dkvants@gmail.com

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kozlov_kirill1987@mail.ru

[3]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
georg.sechko@gmail.com

[4]ОАО Жабинковский сахарный завод
г. Жабинка, Брестская обл., 225100, Республика Беларусь
holod87.87@gmail.com

Для борьбы с автоугоном с помощью кодграббера предлагается противоугонное устройство, повышающее помехоустойчивость принимаемого радиосигнала, который передаётся от устройства дистанционного управления к блоку управления автосигнализацией. Противоугонное устройство состоит из аппаратной части на базе микроконтроллера ATtiny84 фирмы Atmel и программной части (программного обеспечения микроконтроллера).

Ключевые слова: автосигнализация мобильных объектов, автоугон, кодграббер, протокол передачи данных Keeloq, противоугонное устройство.

В современных автосигнализациях бюджетного класса коды постановки и снятия с охраны постоянно изменяются после каждого нажатия на кнопку устройства дистанционного управления автосигнализацией мобильных объектов (обычно это устройство – брелок). Дело в том, что в основе алгоритма шифрования кодов *Keeloq* используется уникальный ключ. Достать ключ из алгоритма теоретически невозможно. Однако любители угона чужих автомобилей (автоугона) легко извлекают код с помощью кодграббера – специального устройства, реализующего возможность вычисления посылок управления блоком сигнализации после анализа всего лишь одной перехваченной посылки управления. Тем самым нарушается целостность информации в автосигнализации автомобиля.

В докладе для борьбы с автоугоном с помощью кодграббера предлагается противоугонное устройство, повышающее помехоустойчивость принимаемого радиосигнала, который передаётся от устройства дистанционного управления к блоку управления автосигнализацией.

Противоугонное устройство состоит из аппаратной части на базе микроконтроллера и программной части (программного обеспечения микроконтроллера). Для повышения помехоустойчивости используется алгоритм, основанный на анализе длительности логического «0» и «1» в принимаемом сигнале.

Протокол передачи данных Keeloq состоит из преамбулы (12 старт битов и 11 пауз между ними общей длительностью 23Te, где Te составляет от 280 до 620 мкс); хедера (длительностью 10 Te); информационной части, состоящей из 66 битов (каждый

информационный бит состоит из импульса (2Te – лог. «0», Te – лог. «1») и паузы – (1Te – лог. «0», 2Te – лог. «1»)). Устройство дистанционного управления (брелок), которое находится у хозяина автомобиля, излучает в радиоэфир управляющую блоком управления автосигнализацией команду (серию от одной и более идентичных по своему содержанию посылок, совокупность которых составляет информационное сообщение). Данный радиосигнал одновременно поступает на кодграббер, который находится у злоумышленника, и на блок управления автосигнализацией, находящийся в машине.

В алгоритме кодоподмены, который используется в кодграббере, идет искажение 1-ой части передаваемой посылки, во 2-ой посылке искажается соответственно другая часть посылки. Данное действие позволяет кодграбберу искажать передаваемый сигнал, что не позволяет идентифицировать команду устройству управления. После чего кодграббер складывает неискаженные части принятых посылок и формирует неискаженную команду, которую впоследствии можно использовать для автоугона.

Для борьбы с данным алгоритмом в предлагаемом противоугонном устройстве анализируется длительность принимаемого импульса (паузы), что позволяет обнаруживать искажаемые области принимаемого сигнала (при длительности помехи более 2Te) и при приеме нескольких идентичных посылок, передаваемых в одном сообщении, устройство восстанавливает исходный сигнал и передает его на устройство управления автосигнализацией, что делает использование кодграбберов бесполезным. Если длительность помехи менее 2Te (в пределах одного информационного бита, состоящего из 3Te (импульса (2Te – лог. «0», Te – лог. «1») и паузы – (1Te – лог. «0», 2Te – лог. «1»)), то устройство анализирует код принятой команды. Каждая из передаваемых посылок в пределах одного сообщения будет отличаться от предыдущей, что позволяет сделать вывод, что команды искажена. После этого устройство передает каждую из принятых посылок на устройство управления с нефункциональным кодом исполняемой команды.

Описанный выше способ защиты информации в автосигнализации мобильных объектов (обеспечения целостности информации в ней) реализован в аппаратной и программной частях спроектированного противоугонного устройства.

Структурная схема аппаратной части состоит из следующих блоков:

– антенна;

– микроконтроллер ATtiny84 фирмы Atmel;

– буфер согласования сигнала;

– преобразователь напряжения.

При помощи антенны на приемник поступает радиосигнал. Приемник фильтрует сигнал, усиливает его и производит демодуляцию, выделяя, тем самым, полезную часть принятого сигнала. После демодуляции сигнал поступает на микроконтроллер, где происходит его анализ. После анализа микроконтроллер формирует выходной сигнал, который поступает либо напрямую, либо через буфер согласования на блок управления автосигнализаций. Микроконтроллер имеет возможность управления режимами работы приёмника.

Программная часть противоугонного устройства (программа для микроконтроллер ATtiny84) написана на языке программирования «C» средствами AVRStudio 6.1. После разработки программы было проведено моделирование её работы в приложении Proteus 7.1.

Создан макет противоугонного устройства. Проверка работоспособности макета в присутствии Государственной Экзаменационной Комиссии показала полную его работоспособность, в том числе работоспособность созданного программного приложения.

УДК 004.42

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ В МОБИЛЬНЫХ ТЕЛЕФОНАХ

А.В. РУДСКИЙ [1], В.В. НИКОЛАЕНКО[2], И.И. ШПАК [3]

[1]ИП Рудский А.В.
ул. Сябровская, 83, г. Брест, 224000, Республика Беларусь
andy.rudsky@gmail.com

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
nickangel.blr@gmail.com

[3]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
shpak@bsuir.by

Проводится анализ и исследование методов защиты пользовательских данных в мобильных телефонах. Разрабатывается прототип программного средства по защите пользовательских данных в операционной системе Android с легким и понятным пользовательским интерфейсом и выгодно отличающимся от имеющихся аналогов на рынке.

Ключевые слова: информационная безопасность, пользовательские данные, программное средство, мобильный телефон, операционная система Android.

В мобильных телефонах существует целый ряд данных, доступ к которым для посторонних лиц нежелателен. Эти данные могут быть самыми разнообразными – от фотографий до пользовательских данных, несанкционированный просмотр которых может быть неприятен владельцу или даже наносит ему конкретный материальный ущерб. В этих условиях актуальной становится задача обеспечения информационной безопасности данных в мобильных телефонах. Одним из методов решения этой задачи является создание программных средств защиты данных.

В докладе рассматривается прототип программного средства по защите пользовательских данных в операционной системе Android с легким и понятным пользовательским интерфейсом и выгодно отличающимся от имеющихся аналогов на рынке. С точки зрения наибольшей значимости для информационной безопасности и одновременной наименьшей стоимости парирования угроз отобраны для последующей работы две угрозы – угроза потерь информации вследствие вирусной атаки и уничтожения или потери данных вследствие несанкционированного доступа.

Создаваемое программное средство поддерживает следующие функции:

– добавление файлов и папок;

– сжатие данных;

– шифрование файлов с использованием алгоритма AES (Advanced Encryption Standard) с длиной ключа 128 и 256 бит;

– возможность замены и извлечения файлов, а также безопасного удаления файлов и папок;

– возможность отменять любую операцию с зашифрованными файлами;

– осуществление функций навигации;

– чтение и сохранение настроек программы;

– защита программы от сбоев при работе;

– установка пароля для шифруемых файлов;
– возможность получения информации файлов и папок в архиве.

Для работы программного средства необходимо мобильное устройство с операционной системой Android версии системы 4 и выше, а также наличие достаточного количества памяти для хранения обработанных файлов и информации о них. Требуется подключение к глобальной сети Internet.

Входной информацией являются файлы или папки, которые пользователь может добавить в архив следующими способами:
– через главное меню программы;
– через браузер файловой системы.

Выходной информацией служит созданный пользователем файл, в котором содержаться зашифрованные данные.

Для разработки ПС выбрана среда разработки Xamarin Studio на основе языка программирования C#. Программа на языке C# выполняется в среде .NET Framework – интегрированном компоненте Windows, содержащем виртуальную систему выполнения (среда CLR) и унифицированный набор библиотек классов. Структура ПС представляет собой совокупность взаимосвязанных программных модулей:
– модуль работы с файловой системой;
– модуль получения списка файлов;
– модуль системных настроек;
– модуль пользовательского интерфейса;
– модуль формирования метаданных;
– модуль нормализации данных;
– модуль шифрования данных.

При запуске ПС пользователь попадает на экран отображения списка зашифрованных файлов (рис. 1). Каждый элемент списка представляет собой информацию о файле: имя, дата обработки, размер. По умолчанию список отсортирован по убыванию по дате шифрования, т.е. последний обработанный файл находится вверху списка. При нажатии на элемент списка пользователю будет отображено окно информации о зашифрованном файле. Экран содержит, помимо списка, панель инструментов, которая находится наверху. Панель отображает название экрана, общее количество файлов в списке и кнопку меню.

Рис. 1. Экран отображения списка зашифрованных файлов

Прототип ПС представляет собой готовый к установке файл с расширением .apk. Программный продукт прошел ряд тестов (функциональное, интеграционное, системное и регрессионное тестирование) и готов к использованию.

УДК 004.42

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОНЛАЙНОВЫХ ИГРАХ И СЕРВИСАХ

С.В. ТЕТЕРИН[1], В.И. ПАЧИНИН[2]

[1]СООО Гейм-Стрим
пр-т Партизанский, 178/2, офис 38, г. Минск, 220028, Республика Беларусь
hypnotypes@gmail.com

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
pachinin@bsuir.by

Анализируется основная угроза информационной безопасности в онлайновых играх и сервисах – угроза несанкционированного доступа к аккаунтам игроков и виртуальным предметам. Предлагается комплекс организационных и технических мероприятий по парированию этой угрозы.

Ключевые слова: онлайновая игра, защита информации, учётная запись, аккаунт, несанкционированный доступ.

Десятки миллионов людей проводят время в онлайновых играх. Для примера, аудитория World of Warcraft – ~11.4 млн человек, World of Tanks – ~60 млн, Guild Wars 2 – ~9 млн, Star Wars: The Old Republic – ~1.3 млн [1, 2]. Игроки используют свою личную информацию (страна проживания, номер мобильного телефона, адрес электронной почты и др.) для формирования своей учётной записи в игре, а также совершения платежей и других операций, передавая ее сервисам онлайн-игр. Помимо этой информации, огромной ценностью являются игровые аккаунты и виртуальные предметы, которые продаются в интернете за большие деньги и представляют большую ценность для их обладателей.

В докладе рассматривается основная угроза информационной безопасности в онлайновых играх и сервисах – угроза несанкционированного доступа. При этом под несанкционированным доступом понимается завладение доступом к учётной записи игрока лицом, не являющимся её владельцем, а под аккаунтом – связка логина/пароля.

Самый несложный и практически не имеющий вариантов защиты способ кражи аккаунтов у пользователей – получение аккаунта из рук жертвы путем «социальной инженерии» – злоумышленник через социальные сети или простое общение с жертвой узнает некоторые данные от пользователя, такие как адрес e-mail, дату рождения, некоторые персональные данные (они могут быть использованы в качестве ответа на секретный вопрос при попытке восстановить доступ к аккаунту) и использует эти данные для получения аккаунта. Также популярным способом является «фишинг» – на почту пользователя приходит письмо, оформленное как письмо от компании-разработчика, с просьбой предоставить пароль от своего аккаунта. Разумеется, письмо подделано злоумышленником. Несмотря на некоторую наивность, данный способ часто приводит к положительным для хакера результатам. Довольно частый способ получения чужих аккаунтов – программы-кейлоггеры, записывающие символы, введенные с клавиатуры пользователя. Более изощренные хакеры могут использовать различные «эксплоиты» (бреши в системе), позволяющие, например, отобразить в браузере пользователя формы для ввода пароля и логина. Естественно, данные формы отправляют данные злоумышленнику. Так же возможны банальные «брутфорсы» (подборы паролей) по уже извест-

ным e-mail адресам. Это лишь некоторые из известных способов получения чужих аккаунтов.

В связи с вышесказанным, игровым компаниям, осуществляющим разработку онлайн-игр необходимы комплексные меры для защиты информации. Каждая онлайновая игра имеет определенный набор сервисов спутников, таких как: платежные системы, позволяющие проводить онлайновые платежи; форумы для общения игроков; сайты поддержки пользователей, используемые для обработки запросов пользователей; комьюнити-сайты, предоставляющие новости, поиск игроков/гильдий и другую функциональность для расширения игровой вселенной в рамках проекта.

Типичная онлайновая игра разделена на две большие составляющие – серверная часть и игровой клиент, устанавливаемый на компьютеры пользователей. В отличие от серверной части, взлом которой является редкой и крайне не тривиальной задачей, клиент, поставляемый игрокам – уязвимое место для взлома. Обычно подобные взломы производятся с целью создания ботов – автоматизированных программ, способных моделировать поведение в игре живого человека. Боты используются для автоматической «прокачки» аккаунтов, что наносит вред самой игре и ее экосистеме.

Сервисы-спутники подвержены хакерским атакам на различных уровнях. Поскольку эти сервисы являются веб-приложениями, для них характерно большое количество уязвимых мест. Обычно цель хакера в таких случаях заключается в получении несанкционированного доступа к аккаунтам других людей.

Часто в архитектуру онлайновых игр и сопутствующих сервисов закладывается идея «единого аккаунта», который является удобным для пользователя и, одновременно, злоумышленника: игрок создает одну пару логин/пароль, и при помощи ее получается возможность доступа не только к своему аккаунту но и к форуму, сайту поддержки, комьюнити-сайту и др. Таким образом, украв аккаунт из базы данных, например форума, злоумышленник получает доступ и к игровому аккаунт.

Для парирования вышеперечисленной угрозы (обеспечения защиты аккаунтов) в докладе предлагаются следующие меры:

– секретные вопросы при попытке восстановить доступ к аккаунту;

– подтверждения операций по телефону («привязка телефона»);

– установка «Captcha» на всех формах логина;

– установка защиты от подбора пароля (невозможность слишком частых попыток ввода пары логин/пароль);

– постоянное обновление и доработка форумов (обычно берутся стандартные форумы от стороннего производителя, которые нередко бывают полны уязвимостей).

На стороне клиента для предотвращения взлома игры и создания ботов предлагается:

– все логические расчеты производить только на стороне сервера;

– формы ввода логина/пароля защищать Capthca;

– проводить надежную архивацию ресурсов игры;

– внедрять систему жалоб и доносов – игроки, которые заподозрят других игроков в «ботоводстве», должны иметь возможность быстро и удобно сообщить об этом администрации проекта; анти-чит системы на сервере.

Необходимо также проводить социальные работы с аудиторией игроков – периодически повышать их грамотность в области сетевой безопасности, напоминать игрокам простые правила: пароль должен быть сложным, администрация проекта никогда не запросит данные об аккаунте у самого пользователя, личные данные лучше не доверять непроверенным людям, антивирус должен быть всегда обновлен и запущен.

УДК 621.396.6-027.31:654.9(076.5)

ОЦЕНКА ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.М. БОРОВИКОВ, Е.Н. ШНЕЙДЕРОВ, Д.А. СТАШЕВСКИЙ, В.Е. МАТЮШКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
bsm@bsuir.by

Для оценки качества работы электронных систем безопасности (ЭСБ) предлагается использовать показатель эффективности функционирования, представляющий собой полную вероятность защиты объекта от проникновения нарушителя с целью хищения материальных и информационных ресурсов.

Ключевые слова: электронная система безопасности, надёжность системы, эффективность функционирования, вероятность защиты объекта.

Надёжность ЭСБ, обеспечивающих защиту объектов, материальных и информационных ресурсов, можно описать с помощью общепринятого показателя надёжности, такого как вероятность работоспособного состояния R, учитывающего вероятности работоспособного состояния устройств, входящих в состав ЭСБ (обозначим эти вероятности через $r(j)$, где j означает конкретное техническое устройство).

Технические устройства ЭСБ с точки зрения формирования и/или правильной обработки сигналов о проникновении на объект нарушителя не являются идеальными. Поэтому для вероятности защиты объекта $P_{\text{защ}}$ имеет место неравенство $P_{\text{защ}} < R$. Более полным обобщённым критерием качества работы ЭСБ является показатель эффективности её функционирования (обозначим показатель через E). Для этого показателя справедливо выражение

$$E = \sum_{i=1}^{N} h_i(t)\Phi_i\,, \tag{1}$$

где $h_i(t)$ – вероятность того, что ЭСБ в момент времени t находится в i-м техническом состоянии; Φ_i – коэффициент эффективности i-го технического ЭСБ, N – число возможных технических состояний.

Переход ЭСБ из одного технического состояния в другое обусловлен потерей работоспособности того или иного устройства ЭСБ. В качестве коэффициентов эффективности Φ_i логично рассматривать вероятность обнаружения нарушителя в случае нахождения ЭСБ в i-м состоянии. В этом случае показатель E будет представлять собой вероятность защиты объекта ($P_{\text{защ}}$) с помощью рассматриваемой ЭСБ.

Предлагаемый подход проиллюстрирован примером анализа простейшей ЭСБ, для которой схема и модель показаны на рис. 1. Условием работоспособного состояния ЭСБ будем считать одновременную работоспособность хотя бы одного из датчиков и работоспособность микропроцессорного приёмно-контрольного устройства (МП ПКУ).

Для определения вероятности i-го состояния ЭСБ использована формула

$$h_i = s(\text{Д1}) \cdot s(\text{Д2}) \cdot s(\text{МП})\,, \tag{2}$$

где $s(j)$ – вероятность, характеризующая техническое состояние (работоспособное или неработоспособное) j-го устройства ЭСБ; $j \rightarrow$ Д1 (датчик 1), Д2 (датчик 2), МП (микропроцессорное приёмно-контрольное устройство).

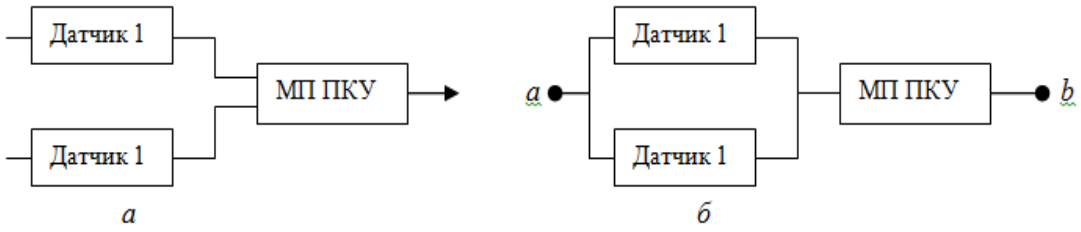


Рис. 1. Схемы, используемые для анализа рассматриваемой ЭСБ:
а – структурная схема ЭСБ; *б* – модель (схема) соединения устройств ЭСБ с точки зрения работоспособности и с точки зрения обнаружения нарушителя

В формулу (2) в качестве значений вероятностей $s(j)$ необходимо подставить вероятность работоспособного состояния $r(j)$, если j-е устройство находится в работоспособном состоянии и вероятность $[1-r(j)]$, если – в неработоспособном состоянии.

Согласно модели рис. 1, *б*, формула расчёта коэффициентов Φ_i получена в виде

$$\Phi_i = [1-(1-p_{Д1})(1-p_{Д2})]p_{МП}. \quad (3)$$

В формуле (3) буквой p обозначены вероятности формирования и/или правильной обработки сигнала о нарушении, а по нижним индексам интуитивно понятно, к какому устройству ЭСБ относится соответствующая вероятность. При расчёте Φ_i по формуле (3) соответствующую вероятность p необходимо принять равной нулю, если устройство находится в неработоспособном состоянии.

Вероятности технических состояний ЭСБ h_i и коэффициенты эффективности, соответствующие этим состояниям, представлены в табл. 1 в предположении, что $r(Д1) = r(Д2) = 0{,}9$; $r(МП) = 0{,}95$. Для вероятностей формирования и/или правильной обработки сигнала о нарушении приняты следующие значения: $p_{Д1} = p_{Д2} = 0{,}9$; $p_{МП} = 0{,}99$.

Табл. 1. Возможные технические состояния рассматриваемой ЭСБ

Номер технического состояния ЭСБ, i	Описание состояния работоспособности устройств ЭСБ			Вероятность технического состояния ЭСБ в целом $h_i(t)$	Коэффициент эффективности технического состояния Φ_i	Произведение $h_i(t)\Phi_i$
	датчик 1	датчик 2	МП ПКУ			
1	1	1	1	0,7695	0,9801	0,7542
2	1	1	0	0,0405	0	0
3	1	0	1	0,0855	0, 891	0,0762
4	1	0	0	0,0045	0	0
5	0	1	1	0,0855	0, 891	0,0762
6	0	1	0	0,0045	0	0
7	0	0	1	0,0095	0	0
8	0	0	0	0,0005	0	0

Примечание. Принятые обозначения для технических состояний устройств ЭСБ: 1 – работоспособное состояние; 0 – неработоспособное состояние.

С учётом схемы (см. рис. 1, *б*) получено: $R = 0{,}9405$. Пользуясь табл. 1, по формуле (1) можно найти $E = P_{защ} = 0{,}9066$. Из этих данных видно, что $P_{защ} < R$.

Показатель $P_{защ}$ даёт более объективный ответ о степени защиты объекта.

УДК 621.391

FINDING OPTIMIZED THRESHOLD FOR SKIN DETECTION IN PORTRAIT IMAGES

SEYED ENAYATALLAH ALAVI, ALI TORABIYAN DEHKORDI

Shahid Chamran University of Ahvaz, Ahvaz, Iran
se_alavi@yahoo.co.uk; alitorabiyan@live.com

Many methods of skin color detection create a model of skin color and assigned a value between zero and one to each pixel. Those methods needs a threshold for classify skin and non-skin. In this paper, we presented an approach for finding the optimal threshold per image in the portrait images. The results of the proposed method show a meaningful improvement of detect skin against use constant threshold for all images.

Keywords: Artificial intelligence, image processing, skin detection, multilayer neural networks, optimal threshold.

Since many skin color model and many strategies for the detection of skin color in images is presented. This method can be divided into two general categories: pixel based and region based.

Many of methods create a model of skin color and compare each pixel with skin model. These methods needs a Threshold for classify pixels to skin and Non-skin from results of the model. This parameter used as a tool to create a balance between TP and FP. But a Threshold for all images will reduce efficiency and accuracy of the system. Our paper proposes a mechanism to detect the optimum Threshold for each portrait image so that we have the highest accuracy and the lowest FP.

Depending on the training set and the images in it some color range may be less than the others and therefore the skin probability of the pixels with these colors be less. For example, Colored People images is also the case and because there are fewer in training set their skin pixels have less Resemblance to the skin, and with a typical threshold many of their pixels will be diagnosed non-skin. In contrast, people with blond hair need higher Threshold because their hair would not be detected as skin.

To achieve this objective, our proposal is that Start with a Threshold, for example, 0.162 (data set images Best threshold Average), segment skin like image then calculate rate of skin pixels in proportion to the image pixels. We argue that if this average was down it means threshold should be low, and if it was up means threshold should be high. At the end we used the extracted feature for training a multilayer neural network MLP (2) that its objective function is optimize Threshold calculated for every pixel. Mentioned Property calculated on Based (1).

$$mean_{skin_\theta} = \frac{\#skin_\theta = 1}{x * y}, T_{Final} = MLP(mean_{skin_\theta}) * \alpha \quad (1)$$

$$0 < T_{Final} < 1, 0 < \alpha < \infty \quad (2)$$

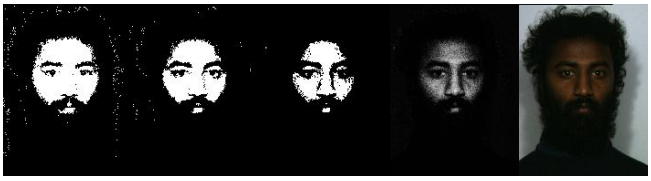
Is number of image skin pixels detected in Threshold θ. x, y is the length and width of the image. T_Final is the system final and optimize threshold for the desired image. α is Added parameter as a tool to balance the detection accuracy and the FP. there is not limit for increased α, but T_Final shouldn't be greater than one.

Here we used a three-dimensional histogram model for model skin color and for better decisions should use the skin and non-skin histogram (3).

$$P_{final} - \frac{P(rgb|skin)}{P(rgb|skin) + P(rgb|\sim skin)} \quad (3)$$

The data set includes 336 images and its guide images that 50 images were used for testing. The results with the best Threshold 0.162 (best Thresholds mean per picture) show 0.0757 difference with optimal Threshold. But with proposed method, the error is reduced to 0.0572.

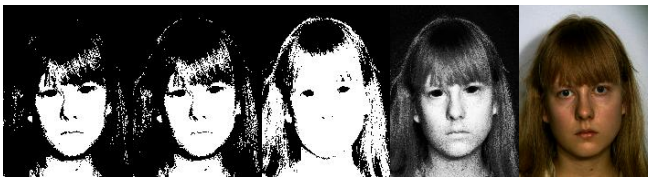
As you can see the results in Fig. 1 picture (*b*) brightness is low because the chances of skin pixels - is low. So with average threshold (Fig. 1, *c*) pixel around the nose are recognized Non-skin. The shortcoming of the proposed method is less (Fig 1, *d*). In Fig. 1, *j* best Threshold used that have lowest rate or percentage of FP but the number of the FP in it is higher than proposed method that is visible of white dots on the hair.



a *b* *c* *d* *j*

Fig. 1. From right to left: *a* – the original image; *b* – Skin like image; *c* – Segmented with average Threshold = 0.162; *d* – calculated with solution Threshold = 0.07; *j* – calculated with optimal Threshold = 0.05

In Fig. 2 (*b*) be see a person with blond hair that her hair color is similar to skin color and with average threshold many of hair pixels detected as skin. But with proposed method has decreased the amount of FP and less hair detected as skin and the result is closer to optimal result. Result of three methods of threshold selection are shown in Table 1.



a *b* *c* *d* *j*

Fig. 2. From right to left: a – the original image; *b* – the skin like image; *c* – Segmented with Average Threshold = 0.162; *d* – calculated with solution Threshold = 0.4; *j* – calculated with optimal Threshold = 0.48

Table 1. Error rates

	Average threshold	*Proposed method*	*Best threshold*
FP Rate	*11%*	*10%*	*9%*
FN Rate	*19%*	*18%*	*16%*

As seen in Tab. 1, Best Threshold also has an error that this caused pixel base approaches inability to complete separation between skin and non-skin pixels with reasons mentioned in the introduction. The results show a reduction of the distance between thresholds was proposed and optimized threshold So that this distance was reduced from 0.0757 for best average threshold to 0.0572 in proposed method. The results in Table 1 show improved detection of skin pixels too. The purpose of this method is only portrait images that can developed it on multiplayer screenshots as future work. For example, with face detection, make ROI and use of a several threshold in an image to improve the performance of the pixel based methods.

УДК 658.29-049.5

АКТУАЛЬНЫЕ ВОПРОСЫ РЕЙТИНГОВЫХ ОЦЕНОК ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. МАЛИКОВ, И.В. БЕНЕДИКТОВИЧ, С.А. ЧУРЮКАНОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
malvvv104@mail.ru

Предложен подход для рейтинговых оценок инцидентов информационной безопасности, основанный на комплексной оценке инцидента по критерию близости совокупного (реального и потенциального) ущерба с учетом уровня технологичности атак.

Ключевые слова: рейтинговые оценки инцидентов информационной безопасности, совокупный ущерб, уровень технологичности атак, оптимизация рисков.

В настоящее время наблюдается значительный количественный и качественный рост числа инцидентов информационной безопасности на объектах различных категорий [1]. Основная часть таких инцидентов осуществляется удаленно через каналы сопряжения и коммуникации. В связи с тем, что владельцами каналов, как правило, являются организации связи, необходима разработка дополнительных нормативно-правовых, организационно-технических и технических мер по их защите.

Одним из эффективных способов, позволяющих охарактеризовать риск произошедшей атаки и сформировать предположения по тенденциям ее дальнейшего развития является создание рейтинговых оценок инцидентов информационной безопасности.

В качестве определяющих параметров оценки множества инцидентов информационной безопасности предлагаются следующие:

1. Совокупный (финансовый и не финансовый) ущерб – $S_{сов.}$
2. Относительный уровень возмещения ущерба – $К_{отн}$.

В качестве дополнительного параметра оценки множества инцидентов информационной безопасности предлагается - параметр технологичности инцидента – $К_{техн}$.

Таким образом, на основе изложенного выше, представление рейтинговой оценки инцидента на основе уровневой значимости инцидентов информационной безопасности – $У_{инц}$ с учетом описанных параметров оценки будет иметь вид:

$$У_{инц}=\{S_{сов}, К_{отн}, К_{техн}\}. \quad (1)$$

Для экономической оценки совокупного (финансового и нефинансового) ущерба инцидента информационной безопасности объекта $S_{сов}$ – предлагается проведение анализа по двум направлениям:

1. Реальный ущерб – ущерб, обладающий признаками: последствия очевидны и документируемы; возможно проведение конечного экономического расчета суммы ущерба.
2. Потенциальный ущерб – ущерб, обладающий признаками: последствия не всегда очевидны и явно документируемы; возможно проведение ориентировочного (предполагаемого) экономического расчета суммы ущерба.

Оценку величины совокупного (финансового и не финансового) ущерба $S_{сов}$ – с отнесением к одному из уровней значимости предлагается осуществлять по двум параметрам:

1. Пороговая величина ущерба, определяемая нормативно-правовыми актами.

2. Относительный уровень возмещения ущерба $К_{отн}$ – определяемый величиной совокупного ущерба – $S_{сов}$ по отношению к совокупной стоимости компании (ресурсов компании) – $S_{ст}$.

В качестве дополнительного показателя оценки инцидента информационной безопасности объекта предлагается ввести параметр технологичности инцидента – $К_{техн}$, показатели которого будет иметь следующие возможные значения:

1. Высокотехнологичный инцидент (H): инцидент не описан в базах знаний по уязвимостям; инцидент является результатом таргетированной атаки (0-day, Watering Hole, социальная инженерия) [2].

2. Низко технологичный инцидент (L): инцидент полностью описан в базах знаний по уязвимостям и сборниках эксплойтов; инцидент не является результатом таргетированной атаки.

3. Смешанный инцидент (HL): инцидент частично описан в базах знаний по уязвимостям и сборниках эксплойтов; инцидент является результатом таргетированной атаки.

В качестве базовых уровней значимости инцидента информационной безопасности – $У_{инц}$ по критерию близости совокупного (реального и потенциального) ущерба предлагаются уровни: A, B, C, D (табл. 1).

Табл. 1. Базовые уровни значимости инцидента информационной безопасности

<table>
<tr><td rowspan="2">$У_{инц}$</td><td colspan="5">Пороговая величина совокупного ущерба по НПА</td><td rowspan="2">$К_{отн}$</td></tr>
<tr><td>Особо крупный</td><td>Крупный</td><td>Значительный</td><td>Средний</td><td>Мелкий</td></tr>
<tr><td>A</td><td>AAA</td><td>AA</td><td colspan="3" rowspan="2">-</td><td>$К_{отн} > 0,5$</td></tr>
<tr><td>B</td><td>BBB</td><td>BB</td><td>$К_{отн} \leq 0,5$</td></tr>
<tr><td>C</td><td colspan="2" rowspan="2">-</td><td>CCC</td><td>CC</td><td>C</td><td>$К_{отн} > 0,5$</td></tr>
<tr><td>D</td><td>DDD</td><td>DD</td><td>D</td><td>$К_{отн} \leq 0,5$</td></tr>
</table>

Таким образом, предложенный выше подход для рейтинговых оценок инцидентов информационной безопасности, основанный на комплексной оценке инцидента по критерию близости совокупного (реального и потенциального) ущерба с учетом уровня технологичности атак, позволяет провести эффективную оценку совокупного ущерба, возможности дальнейшего функционирования объекта и проведения компенсационных выплат по результатам инцидента. Практическое использование рейтинговых оценок инцидентов информационной безопасности со стороны владельцев каналов сопряжения и коммуникаций позволит оптимизировать риски для финансово-экономической деятельности объектов связи.

Список литературы

1. DDoS-атаки первого полугодия 2013 года // securelist.com [Электронный. ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_ 2013_ goda – Дата доступа: 10.01.2014.

2. Политики безопасности: нецелевое использование ресурсов // securelist.com [Электронный ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/blog/20776 8878/ Politiki_bezopasnosti_netselevoe_ ispolzovanie_resursov – Дата доступа: 10.01.2014.

УДК 658.29-049.5

ИССЛЕДОВАНИЕ СТРУКТУРЫ И ТЕХНОЛОГИЙ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В.В. МАЛИКОВ, Р.В. РАБЦЕВИЧ, С.В. ПУЗЫНА

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
malvvv104@mail.ru

Предложена классификация рынка киберпреступности. Проведено исследование технологий совершения преступлений в системах безналичных электронных платежей сервисов сети Internet.

Ключевые слова: интернет-мошенничество, спам, DDos-атаки, рынок криминальных средств систем и услуг, преступления в системах безналичных электронных платежей.

Глобальный рынок киберпреступности активно развивается и совершенствуется в соответствии с передовыми направлениями информатизации общества, внедрением электронных систем коммуникаций, электронных платежных систем [1].

В ходе исследования проведена декомпозиция рынка киберпреступности на законченные функциональные уровни и модули (рис. 1).

Рис. 1. Классификация рынка киберпреступности

Предлагается использование варианта декомпозиции, который учитывает полный технологический цикл осуществления атак, включающий как разработку вредоносного программного обеспечения, так и непосредственно его использование в преступных целях. В качестве

базовых уровней предлагаются следующие: интернет-мошенничество, спам, DDos-атаки, рынок криминальных средств систем и услуг.

Наибольший интерес для криминального организатора киберпреступлений представляют безналичные электронные платежи пользователей сервисов сети internet [2].

Основные варианты перехвата управления в сервисах безналичных электронных платежей приведены на рис. 2.

Для устранения возможностей перехвата и повышения уровня безопасности платежными сервисами используется алгоритм двухфакторной аутентификации пользователя. Однако, наиболее развитые и технологичные троянских программы, используемых киберпреступниками, например банковский троянец ZeuS (Zbot) совместно с мобильным троянцем ZeuS-in-the-Mobile (ZitMo), могут обходить данную систему защиты Другие системы защиты сервисы безналичных электронных платежей также нейтрализованы киберпреступниками: система chipTAN — банковский троянец SpyEye; система на основе USB-токена — банковский троянец Lurk.

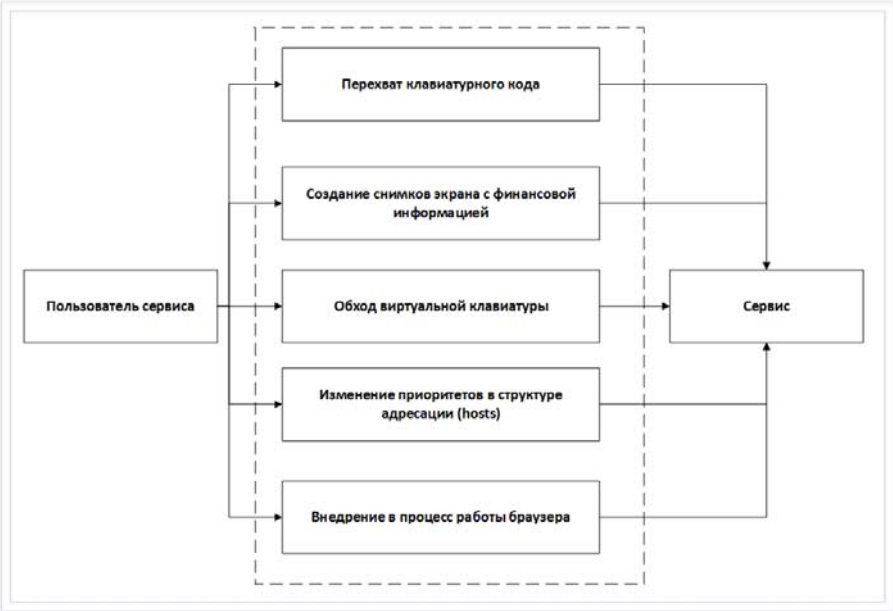


Рис. 2. Схема перехвата управления в сервисах безналичных электронных платежей

Проведение исследования структуры и технологий совершения киберпреступлений позволяет государственным регуляторам и организациям по борьбе с киберпреступлениями оперативно реагировать на инциденты информационной безопасности, формировать методики оперативно-розыскных мероприятий и повышать общий уровень информированности граждан.

Список литературы

1. Рынок преступлений в области высоких технологий: состояние и тенденции 2013 года // group-ib.ru [Электронный ресурс]. – 2013. – Режим доступа: http://www.group-ib.ru/list/1008-analytics/?view=article&id=1155. – Дата доступа: 14.01.2014.

2. Защита от виртуальных грабителей // securelist.com [Электрон. ресурс]. – 1997. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050811/Zashchita_ot_virtualnykh_grabiteley – Дата доступа: 15.01.2014.

УДК 614.841.343:699.814.6

ЭФФЕКТИВНОСТЬ СИСТЕМ ПОЖАРНОЙ БЕЗОПАСНОСТИ МНОГОЭТАЖНЫХ ЗДАНИЙ

В.Е. ГАЛУЗО, А.И. ПИНАЕВ, В.В. МЕЛЬНИЧУК, В.В. ХОРОШКО

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
valga51@yandex.ru

Противодымная защита является обязательным атрибутом систем пожарной безопасности многоэтажных зданий. При проектировании этих систем решается задача выбора эффективной тактики и оборудования ее обеспечивающего. Однако, при испытании этих систем зачастую проявляются технические проблемы по их сдаче в эксплуатацию. В связи с этим представляют интерес работы по практической рекомендации построения систем противодымной защиты.

Ключевые слова: системы пожарной безопасности, системы противодымной защиты, системы дымоудаления.

Деятельность в области пожарной безопасности является лицензируемой. Одним из основных требований к лицензиату является квалификация работников. Подготовка специалистов для этой сферы деятельности ведется в БГУИР, что хорошо известно органам, выдающим лицензии. Непременным требованием к специалистам занятым в области безопасности является руководство в своей деятельности соответствующими техническими нормативно-правовыми актами (ТНПА). Однако, некоторые ТНПА из-за своего несовершенства подвергаются постояной переработке, что происходит при непосредственном участии специалистов, занятых в этой сфере, в том числе сотрудников нашего ВУЗа. В данной работе приводятся практические рекомендации по разработке тактики построения и проектирования систем противодымной защиты (ПДЗ).

Основной задачей системы противодымной защиты (ПДЗ) многоэтажных зданий является уменьшение и предотвращение задымления путей эвакуации в начальной стадии пожара. Она решается путем устройства незадымляемых лестничных клеток и дымоудаления (ДУ) из коридоров, а также исключения распространения дыма через шахты лифтов.

В соответствии с [1], в многоэтажных зданиях высотой свыше 30,0 м и более следует использовать незадымляемые лестничные клетки и дымоудаление (ДУ) из коридоров. При этом не менее 50 % лестничных клеток должны быть незадымляемыми типа Н1. Согласно [2] незадымляемость лестничных клеток Н1 обеспечивается за счет устройства входов на них через наружную воздушную зону (лоджию). В соответствии с [3] расход продуктов горения, удаляемых из каждого коридора системой ДУ, рассчитывается из условия защиты дверей эвакуационных выходов от проникания дыма за их пределы, что может быть необходимо для обеспечения незадымляемости лестничных клеток Н2 и Н3 [2]. Согласно [3] ДУ необходимо из коридоров без естественного освещения длиной более 12,0 м. Таким образом, из анализа [2] и [3] следует, что ДУ в многоэтажных зданиях с лестницами только типа Н1 необходимо лишь в случае коридора без естественного освещения при его длине более 12,0 м.

Особые проблемы, связанные с обеспечением перепада давления на закрытых дверях путей эвакуации, избыточного давления на нижних этажах и скорости воздуха в дверном проеме при выходе с этажа пожара, возникают при проектировании лестниц

Н2 [2]. Кроме того, если и удается обеспечить при испытаниях необходимые значения перечисленных параметров, то в реальных условиях эвакуации при пожаре это скорее всего маловероятно из-за того, что будут открыты двери на других этажах кроме этажа пожара. Поэтому от этого типа незадымляемой лестницы следует отказаться.

Наиболее эффективным вариантом является использование незадымляемых лестничных клеток Н1 и Н3 [2]. При проектировании систем ПДЗ с лестницами Н3 предлагается вести расчет необходимого расхода воздуха подаваемого в тамбур-шлюз из условия обеспечения скорости воздуха равного 1,3 м/с в открытой двери на этаж пожара. Кроме того, для исключения завышенного значения перепада давления на закрытых дверях при эвакуации следует дверь из тамбура на лестницу Н3 делать самооткрывающейся или разблокировать ее, если она подключена к системе контроля доступа.

В соответствии с [1] двери лестничных клеток всех типов, ведущие в общие коридоры, должны открываться по направлению выхода из здания и их следует проектировать дымонепроницаемыми, что обеспечивается оборудованием дверей приборами для самозакрытия и устройством уплотнений в притворах. При срабатывании пожарной автоматики откроется клапан дымоудаления в коридоре на этаже пожара и вентилятор системы ДУ. Но из-за того, что двери на лестницу и все остальные проемы в здании закрыты, никакое удаление дыма происходить не будет. Кроме того, из-за разряжения воздуха, создаваемого вентилятором ДУ, двери на пути эвакуации будет открыть трудно. Для обеспечения эффективности ДУ и уменьшения перепада давления на закрытых дверях путей эвакуации предлагается устанавливать на этаже пожара клапаны сброса давления или использовать самооткрывающиеся окна.

При возникновении пожара в помещении продукты горения через оставленную открытой при эвакуации или прогоревшую дверь выходят в коридор, вызывая срабатывание автоматики противодымной защиты. Из-за наличия в помещении естественной обменной вентиляции при включении ДУ через помещение будет проходить воздух, что усугубит пожарную обстановку в помещении. Следовательно, в шахтах естественной вентиляции необходимо устанавливать клапаны, перекрывающие движение воздушных масс при срабатывании автоматики ДУ.

Большое значение имеет также правильный выбор и монтаж декоративных решеток на клапанах ДУ. Универсальной как для горизонтальных воздуховодов, так и вертикальных шахт ДУ будет декоративная решётка-сетка типа «рабица», которая при любом способе монтажа будет вносить малый коэффициент местного сопротивления. В соответствии с [4] при измерении расхода воздуха удаляемого через клапан ДУ во время проведении испытаний необходимо снимать декоративные решетки, изменяющие направление воздушного потока. Но при снятой решетке расход воздуха будет больше расчетного. Поэтому в проекте необходимо указывать расходы воздуха, удаляемого через клапан как при снятой так установленной декоративной решетке.

Список литературы

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

2. СНиП 21-01-97. Пожарная безопасность зданий и сооружений.

3. ТКП 45-4.02-273-2012. Противодымная защита зданий и сооружений при пожаре. Системы вентиляции. Строительные нормы и правила проектирования.

4. НПБ 23 – 2010. Противодымная защита зданий и сооружений. Методы приемо-сдаточных и периодических испытаний.

УДК 004.353.2

МЕТОДИКА РАСЧЕТА ТЕПЛОВЫХ ПОЛЕЙ СРЕДСТВ ТЕПЛОВОЙ ЗАЩИТЫ

ОКПАЛА ХЕНРИ АФАМ, АЛИ ХАМЗА АБДУЛЬКАБЕР АБДУЛЬКАДЕР

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Предложена методика расчета тепловых полей средств тепловой защиты. Показана возможность ее реализации с использование программы Elcut.

Ключевые слова: средство тепловой защиты, геометрическая модель, граничные условия.

Защита информации от утечки по тепловому каналу может быть обеспечена за счет использования средств тепловой защиты (СТЗ), которые обеспечивают снижение теплового контраста между защищаемым объектом и фоном, на котором он размещается. Для практической реализации СТЗ необходимо выполнить выбор и обоснование материалов, которые будут определять теплофизические свойства таких конструкций, их технологичность и стоимость. В качестве основы для создания таких конструкций могут использоваться металлы и их сплавы как способные относительно быстро нагреваться и охлаждаться [1], полимерные материалы, характеризующиеся невысоким значением массы [2], и волокнистые материалы (целлюлоза и синтетические волокна) с развитой капиллярно-пористой структурой [3].

Решение такой задачи разработки базовых модулей СТЗ может быть реализовано за счет использования численных методов моделирования [4] реализуемых рядом программ. Широко используемым является метод конечных элементов [5], характеризующийся вычислительной гибкостью при моделировании взаимодействия электромагнитных полей со сложными объектами. В качестве программной среды, реализующей данный метод, представляется целесообразным применение программы Elcut, которая позволяет выполнить расчет теплового поля с учетом следующих неопределенностей:

– зависимость теплопроводности от температуры;
– определения источника поля, тепловая мощность которого зависит от температуры;
– нелинейности процесса радиационного теплообмена.

Основным преимуществом программы Elcut является высокая скорость решения задачи при обеспечении практически линейной зависимости времени решения от размерности задачи, что позволяет в значительной степени сократить временные затраты на проведения расчетов. Для других аналогичных программ время расчета увеличивается квадратично при росте количества узлов сетки [6].

Основные этапы методики расчета теплового поля СТЗ представлены на рис. 1. На первом этапе выполняется построение геометрической модели СТЗ с учетом ее линейных размеров. Такая модель представляет собой набор геометрических объектов с заданными связями между ее элементами набора и свойствами материалов, источниками поля, граничными условиями. Свойства используемых материалов, параметры источника поля и граничные условия, а также шаг ее дискретизации задаются на этапе описания модели. После чего выполняется построение сетки конечных элементов.

Рис. 1. Методика расчета теплового поля средств тепловой защиты

Точность расчета теплового поля зависит от шага дискретизации геометрической модели, которым определяется количество конечных элементов. На третьем этапе выполняется расчет теплового поля. Расчет теплового поля выполняется при условии стабильных значений температур.

В программе Elcut результаты расчеты могут быть представлены несколькими способами. Например, в виде:

– картины поля (отображения температуры по площади геометрической модели, отображение изотерм, направления векторов теплового потока);

– локальными значениями (отображение параметров поля в локальной точке модели);

– интегральными значениями (отображение параметров поля для анализируемой области);

– построения графических зависимостей параметров поля по контуру (прямая или ломаная линия, состоящая из отрезков прямых и дуг окружностей);

– построения таблиц параметров поля.

Список литературы

1. *Зиновьев В.Е.* Теплофизические свойства металлов при высоких температурах. М. : Металлургия, 1989.

2. *Михайлин Ю.А.* Термоустойчивые полимеры и полимерные материалы. СПб. : Профессия, 2006.

3. *Лыков А.В.* Явления переноса в капиллярно-пористых телах. М. : Государственное издательство технико-теоритической литературы, 1954.

4. *Самарский А.Н.* Введение в численные методы. М. : Наука, 1982.

5. *Румянцев А.В.* Метод конечных элементов в задачах теплопроводности. Калининград. : КГУ, 1997.

6. *Дубицкий С.* ELCUT – инженерная система моделирования двумерных физических полей // CADmaster. – 2001. – № 1. – С. 17–21.

УДК 004.353.2

РАДИОЭКРАНИРУЮЩИЕ ЭЛЕМЕНТЫ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ ДЛЯ ЭКРАНИРОВАННЫХ ПОМЕЩЕНИЙ НА ОСНОВЕ ПОРОШКООБРАЗНЫХ ОТХОДОВ ПЛАВКИ ЧУГУНА

НЕАМАХ МУСТАФА РАХИМ НЕАМАХ, СУДАНИ ХАЙДЕР ХУССЕЙН КАРИМ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Приводятся результаты исследования элементов строительных конструкций выполненных на основе силикатного кирпича и радиоэкранирующего искусственного камня.

Ключевые слова: коэффициент отражения, коэффициент передачи, порошкообразные отходы плавки чугуна.

Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет создания экранированных помещений предназначенных для размещения средств обработки конфиденциальной информации. Создание таких помещений возможно за счет их отделки радиоэкранирующими материалами.

Разработана конструкция радиоэкранирующего искусственного камня имеющего форму параллелепипеда (одинарного кирпича), номинальные размеры которого составляют 250x120x65 мм [1]. В качестве материалов для формирования такой конструкции использовалась смесь порошкообразных отходов плавки чугуна с размером фракции 20 мкм (50 % по массе) и портландцемента (50 % по массе). Масса кирпича должна быть не более 4,3 кг, поэтому в конструкцию был введен пористый гравий [2] с размером фракции 10…20 мм. Таким образом, вес радиоэкранирующего искусственного камня составил 3,6 кг.

Из разработанного радиоэкранирующего искусственного камня был выполнен фрагмент строительной конструкции (стена толщиной 65 мм) и измерены ее коэффициенты отражения и передачи. Для сравнения радиоэкранирующих свойств предложенного материала с существующими строительными материалами, исследованы коэффициенты передачи и отражения фрагмента строительной конструкции (стена толщиной 65 мм) выполненной из силикатного одинарного кирпича характеризующегося таким же линейным размером, как и разработанный радиоэкранирующий искусственный камень.

Показано, что у разработанного радиоэкранирующего искусственного камня коэффициент передачи меньше, чем у силикатного кирпича на -11,1…-33,4 дБ в диапазоне частот 0,7…2 ГГц и на -18,3…-19,1 дБ в диапазоне частот 2…18 ГГц (рис. 1), что обуславливает более низкий коэффициент отражения фрагмента строительной конструкции выполненной из силикатного кирпича, который составляет -1,2…-16,3 дБ в диапазоне частот 0,7…2 ГГц и -0,1…-12,5 дБ в диапазоне частот 2…18 ГГц.

Размещение металлического листа за исследуемыми элементами строительных конструкций, приводит к увеличению значения коэффициента отражения для фрагмента строительной выполненного из силикатного кирпича, который составляет -1,5…-21,5 дБ в диапазоне частот 0,7…2 ГГц и -4,1…-24,2 дБ в диапазоне частот 2…18 ГГц.

Показано, что силикатный кирпич обладает слабыми защитными свойствами. В диапазоне частот 0,7…9 ГГц регистрируется значение уровня мощности прошедшего ЭМИ через такую конструкцию 0,1…4,7 мВт при мощности падающей ЭМВ от 1 до

5 мВт. Для фрагмента строительной конструкции выполненной из радиоэкранирующего искусственного камня уровень мощности прошедшей ЭМВ составляет 0,1…0,25 мВт при тех же параметрах воздействия, что и в предыдущем случае (рис. 2).

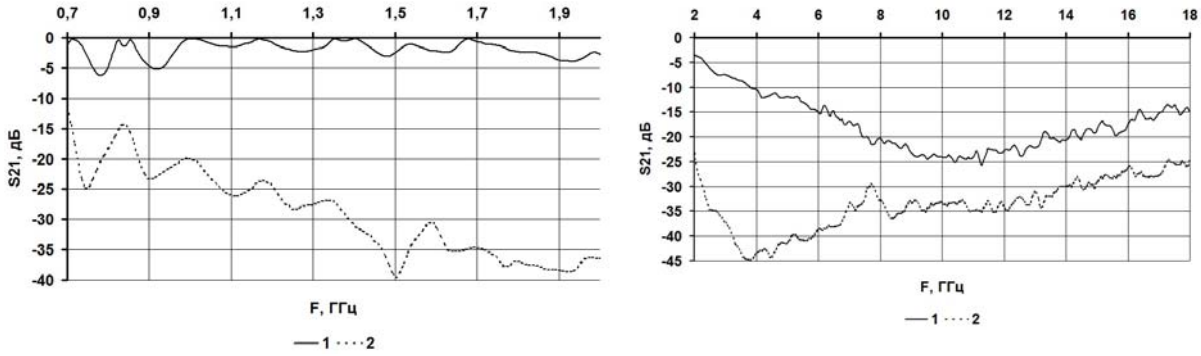
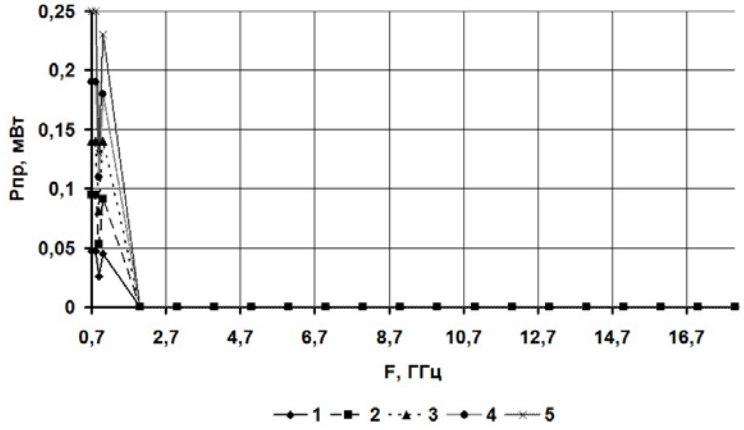


Рис. 1. Частотные зависимости коэффициентов коэффициента передачи фрагментов строительных конструкций (стен) выполненных из: 1 – силикатного кирпича; 2 – радиоэкранирующего искусственного камня



Мощность падающей ЭМВ: 1 – 1 мВт; 2 – 2 мВт; 3 – 3 мВт; 4 – 4 мВт; 5 – 5 мВт

Рис. 2. Частотная зависимость уровня мощности электромагнитного излучения, прошедшего через фрагмент строительной конструкции выполненной из радиоэкранирующего искусственного камня

Список литературы

1. Кирпич и камни керамические. Технические условия : СТБ 1160–99. – Введ. 02.06.99. – Минск. : Министерство архитектуры и строительства Республики Беларусь, 1999.

2. Гравий, щебень и песок искусственные пористые. Технические условия : ГОСТ 9757–90. – Введ. 01.01.91. – М. : Государственная ассоциация «Союзстройматериалы» : Изд-во стандартов, 1990.

УДК 004.056.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОКОНЕЧНОГО БАНКОВСКОГО ОБОРУДОВАНИЯ

ГОНДАГ САЗ МОСТАФА МОХАММАД,
МОЗДУРАНИ ШИРАЗ МОХАММАД ГОЛАМХОССЕЙН

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Рассмотрена проблема обеспечения безопасности современных терминалов самообслуживания, применяемых в банковским секторе.

Ключевые слова: банковский терминал, мошенничество.

Предложение банковских услуг через сеть терминалов самообслуживания становится массовым явлением. Как показывает мировая практика 90% банковских услуг, оказываемых в рамках традиционных отделений банка, может быть не только автоматизировано, но и переведено в сферу самообслуживания с помощью современных терминальных устройств.

Существующая система безналичных расчетов по розничным платежам на основе применения электронных платежных инструментов представлена в основном системами расчетов с использованием банковских пластиковых карточек и электронных денег.

В целях обеспечения безопасной и надежной деятельности при осуществлении операций с электронными деньгами банки должны соблюдать нормативы безопасного функционирования.

Под безопасностью системы банковских терминалов понимают их свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных (умышленных и неумышленных) воздействиях на нее. Следует отметить, что природа воздействия может быть самой различной, а следовательно и поле для угроз безопасности достаточно обширное.

Для многих банков характерно то, что нарушение безопасности информации в их конечных банковских терминалах может нанести огромный материальный ущерб, как самим банкам, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности, что ведет к необходимости реализации комплексной защиты.

Комплексный подход к обеспечению безопасности, а так же постоянный мониторинг и поиск новых угроз являются ключевым моментом обеспечения безопасного функционирования конечных банковских терминалов.

Физическое воздействие на конечный банковский терминал - один из первоочередных вопросов. Защита от вандализма, погодных условий, попытки физического взлома – решаются путем совершенствования конструкции терминалов: установкой сейфов с различными видами замков (с двойной комбинацией, с двойной комбинацией и дистанционным доступом и др.); доработкой кассет и контейнеров загрузки, хранения банкнот, исключающих доступ к денежным средствам; установкой различного рода тревожных датчиков (датчики тревожной сигнализации, сейсмические датчики, датчик температуры и др.); установкой источника бесперебойного электропитания; установкой встроенной камеры видеонаблюдения, а так же тщательным исследованием места установки терминала с точки зрения безопасности его использования.

Внешний вид терминала, а так же расположение его основных функциональных частей является не только отличительными признаками того или иного производителя устройства, но и тщательно продуманной стратегией безопасности.

В сфере мошенничества электронных платежей при обращении с кредитными картами, невозможно выделить единичную причину позволяющую совершать преступление. Так угрозы в виде «кардинга», «фишинга», пользования украденной (утерянной) картой, заявление от чужого имени и др. содержат в себе как социальные аспекты, так и уязвимости программного обеспечения и самого устройства терминала.

Эффективной мерой противодействия, в данном случае, является обучение клиентов банковских терминалов правилам пользования терминалов и мерам безопасности при обращении с картами электронных платежей, а так же своевременное их уведомление о выявленных опасностях.

Переходя с использования в своих банкоматах OS/2 на применение Windows и IP-сети, банки соответственно в корне меняют и систему подключения к своим информационным сетям. Во многих случаях это означает, что банкоматы и обычные офисные компьютеры банков оказываются подключенными к одним и тем же вычислительным сетям. Как следствие, сети банкоматов, инфокиосков, обменных пунктов и др. могут быть подвержены всем существующим видам угроз – вирусным атакам, злонамеренным действиям персонала, ошибкам администраторов, проникновениям изнутри и т.д.

Пути решения проблемы лежат в четком планировании и проектировании строящейся сети терминалов с учетом современных тенденций развития телекоммуникационных сетей, а так же использовании передовых технологий защиты информации: межсетевого экранирования; шифровании трафика; организации системы антивирусной безопасности и установки обновлений операционной системы; разработке политики безопасности функционирования системы; грамотном делегировании полномочий администраторов и обслуживающего персонала и др.

Следует так же учитывать тенденцию унификации электронных платежных сообщений и объединение в одну платежную систему ранее разрозненных организаций, что с упрощением взаимодействия между финансовыми учреждениями, в то же время, создает предпосылки для новых угроз безопасности.

УДК 621.391

FAST COMPUTATION OF THE INSTANT WALSH SPECTRUM

A.A. BUDZKO, IBENEME E. AUGUSTINE

Belarusian State University of Informatics and Radioelectronics
6, P. Brovki Str., Minsk, 220013, Republic of Belarus
kafrts1@bsuir.by

Walsh transforms have become a very important instrument in science and technique applications during the recent years. The advantage of Walsh functions are primarily due to the efficiency of implementation and signal manipulation. For digital networks, pulse type waveforms like Walsh functions are more suitable than sinusoidal waveforms. The instant Walsh spectrum transforms are very useful in a lot of applications and due to this the fast computation algorithms and special type of processors for the computations represent a high interest.

Key words: instant Walsh spectrum transforms, fast Walsh transform, algorithms for computation of the instant Walsh transform.

In the theory of spectra transforms certain concepts of spectra were established. Walsh spectrum are factors of transformation in this or that system of ordering Walsh functions from sequence of values of an input signal. This Walsh transforms are carried out with values of an input signal (0 ÷ *N*-1), (*N* ÷ 2*N*-1), (2*N* ÷ 3*N*-1) etc. (where $N = 2^n$), i.e. on compound intervals. Number of operations for computation the factors of Walsh transform at use of fast algorithms of calculations are equal to $N\log_2 N$.

Other concept of a spectrum is the power spectrum.

The third concept of a spectrum is a full power spectrum that is invariant to cyclic shift. There are few algorithms for fast computation of the power spectrum, but these types of spectrums haven't technique applications.

However in the theory and many practical applications, it is important to make a Walsh spectrum estimation on a sliding interval, i.e. to carry out calculation of factors of transformation from the sequences made from *N* of values of an input signal, received after each new value of an input signal. Thus, Walsh transforms from sequences made of $0 + N - 1,\ 1 + N,\ 2 + N + 1$ and etc. values of an input signal are carried out.

In the field of harmonic analysis [1] the concept of an instant spectrum, i.e. a spectrum of reflecting property of process time has been entered at present. This concept corresponds to a spectrum on a sliding interval and consequently expediently to enter concept of the instant Walsh spectrum.

If to write down Walsh transform from a vector of an input signal

$$\vec{f}_i = [f_i, f_{i+1}, \ldots, f_{i+N-1}]^T$$

at consecutive change of an index ***i*** the elementary definition of an instant Walsh spectrum in a matrix form will have the following appearance

$$\vec{F} = W_N \cdot \vec{f}_i$$

Computation of an instant Walsh spectrum can be carried out by processor of fast Walsh transform of parallel type, and also by a group of processors of consecutive type. For any estimation of an instant Walsh spectrum it is required $N \cdot \log_2 N$ operations.

For processors of fast Walsh transform of parallel type the following sequence of conversion of an input signal is characteristic. Values of an input signal arrive in the input register of the processor and after N values of an input signal are written down, computation process of coefficients of transform begins. Thus, calculations are carry out in parallel form with all *N* values of an input signal on each iteration and Walsh transform coefficients on a processor output turn out simultaneously (in parallel form). To obtain the instant Walsh spectrum it is necessary to produce calculations of Walsh transform coefficients after arrival of each new value of an input signal. The processor of parallel type admits it.

In processors of serial type values of an input signal arrive sequentially and conversion coefficients on an output appear also sequentially. To carry out calculation of the instant spectrum it is necessary to use *N* processors of serial type. Thus in the first processor values of an input signal arrive immediately, in the second with a time delay on one clock period, in the third with a time delay on two clock periods etc. Values of Walsh coefficients on outputs of processors after 2*N* and more clock periods will represent the instant Walsh spectrum.

However, investigating iterative structure of computation of spectral factors from vectors $\vec{f}_i, \vec{f}_{i+1}, \vec{f}_{i+2}$ etc., it is possible to notice that in these transformations there are common intermediate results of calculations. Using these results of calculation of factors of transformation from a vector $\vec{f}_i$ at calculation of factors of transformation from a vector $\vec{f}_{i+1}$ etc. it is possible to reduce necessary number of operations for any new estimation of an instant Walsh spectrum.

In the report the developed graphs and algorithms of calculation of an instant spectrum in whom the common intermediate results of calculations are used that has allowed to reduce number of operations for each new estimation of an instant spectrum to *2(N-1*) are resulted. In the report special processors of fast calculation of an instant spectrum also are offered, their speed and hardware expenses is analyzed. Considered processors allow to receive also a spectrum on compound intervals and to receive factors of transformation in any system of ordering Walsh functions.

References

1. *Харкевич А.А.* Спектры и анализ. Физмат, М.,1962.

УДК 681.3

НЕЛИНЕЙНЫЕ ПОМЕХОУСТОЙЧИВЫЕ КОДЫ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Д.М. БИЛЬДЮК, С.Б. САЛОМАТИН

[1]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
radno@bsuir.by

Рассматриваются криптографические помехоустойчивые коды на базе симметричных алгоритмов шифрования (DES, AES, ГОСТ 28147, СТБ 34.101.31). Произведен сравнительный анализ дистанционных свойств и характеристик декодирования данного класса кодов и двоичных кодов БЧХ.

Ключевые слова: криптографическое преобразование данных, помехоустойчивое кодирование, симметричные алгоритмы шифрования, границы помехоустойчивого кодирования, нелинейный код.

Двоичный помехоустойчивый криптографический код (*R*-код) с параметрами $(n,k,d_{\min})$ определяется как множество отображённых *k*-мерных векторов $\mathbf{a}=(a_0,a_1,\ldots,a_{k-1})\in GF(2^k)$ в другое множество *n*-мерных векторов $\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})\in GF(2^n)$, $k<n$, с минимальным расстоянием Хэмминга среди всех возможных пар кодовых слов – $d_{\min}$ [1]. Отображение реализуется на основе криптографического алгоритма $R_{m,n}$ с ключом шифрования $\mathbf{s}=(s_0,s_1,\ldots,s_{m-1})\in GF(2^m)$, вектором избыточности $\mathbf{v}=(v_0,v_1,\ldots,v_{r-1})\in GF(2^r)$, $r=n-k$, и задается функцией $\varphi(\mathbf{a},\mathbf{s},\mathbf{v}):GF(2^k)\to GF(2^n)$ [1]:

$$\mathbf{c}\leftarrow\varphi(\mathbf{a},\mathbf{s},\mathbf{v}):(\mathbf{a},\mathbf{s},\mathbf{v})\to R_{m,n}(\mathbf{a}\mid\mathbf{v},\mathbf{s}). \tag{1}$$

Параметры *m* и *n* (длина ключа шифрования и длина блока шифрования соответственно) в основном режиме (режиме электронной кодовой книги) криптографического преобразования могут принимать фиксированные значения [1]. Для формирования *R*-кода произвольной длины *n* необходимо использовать режимы криптографического преобразования с обратной связью длины в один бит, вектор инициализации $\mathbf{iv}=(iv_0,iv_1,\ldots,iv_{m-1})\in GF(2^u)$, можно считать частью ключа. Тогда отображение задается функцией $\psi(\mathbf{a},\mathbf{s},\mathbf{v},\mathbf{iv}):GF(2^k)\to GF(2^n)$ [1]:

$$\begin{aligned}
&\mathbf{c}\leftarrow\psi(\mathbf{a},\mathbf{s},\mathbf{v},\mathbf{iv}):(\mathbf{a},\mathbf{s},\mathbf{v},\mathbf{iv})\to(\\
&\quad\mathbf{o}\leftarrow\mathbf{iv};\ \mathbf{a'}\leftarrow\mathbf{a}\mid\mathbf{v};\\
&\quad\textbf{for}\ i\ \textbf{from}\ 0\ \textbf{to}\ n-1\ \textbf{do}\\
&\qquad c_i\leftarrow\left(Rijndael_{m,u}(\mathbf{o},\mathbf{s})\right)_{u-1}\oplus a'_i;\ \mathbf{o}\leftarrow(o_1,o_2,\ldots o_{u-1},c_i);\\
&\quad\textbf{end do};\\
&\quad\textbf{return}\ \mathbf{c};\ ).
\end{aligned} \tag{2}$$

Отображения при помощи функций (1) и (2) задают помехоустойчивый код с близкими дистанционными свойствами [2].

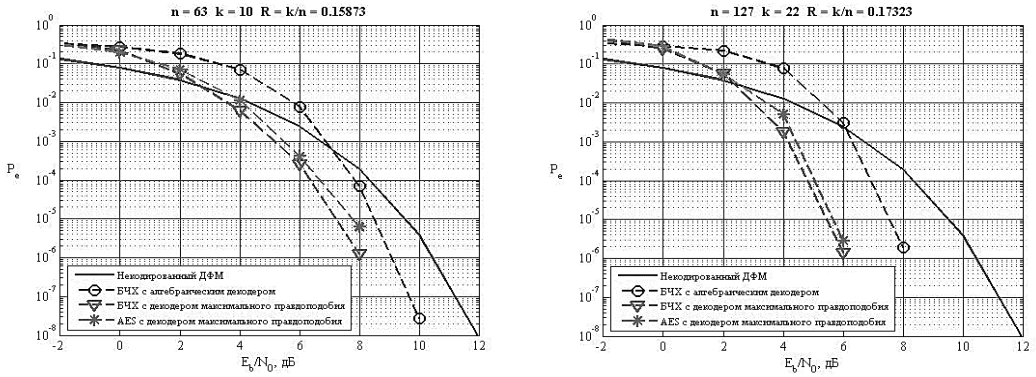
Сравнительный анализ эффективности корректирующих кодов *R* и БЧХ осуществляется с использованием вероятности ошибки на бит P_{eb} информационного слова **a** в зависимости от E_b / N_0 в канале с АБГШ [3] Параметры выбранных для сравнения кодов представлены в табл. 1.

Табл. 1. Параметры *R* и БЧХ кодов

n	7	15	15	15	31	31	31	31	63	63	63	63	63	127	127	127
k	4	5	7	11	6	11	16	21	7	10	16	18	24	8	15	22
$d_{\min}$ (БЧХ)	3	7	5	3	15	11	7	5	31	27	23	21	15	63	55	47
$d_{\min}$ (R)	2	4	2	1	8	3	1	1	19	15	9	7	2	44	32	20

Формирование *R*-кода осуществлялось с использованием функции (2), вектора избыточности **v** и инициализации **iv** использованы с координатами равными нулю. Вектор **s** – случайный.

Примеры результатов моделирования для табл. 1 представлены на рис. 1.



а *б*

Рис. 1. Примеры результатов моделирования с использованием *R* и БЧХ кодов с параметрами (63,10) (*а*) и (127,22) (*б*)

Представленные результаты показывают, что:

– ДМП осуществляет декодирование за границей корректирующей способности помехоустойчивого кода;

– существуют *R*-коды с зависимостью P_{eb} от отношения E_b / N_0 близкой к зависимости БЧХ-кодов при одинаковых параметрах (n,k), в случае использования ДМП (заметим, что $d_{\min}$ *R*-кода меньше чем у БЧХ-кода – см. табл. 1).

Список литературы

1. *Бильдюк Д.М., Саломатин С.Б.* // Декодирование нелинейного помехоустойчивого кода на базе криптографического алгоритма rijndael, Доклады БГУИР №8(70), 2012 – с.75-80.

2. *Фомичев В.М.* // Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н. Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

3. *MacWilliams F.J., Sloane N.J.A.* // The Theory of Error- Correcting Codes. North-Holland, 1977.

УДК 537.874.7

ИССЛЕДОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ СВОЙСТВ ВЛАГОСОДЕРЖАЩИХ ЭКРАНОВ ЭМИ НА ОСНОВЕ ВОЛОКНИСТЫХ ПОЛОТЕН С РАЗЛИЧНЫМИ ПАРАМЕТРАМИ СТРУКТУРЫ

И.А. ГРАБАРЬ, Н.В. НАСОНОВА, KAMEIL IEHAB ABDULJABBAR

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
NasonovaN@bsuir.by

Исследованы электромагнитные характеристики натуральных и синтетических волокнистых полотен с разной поверхностной плотностью и разным влагосодержанием в диапазоне СВЧ.

Ключевые слова: поверхностная плотность, экран электромагнитного излучения, тканые материалы из натуральных и синтетических волокон.

Применение экранов на основе материалов, содержащих воду или водные растворы, способствует снижению электромагнитных излучений. Водосодержащие ЭМИ экраны используются в качестве технических средств защиты от утечки информации по электромагнитному каналу, а также как средство защиты биологических объектов в СВЧ диапазоне. В настоящее время разрабатываются и интенсивно исследуются данные виды экранов.

Основным фактором, влияющим на эффективность экранирования ЭМИ, является концентрация жидкости в объеме пористого материала. Химически чистая вода является диэлектриком с высоким значением диэлектрических потерь в диапазоне СВЧ и может быть использована в качестве компонента композиционного материала.

В данной работе были изучены электромагнитные свойства экранов на основе водосодержащих натуральных и синтетических волокнистых полотен с разной поверхностной плотностью и разным водосодержанием.

Исследуемые образцы (табл. 1) в виде пластин размером 350×450 мм, были изготовлены из тканевых и трикотажного полотна с различным объемным содержанием воды.

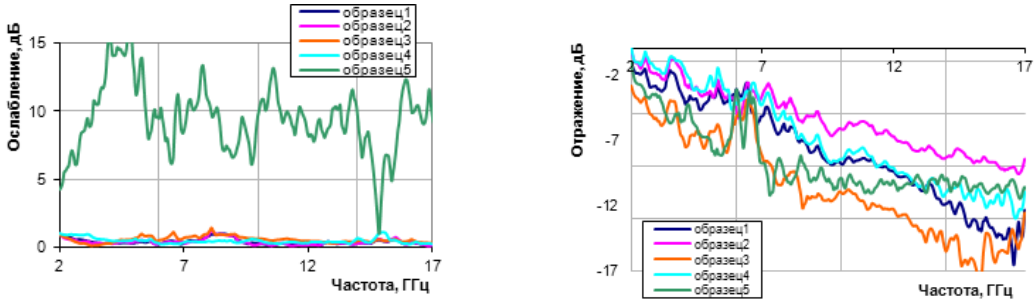
Табл. 1. Описание образцов

№	Толщина, мм	Поверхностная плотность, г/м^2	Материал
1	1,3	208	Хлопкополиэфирное тканое полотно
2	1,6	180	Сетчатое тканое полотно из натуральных волокон
3	1,4	156	Сетчатое тканое полотно из натуральных волокон
4	1,3	208	Синтетическое тканое полотно
5	1,6	1332	Трикотажное полотно

Экранирующие характеристики оценивались измерением частотных характеристик ослабления и коэффициента отражения ЭМИ в диапазоне частот 2…17 ГГц методом скалярного анализа цепей.

При сравнении образцов с водосодержанием 50 % (рис. 1) выявлено, что на частоте 10 ГГц тканые полотна обладают ослаблением ЭМИ 0,3…0,53 дБ, сетчатые

полотна ослабляют ЭМИ на 0,23…0,63 дБ, а трикотажное полотно – до 12,65 дБ. Коэффициент отражения изменился для хлопкополиэфирного полотна до –8,81 дБ, до –6,14 для сетчатой хлопковой ткани, до –10,968 дБ сетчатого полотна из синтетических тканей, до –8,45 дБ для синтетической ткани и для трикотажного полотна коэффициент отражения изменился до –10,27 дБ.

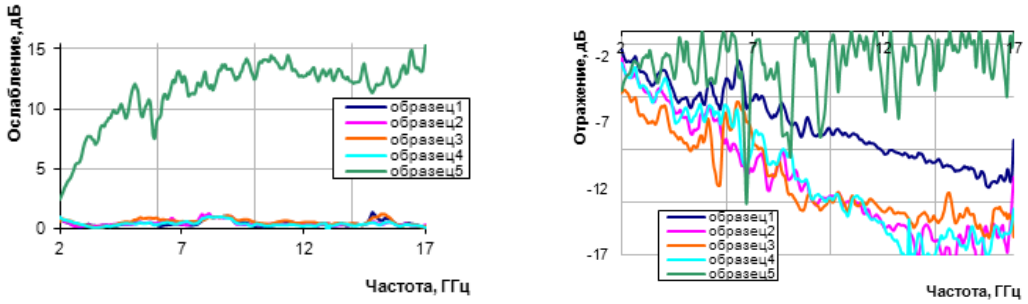


а *б*

Рис. 1. Ослабление (*а*) и отражение (*б*) ЭМИ образцами с влагосодержанием 50 % масс.

При исследовании тканых образцов толщиной 1,3 мм и водосодержанием 70% (рис. 2) выявлено, что на частоте 10 ГГц тканые полотна снижают мощность ЭМИ на 0,21…0,34 дБ, сетчатые полотна обладают ослаблением ЭМИ до 0,35…0,53 дБ, а трикотажное полотно – 6,9 дБ вследствие значительно большего содержания воды в пористой структуре полотна. Коэффициент отражения тканых полотен на металлической подложке составляет -7,66…-12,7 дБ, и –9,5 дБ для трикотажного полотна.

Результаты измерений показывают, что характеристики ослабления и коэффициента отражения для тканых образцов как на основе синтетических, так и натуральных волокон, близки. Это может свидетельствовать, что основная доля ослабления определяется долей капиллярной воды в пространстве между нитями



а *б*

Рис. 2. Ослабление (*а*) и отражение (*б*) ЭМИ образцами с влагосодержанием 70 % масс.

Таким образом, применение влагосодержащих тканых натуральных и синтетических материалов на поверхности металла позволяет получить коэффициент отражения на уровне -7,66…-12,7 дБ, а использование трикотажного полотна позволяет ослабить ЭМИ в среднем на 10…13 дБ вследствие более высокой поверхностной плотности и капиллярной структуры.

УДК 621.794.61:621.357.8:669.71

ВСПЕНЕННЫЕ КОМПОЗИЦИОННЫЕ МАТЕРИАЛЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

АЛЬЛЯБАД ХУССЕЙН МОХАМЕД, АЛЬ-АЛЕМ АХМЕД САИД

Центральное агентство по исследованию и производству
ул. Алькабер, г. Триполи, Ливия
Hussen-1968@tut.by

Специальные материалы позволяют блокировать большинство из технических каналов утечки информации. Композиционные материалы с водными растворами перспективны для экранирования электромагнитного излучения СВЧ-диапазона. Вспененные водные растворы с порошковыми компонентами позволяют получить ослабление ЭМИ в пределах 4…12,5 дБ при коэффициенте отражения –0,1…-8,0 дБ в диапазоне частот 8,0…11,5 ГГц при толщине вспененной основы 5 мм.

Ключевые слова: защита информации, композиционные материалы, эффективность экранирования, вспененные материалы.

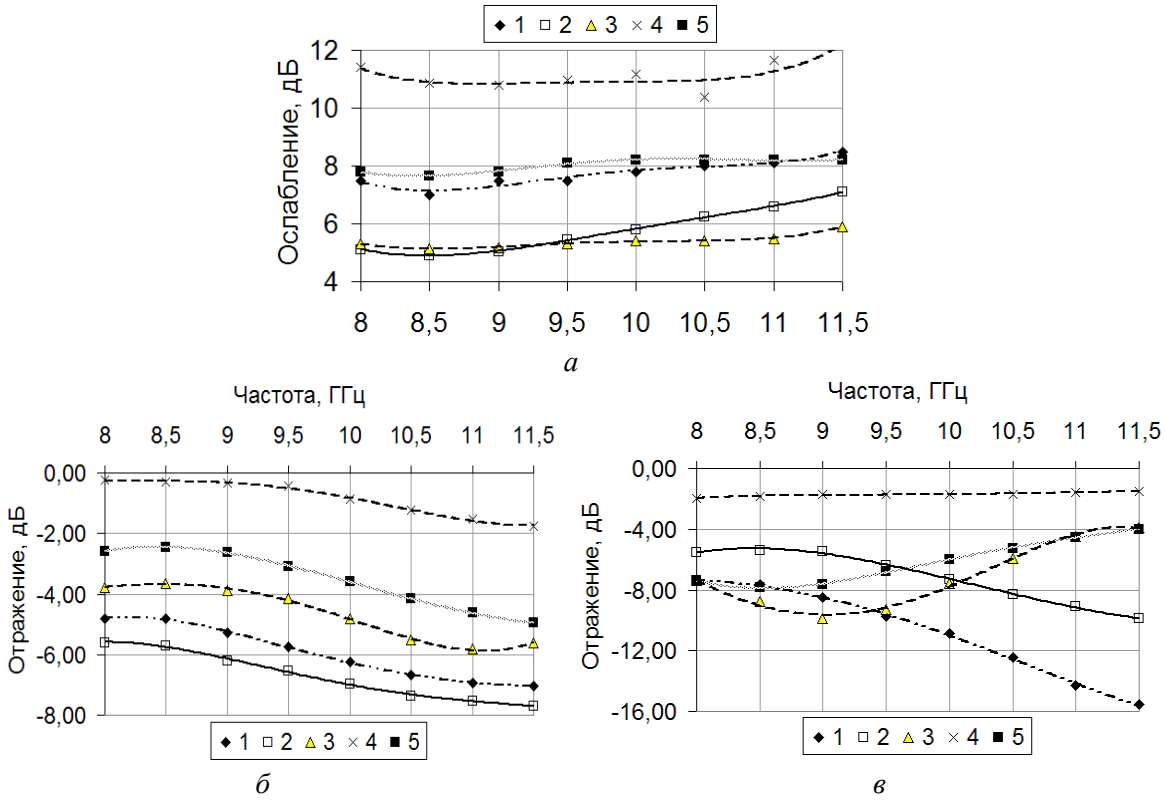
По физической природе носителя наиболее уязвимыми с точки зрения утечки информации, являются электромагнитные, визуально-оптические и тепловые технические каналы утечки информации, что связано с возможностью скрытого получения информации о защищаемых объектах независимо от расстояния.

Эффективным методом снижения уровня информационных сигналов является экранирование их источников, которое заключается в ограничении распространения электромагнитных волн в определенную область пространства путем рассеяния, переотражения энергии электромагнитных колебаний и преобразования ее в тепловую энергию в экранирующих материалах с резистивными, диэлектрическими или магнитными потерями.

Анализ существующих конструкций экранов электромагнитного излучения (ЭМИ) показывает, что эффективность экранирующих устройств определяется электрическими и магнитными свойствами материала экрана, конструкцией экрана, его геометрическими размерами и частотой излучения.

Использование законсервированных водных растворов в конструкциях экранов ЭМИ позволяет повысить широкодиапазонность их эксплуатации в СВЧ-области, управляемо изменять оптические характеристики их поверхности. Влагосодержащие порошкообразные материалы в различных технологических наполнителях, красках достаточно устойчивы к низким (до -30°С) и высоким (до +100°С) эксплуатационным температурам и могут быть нанесены на любые поверхности и элементы конструкций.

Исследовалась эффективность экранирования ЭМИ жидкостными вспененными материалами, синтезированными по предложенной методике введения водных наполнителей, содержащих порошкообразные мелкодисперсные силикагели, шунгит, диоксид титана, хлористый натрий, размещаемых в пространственных каркасах жидкости. Для снижения массогабаритных характеристик защитных экранов предложено использовать в качестве матриц экранов вспененные среды, формирующие пространственную дисперсную структуру различных жидкостей.



1 – водный вспененный раствор, 2 – водный вспененный раствор с порошком силикагеля 7:3 (об.), 3 – водный вспененный раствор с порошком шунгита 7:3 (об.), 4 – водный вспененный раствор с порошком диоксида титана 7:3 (об.), 5 – водный вспененный раствор NaCl

Рис. 1. Частотные зависимости ослабления ЭМИ (*а*) композиционными материалами со вспененными водными растворами и порошками различного состава и коэффициент отражения образцов (*б*) и многослойной конструкции с металлическим отражателем (*в*)

Использование вспененных водных растворов предоставляет возможность получения изделий с различными параметрами структуры, а также сложной формы для использования их в качестве экранов ЭМИ. Результаты исследований влияния состава наполнителя на экранирующие характеристики водосодержащих материалов показывают, что в диапазоне частот 8,0…11,5 ГГц при толщине вспененной основы 5 мм ослабление ЭМИ колеблется в пределах 4…12,5 дБ при коэффициенте отражения – 0,1…-8,0 дБ.

Продолжаются исследования по снижению коэффициента отражения ЭМИ за счет использования гигроскопичных водных растворов органических и неорганических соединений, что приводит к повышению концентрации воды, увеличению проводимости и диэлектрической проницаемости раствора. Многослойная конструкция, в которой в качестве второго слоя установлена металлическая фольга, позволяет повысить эффективность ослабления ЭМИ до 40 дБ при изменении частотной зависимости коэффициента отражения вследствие неоднородной структуры компонентов поглощающего материала в пределах -15,6…-12,1 дБ.

УДК 681.586.712:546.214

СЕЛЕКТИВНЫЕ ГАЗОВЫЕ СЕНСОРЫ НА МИКРОПРОФИЛИРОВАННЫХ ПОДЛОЖКАХ ИЗ АНОДНОГО ОКСИДА АЛЮМИНИЯ

Н.И. МУХУРОВ, С.В. ДЕНИСЮК, О.Н. КУДАНОВИЧ, Э.Э. КОЛЕСНИК

Институт физики Национальной Академии наук Беларуси
пр-т Независимости, 68, г. Минск, 220072, Республика Беларусь
s.denicuk@dragon.bas-net.by

Высокая термическая стабильность и нанопористая структура анодного оксида алюминия предопределяют его использование в качестве перспективного конструкционного материала газовой сенсорики. Уникальные возможности анодной алюмооксидной технологии позволяют формировать в одном технологическом цикле один, два и более изолированных чувствительных элемента на одной диэлектрической подложке, тем самым повышая функциональные возможности полупроводниковых газовых сенсоров.

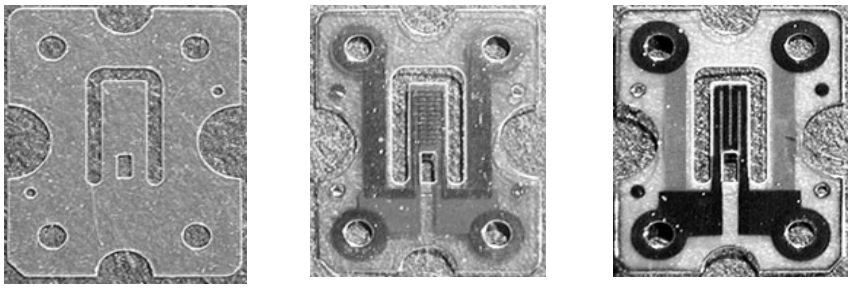
Ключевые слова: газовые сенсоры, диэлектрическая подложка, анодный оксид алюминия, рабочая область.

Широкая номенклатура химических сенсоров газового анализа разных типов и конструкций реализуется на основе наиболее распространённой в микроэлектронике кремниевой технологии. Однако в ряде случаев работа сенсора сопряжена с высокими температурами. Это накладывает ограничение на использование кремния, малопригодного в качестве конструктивного материала при температурах выше 450 °С. В данных условиях более перспективно использование оксида алюминия. В лаборатории микроэлектроники, механики и сенсорики Института физики НАН Беларуси разработана технология формирования тонкопленочных диэлектрических подложек с микропрофилированием произвольной конфигурации из оксида алюминия, получаемого электрохимическим окислением [1].

Создание подложек основано на процессе анодного окисления алюминия. Получаемый аморфный Al_2O_3 при нагреве выше 800 °С испытывает полиморфные превращения, переходя в одну из поликристаллических метастабильных фаз. Как показали исследования, для газовых сенсоров наиболее пригодна γ-фаза Al_2O_3, поскольку она стабильна в диапазоне до 950 °С в течение тысяч часов. Основные тонкопленочные проводящие материалы сенсорики (золото, платина, нихром) обладают удовлетворительной адгезией к оксиду алюминия. Специфической особенностью анодного Al_2O_3 является самоорганизующаяся нанопористая структура, которая позволяет получать детали с планарными и объемными элементами сложной конфигурации с прецизионной точностью (клин травления порядка 0,01% при толщинах в сотни микрометров).

Формирование конфигурации подложки осуществляться стандартными фотолитографическими средствами, используемыми в микроэлектронике, и может проводится на разных этапах технологического процесса: при анодировании алюминия либо травлением оксида алюминия. Разработаны несколько конструкций подложек для разных типов сенсоров. На рис. 1 показана универсальная подложка полупроводникового адсорбционно-резистивного газового сенсора [2] с одной рабочей областью. Рабочая область расположена на консольной части подложки и отделена от остального массива сквозными щелями за исключением перемычек, расположенных параллельно по углам одной из ее сторон, с целью снижения механических деформаций вследствие термического расширения материала подложки и увеличения срока службы сенсора. Кроме

этого, локализация рабочей области уменьшает затраты энергии на нагрев, что особенно важно для переносных устройств. Такой подход позволяет снизить энергопотребление сенсора до величин менее 1 мВт/°С.



а *б* *в*

Рис. 1. Универсальная подложка газового сенсора, выполненная из γ-Al_2O_3 (*а*), поверхность подложки с чувствительным слоем и системой информационных электродов (*б*), поверхность подложки с тонкопленочным нагревателем в виде меандра (*в*)

Для анализа газовых смесей с двумя неизвестными компонентами в реальном времени предложена конструкция адсорбционно-резистивного газового сенсора на основе оксидов переходных металлов с двумя рабочими областями (рис. 2). Обе рабочие области консольного типа отделены от остальной подложки сквозными щелями, образуя локализованные зоны нагрева. В зависимости от конкретной задачи по детектированию газов материалы обеих чувствительных пленок могут быть одинаковыми либо разными. В первом случае для достижения относительной селективности используются различные температуры рабочих областей. Во втором – различия в температурах рабочих областей дополняются отличающимися характеристиками используемых в качестве чувствительных элементов оксидов металлов.

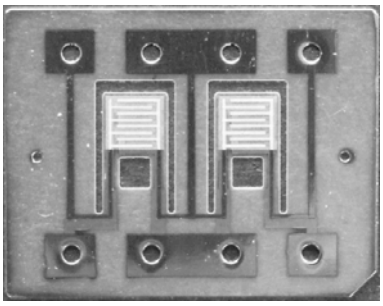


Рис. 2. Адсорбционно-резистивный газовый сенсор с двумя чувствительными областями

Применение анодного оксида алюминия в качестве материала диэлектрической подложки позволяет формировать несколько чувствительных элементов в одном сенсоре. Это дает возможность одновременно и селективно детектировать большее количество компонентов в сложных газовых смесях с помощью одного прибора.

Список литературы

1. *Лыньков Л.М., Мухуров Н.И*. Микроструктуры на основе анодной алюмооксидной технологии. Минск, 2002.

2. *Мухуров Н.И, Ефремов Г.И., Куданович О.Н.* Устройства микромеханики и микросенсорики на нанопористом оксиде алюминия. Минск, 2005.

3. *Мухуров Н.И., Денисюк С.В., Куданович О.Н.* Адсорбционно-резистивный газовый сенсор / Заявка на полезную модель u20130926 от 13.11.2013.

УДК 621.382.001.63

ДЕТЕКТОР ИОНИЗИРУЮЩИХ И УЛЬТРАФИОЛЕТОВЫХ ИЗЛУЧЕНИЙ

И.В. ГАСЕНКОВА[1], Л.М. ЛЫНЬКОВ[2], Н.И. МУХУРОВ[1], Я.М. ВАХИОХ[2]

[1]Государственное научное учреждение "Институт физики имени Б.И. Степанова Национальной академии наук Беларуси"
пр-т Независимости, 68, г. Минск, 220072, Республика Беларусь
gasenkova@inel.bas-net.by

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Сенсор ионизирующих и ультрафиолетовых излучений сформирован на подложках из анодного оксида алюминия с периодической системой микроотверстий, заполненных чувствительными к ионизирующему излучению сцинтилляторами. На одной из поверхностей подложки размещен фотоприемник, а на противоположной − чувствительное к ультрафиолетовым излучениям тонкопленочное покрытие. Сенсор может быть использован для контроля радиационной обстановки и уровня ультрафиолетовых излучений.

Ключевые слова: сенсор ионизирующих и ультрафиолетовых излучений, конструкция, подложки из анодного оксида алюминия.

Вопросы охраны окружающей среды имеют первостепенное значение для жизнедеятельности человечества. Среди них важнейшими являются обнаружение и контроль радиационных и ультрафиолетовых излучений. В связи с этим, возможность оценки одновременно пороговых уровней ионизирующих и ультрафиолетовых излучений позволяет в одном сенсоре реализовать функции чувствительного элемента с широкими функциональными возможностями.

Регистрация воздействия и последующие измерения ионизирующих излучений (ИИ) возможны с применением следующих методов, использующих оценку характеристик сред: ионизационный, сцинтилляционный, химический, фотографический, тепловой или калориметрический. С использованием перечисленных методов обнаружения ИИ изготавливаются различные детекторы этих излучений, которые являются одной из трех составных частей дозиметрических приборов: чувствительный элемент (детектор) излучений − первичный преобразователь − регистрирующая система.

Детектор ионизирующих излучений – чувствительный элемент средства измерений, предназначенный для регистрации ионизирующего излучения, функционирование которого основано на явлениях, возникающих при прохождении ионизирующего излучения через вещество (рабочую среду детектора). Детектор ультрафиолетовых излучений – чувствительный элемент средства измерений, предназначенный для регистрации ультрафиолетового излучения, функционирование которого основано на явлениях, возникающих при прохождении ультрафиолетового излучения через вещество (рабочую среду детектора).

Один из простейших вариантов конструкции детектора радиоактивного излучения включает подложку из полиэфирных смол с внедренными частицами фотолюминесцирующего соединения [1]. В фотоприёмнике происходит преобразование излучения в импульс тока, усиление его и, при необходимости, запись регистрирующей аппаратурой. Однако такой детектор радиоактивного излучения не достаточно чувствителен, имеет узкий рабочий диапазон регистрации ионизирующих излучений, весьма чувствителен к изменению характеристик окружающей среды: температура, уровень солнечного и ионизирующих излучений. Так как материал несущей подложки (пластик) под

действием рентгеновского излучения разрушается, такие индикаторы не могут быть многократными и долговечными.

Для повышения чувствительности, стабильности и расширения рабочего диапазона при минимальных массогабаритных характеристиках нами предложен конструктивный вариант детектора с расширенными функциональными возможностями за счет дополнительной чувствительности к ультрафиолетовым излучениям при сохранении минимальных массогабаритных характеристик [2]. Детектор (рис. 1) содержит фотоприемник 3, размещенный на одной из поверхностей диэлектрической подложки 1 с периодической системой отверстий 2, заполненных не полностью чувствительным к ионизирующим излучениям частицами люминесцирующего вещества 4. Части отверстий, обращенные к источнику ультрафиолетового излучения 7, заполнены до поверхности чувствительными к ультрафиолетовому излучению частицами люминесцирующего вещества 5. Дополнительно на этой поверхности подложки сформировано тонкопленочное покрытие 6 из того же люминесцирующего вещества.

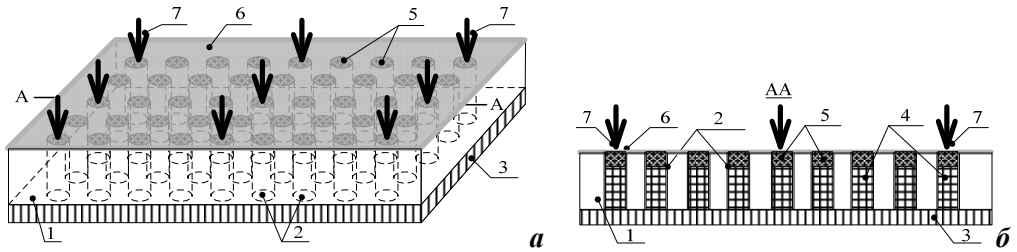


Рис. 1. Детектор ионизирующих и ультрафиолетовых излучений: общий вид (а), поперечное сечение (б), 1 – диэлектрическая подложка, 2 – отверстия, 3 – фотоприемник, 4 – частицы люминесцирующего от рентгена компонента, 5 – частицы люминесцирующего от ультрафиолета компонента, 6 – тонкопленочное покрытие, чувствительное к ультрафиолету, 7 – источник ультрафиолетовых излучений.

За счет малых размеров частиц сцинтиллятора (от единиц до сотен нанометров), его разного состава и чувствительности к ионизирующим и ультрафиолетовым излучениям в широком диапазоне энергий, достигается расширение функциональных возможностей сенсора. Заполнение в верхней (на рис. 1) части отверстий частицами люминесцирующего от ультрафиолета компонента и формирование на поверхности диэлектрической подложки, противоположной фотоприемнику тонкопленочного покрытия, чувствительного к ультрафиолету, позволяют воспринимать сенсором как рентгеновское, так и ультрафиолетовое излучения.

При воздействии ионизирующих излучений поток частиц или квантов возбуждает атомы люминесцирующей от рентгена компоненты, и они испускают фотоны в видимой области спектра. Это излучение регистрируется фотоприёмником, преобразуется в электрический ток, усиливается и отображается регистрирующей системой. При воздействии ультрафиолетовых излучений возбуждаются атомы чувствительных к люминесцирующей от ультрафиолета компоненты. Они испускают фотоны в видимой области спектра, которые фиксируются визуально по изменению окраски поверхности диэлектрической подложки, обращенной к источнику ультрафиолетового излучения.

Список литературы

1. Детектирующий радиацию пластик. [Электронный ресурс]. – Режим доступа: http://www.nirs.go.jp/ENG/press/06_29.pdf, http://www.membrana.ru/particle/16724.

2. *Лыньков Л.М, Мухуров Н.И., Гасенкова И.В., Вахиох Я.М.* Детектор ионизирующих и ультрафиолетовых излучений / Пат. РБ №9551.

УДК 004.7:65.012.8

ОСОБЕННОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ИХ УЯЗВИМОСТИ

И.В. РУСАКОВ[1], А.М. ПРУДНИК[2]

[1]ООО «Исток истины»
ул. Геологическая, 117, к. 1, г. Минск, 220138, Республика Беларусь
IstokIstin@tut.by

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
aleksander.prudnik@bsuir.by

Приводится обоснование разработки, а также практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) для государственных учреждений в соответствии со стандартом СТБ ISO/IEC 27001:2011 «Системы менеджмента информационной безопасности. Требования».

Ключевые слова: защита информации, недекларированные возможности, уязвимость.

Для обеспечения конфиденциальности, целостности и доступности информации необходимо обеспечивать функционирования информационных систем, которые создают, хранят и передают данную информацию.

Различают следующие способы получения несанкционированного доступа к информации:

– подслушивание разговоров в помещении или автомашине с помощью предварительно установленных «радиожучков» или диктофонов;

– контроль телефонов, телефонных и прочих линий связи, радиотелефонов и радиостанций;

– дистанционный съём информации с различных технических средств, в первую очередь, с мониторов и печатающих устройств компьютеров и другой электронной техники;

– облучение оконных стекол в помещении, где ведутся «интересные разговоры» или, например, направленное радиоизлучение, которое может заставить «откликнуться и заговорить» детали в телевизоре, в радиоприемнике или другой технике;

– использование недокументированных возможностей в технических и информационных системах (установка расположения, прослушивание).

Одним из основных направлений специальной защиты является поиск техники подслушивания или поисковые мероприятия. В системе защиты объекта поисковые мероприятия выступают как средства обнаружения и ликвидации угрозы съема информации.

Под безопасностью информационной системы подразумевается ее защищенность от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации. Другими словами вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения или уничтожения.

Если взять модель, описывающую любую управляемую информационную систему, можно предположить, что возмущающее воздействие на нее может быть случай-

ным. Именно поэтому, рассматривая угрозы безопасности информационным системам, следует сразу выделить преднамеренные и случайные возмущающие воздействия.

Средства защиты информации могут быть выведены из строя, например из-за дефектов аппаратных средств или уязвимости используемых алгоритмов. Также существенное отрицательное воздействие на защищенность информации могут оказать действия персонала, что влечет за собой снижение эффективности защиты при любых других благоприятных условиях. Кроме этого в программном обеспечении могут возникать непреднамеренные ошибки и другие сбои информационной системы. Все это негативно влияет на эффективность защиты информации любого вида информационной безопасности, который существует и используется в информационных системах.

Защита информации от компьютерных вирусов предполагает программно-аппаратные средства защиты информации, которые предотвращают несанкционированное действие вредоносных программ, пытающихся завладеть данными и выслать их злоумышленнику, либо уничтожить информацию базы данных.

Задача защиты информации заключается в том, чтобы усложнить или сделать невозможным проникновение к данным, ради чего взломщики в своих противоправных действиях ищут наиболее достоверный источник секретных данных. А так как хакеры пытаются получить максимум достоверных секретных данных с минимальными затратами, то задачи защиты информации — стремление запутать злоумышленника: служба защиты информации предоставляет ему неверные данные, защита компьютерной информации пытается максимально изолировать базу данных от внешнего несанкционированного вмешательства.

Защита компьютерной информации для взломщика — это те мероприятия по защите информации, которые необходимо обойти для получения доступа к сведениям. Архитектура защиты компьютерной информации строится таким образом, чтобы злоумышленник столкнулся с множеством уровней защиты информации: защита сервера посредством разграничения доступа и системы аутентификации пользователей и защита компьютера самого пользователя, который работает с секретными данными. Защита компьютера и защита сервера одновременно позволяют организовать схему защиты компьютерной информации таким образом, чтобы взломщику было невозможно проникнуть в систему, пользуясь столь ненадежным средством защиты информации в сети, как человеческий фактор. То есть, даже обходя защиту компьютера пользователя базы данных и переходя на другой уровень защиты информации, хакер должен будет правильно воспользоваться данной привилегией, иначе защита сервера отклонит любые его запросы на получение данных и попытка обойти защиту компьютерной информации окажется тщетной.

Сегодня для реализации эффективного мероприятия по защите информации требуется не только разработка средства защиты информации в сети и разработка механизмов модели защиты информации, а реализация системного подхода или комплекса защиты информации — это комплекс взаимосвязанных мер. Данный комплекс, как правило, использует специальные технические и программные средства для организации мероприятий защиты информации. Однако нельзя исключать и человеческий фактор, что также необходимо предусматривать при защите информации.

Кроме того, сегодня разработаны и имеют место некоторые модели защиты информации, которые содержат нормативно-правовые акты и морально-этические меры защиты информации и противодействия атакам извне, что необходимо совершенствовать и дополнять с развитием научно-технического прогресса.

УДК 004.353.2

МОДЕЛИРОВАНИЕ ВЗАИМОДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ В ОБЛАСТИ 25-60 ГГц С МАССИВАМИ ОРИЕНТИРОВАННЫХ УГЛЕРОДНЫХ НАНОТРУБОК

А. АТДАЕВ, А.Л. ДАНИЛЮК, С.Л. ПРИЩЕПА

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Приводятся результаты моделирования поглощающих свойств экранов электромагнитного излучения на основе массивов углеродных нанотрубок с распределенными ферромагнитными наночастицами.

Ключевые слова: углеродная нанотрубка, нанокомпозит, СВЧ излучение, магнитная проницаемость.

Среди большого многообразия нанокомпозитных материалов, используемых в качестве экранов электромагнитного излучения, углеродосодержащие материалы привлекают в последнее время большой интерес. В первую очередь интерес вызван оригинальными свойствами углеродной матрицы и каталитических ферромагнитных наночастиц, распределенных по объему массива углеродных нанотрубок. В данной работе проводится моделирование поглощающих свойств нанокомпозита на основе массивов углеродных нанотрубок с распределенными наночастицами железа и цементита.

Приведены результаты моделирования коэффициентов отражения и поглощения электромагнитного излучения (ЭМИ) сверхвысокочастотного диапазона 25-60 ГГц массивами вертикально ориентированных углеродных нанотрубок (УНТ), содержащими ферромагнитные наночастицы железа и цементита.

Определение коэффициентов отражения и поглощения ЭМИ массивом УНТ проведено с помощью модели, учитывающей как магнитных свойств наночастиц, так и проводящих, структурных и магнитных свойств углеродной среды (включая намагниченность углеродной подсистемы), а также наличие переходной оболочки между наночастицами и УНТ, которая характеризуется соответствующим импедансом [1]. Рассчитаны коэффициенты отражения и поглощения, проведено сравнение с соответствующими экспериментальными данным для диапазона 25-40 ГГц.

Получены частотные зависимости коэффициентов отражения и поглощения ЭМИ массивами УНТ, установлена их взаимосвязь с электропроводящими и магнитными свойствами массива УНТ и магнитных наночастиц.

Показано, что значение коэффициента отражения в диапазоне 25-40 ГГц составляет порядка -10 дБ, а значение коэффициента прохождения – порядка -40 дБ, которые слабо уменьшаются с ростом частоты. В диапазоне 40-60 ГГц расчетные значения характеризуются нелинейными зависимостями от частоты, что связано с существованием ферромагнитного резонанса наночастиц в этой области.

Проведено моделирование зависимостей магнитной проницаемости массива углеродных нанотрубок в частотной области 25-60 ГГц.

Приведены результаты моделирования комплексной магнитной проницаемости массива вертикально ориентированных углеродных нанотрубок (УНТ), содержащих ферромагнитные наночастицы железа и цементита в частотном диапазоне 8-40 ГГц.

Определение комплексной магнитной проницаемости проведено с помощью модели для разупорядоченного наноструктурированного композита, которая учитывает магнитную и диэлектрическую проницаемости ферромагнитных наночастиц, магнитную и диэлектрическую проницаемости углеродной матрицы, объемную долю наночастиц, их размер, импеданс резистивной оболочки, окружающей наночастицы, а также резонансную частоту ферромагнитного резонанса (ФМР) системы ферромагнитных наночастиц, удельную проводимость массива УНТ.

Расчеты проведены для следующих параметров нанокомпозита: размер наночастиц 30-50 нм, относительная магнитная проницаемость матрицы (4±2)+i(0.5±0.2), относительная магнитная проницаемость наночастиц 7±3+i(0.5±0.2), объемная концентрация наночастиц 5-10%, частота ФМР – 42 ГГц, удельная проводимость массива 100-120 $(\text{Ом м})^{-1}$.

Показано, что магнитная проницаемость массива УНТ в диапазоне 25-40 ГГц частотные зависимости реальной и мнимой частей магнитной проницаемости нанокомпозита являются немонотонными. Полученные результаты говорят о наличии магнетизма углеродной подсистемы, который вероятно носит индуцированный характер.

В диапазоне 40-60 ГГц частотные зависимости реальной и мнимой частей магнитной проницаемости носят резонансный характер.

Проведено моделирование зависимостей диэлектрической проницаемости массива углеродных нанотрубок в частотной области 25-60 ГГц. Установлено, что в области 25-40 ГГц реальная часть диэлектрической проницаемости практически не меняется, а комплексная спадает с ростом частоты. В области 40-60 ГГц с ростом частоты уменьшается также и реальная часть диэлектрической проницаемости нанокомпозита.

Список литературы

1. *Labunov V.A., Danilyuk A.L., Prudnikava A.L.* et al Microwave Absorption in Nanocomposite Material of Magnetically Functionalized Carbon Nanotubes / Journal of Applied Physics, Vol. 112, No.2, P.024302(1-9), 2012.

УДК 621.391.82

МАСКИРОВАНИЕ ВИДЕОСИГНАЛА АДАПТИВНЫМ ВИДЕОШУМОВЫМ СИГНАЛОМ С РАЗРУШЕНИЕМ СИНХРОИМПУЛЬСОВ

В.К. ЖЕЛЕЗНЯК[1], А.В. БАРКОВ[2]

[1]*Полоцкий государственный университет*
ул. Блохина, 29, г. Новополоцк, 211440, Республика Беларусь
vlad@psu.by

[2]*Полоцкий государственный университет*
ул. Блохина, 29, г. Новополоцк, 211440, Республика Беларусь
a.barkou@tut.by

Восстановление видеосигналов основано на их синхронности и возможности накопления видеокадров. Для восстановления видеокадра в шумах необходимо обнаружить его элементы. Метод маскирования от утечки видеосигналов систем передачи и обработки видеоинформации маскирует синхроимпульсы восстановленными их противофазной компенсацией, маскирование информационной составляющей видеокадров реализуется синхронным и адаптивным видеошумовым кадром.

Ключевые слова: защита видеосигнала, восстановление и компенсация синхроимпульсов, маскирование видеосигналов, статический видеокадр.

Меры защиты информации формируют в зависимости от условий применения видеосистемы. Формирование требований защиты информации вне зависимости от источников излучения, среды распространения, средств извлечения информации, места и времени эксплуатации снижает рациональность мер защиты информации [1]. Меры защиты информации основаны на ослаблении взаимодействия видеосистемы с системой обнаружения и перехвата. Обеспечение скрытности функционирования информационных систем [1] является непременным условием мер защиты информации.

Анализ литературных источников [2, 3] выявил, что все описанные методы и принципы восстановления основаны на определении параметров синхроимпульсов и накоплении видеокадров для улучшения отношения сигнал/шум (ОСШ). Синхронное накопление (периодическое усреднение) является эффективным методом для увеличения ОСШ периодического сигнала. Накопление видеосигнала возможно при условиях [3, с. 96], когда кадровый сигнал на экране остается стабильным и неизменным в течение времени T, то есть f_vT кадров могут быть накоплены при частоте кадров f_v и её высокой точности. Таким образом, накопление видеосигнала возможно при наличии данных синхронизации. Восстановление видеосигнала устанавливается структурой и параметрами видеокадров в шумах.

Анализ методов общих принципов восстановления видеосигналов [2, 3] и определил два основных направления активного маскирования видеосигналов:

– разрушение сигналов методом компенсации, при котором уровень маскируемого сигнала на выходе канала утечки близок к нулю [1];

– маскирование помехой сигнала, значительно превышающей его уровень в канале утечки.

Анализ современных методов активного маскирования выявил необходимость учёта тонкой структуры видеосигнала: тонкая структура видеосигналов обусловливает необходимость анализировать как узкополосную составляющую, обусловленную нали-

чием синхросигналов и широкополосную информативную составляющую видеосигнала. Особенности видеосигналов требуют создания методов защиты, которые учитывают статические (неподвижные) и динамические (подвижные) параметры видеокадров. Предложено для надёжного маскирования формировать синхронные статические видеошумовые кадры.

Для эффективного маскирования видеосигнала с учетом его особенностей, обусловленных его форматом, предложено разрушать синхроимпульсы видеосигнала в КУИ; адаптивно маскировать информативную составляющую видеокадра синхронными цветными видеошумовыми кадрами.

Метод разрушения синхроимпульсов основан на том, что синхроимпульсы восстанавливают из видеосигнала в КУИ обработкой в частотной области методом, предложенным авторами [5] и разрушают их в КУИ противофазной компенсацией.

Предложен и обоснован метод маскирования от утечки видеосигналов систем передачи и обработки видеоинформации. Восстановленные синхроимпульсы позволяют сформировать маскирующие статический (неподвижный) видеошумовой цветной кадр для адаптивного маскирования сигнального статического (неподвижного) и динамического (подвижного) видеокадра. Это позволило улучшить защищенность видеосигнала пропорционально отношению корня квадратного число видеокадров к количеству смен шумового видеокадра, так при накоплении видеосигнала со среднестатистической длительностью 30 с при n=750 и k=6 улучшает в 11 раз защищенность по отношению сигнал/шум. Смена шумовых видеокадров повышает эффективность маскирования.

Список литературы.

1. *Железняк В.К.* Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006.

2. *Markus G.K*. Security Limits for Compromising Emanations [Electronic resource] / Computer Laboratory, University of Cambridge,. 15 JJ Thomson Avenue, Cambridge CB3 0FD. Mode of access : www.cl.cam.ac.uk/~mgk25/ches2005-limits.pdf. – Date of access : 30.09.2013.

3. *Suzuki, Y., Akiyama Y.* Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals / Proc. 2010 IEEE Int. Symp. EMC, 2010.

4. *Markus G K.* Compromising emanations: eavesdropping risks of computer displays. Chapter 5: Emission limits. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.

5. *Железняк В.К, Барков А.В*. Способ обнаружения периодической импульсной последовательности и оценки ее периода / Патент РБ № 17138.

УДК 621.372.037.372

ИЗМЕРИТЕЛЬНЫЕ СИГНАЛЫ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧИ В ЦИФРОВОЙ ФОРМЕ

Д.С. РЯБЕНКО, В.К. ЖЕЛЕЗНЯК

Полоцкий государственный университет
ул. Блохина, 29, г. Новополоцк, 220440, Республика Беларусь
denekor@gmail.com

Обусловленное высокой достоверностью предельное качество передачи речевых сигналов в цифровой форме обладает несомненными преимуществами перед аналоговыми сигналами. Взаимное преобразование цифровых и аналоговых сигналов генерирует новые каналы утечки информации, что усложнило способы их защиты и разработки новых методов и средств оценки защищенности.

Ключевые слова: разборчивость речи, канал утечки информации, пропускная способность.

Критерием оценки защищенности речевого сигнала в цифровой форме от утечки предложено и научно обосновано числовое значение вероятности ошибочного приема бита, соответствующее критерию оценки защищенности речевого сигнала в аналоговой форме – нормированному значению величины разборчивости речи, для которой разработаны современные методы и средства оценки. Многообразие представления цифровых битовых речевых сигналов с основанием кода m и цифровых модулированных (тональных) речевых сигналов (АМн, ЧМн, ФМн, ОФМ, КАМ), потребовало выбрать и обосновать измерительный сигнал, основным требованием к которому является высокая помехоустойчивость и достоверность.

Из анализа литературных источников следует вывод, что современные методы оценки передачи информации исследованы для цифровых каналов с малой вероятностью ошибки, а для «хороших» и «плохих» каналов – по моделям оценки ошибок. Такие методы не могут быть применены для каналов утечки цифровых речевых сигналов, основной особенностью которых является вероятность ошибочного приема бита, близкая к пределу Шеннона. Это обусловливает разработку на новых принципах единых высокопроизводительных методов оценки защищенности цифровых каналов утечки речевой информации по единому критерию для аналоговых и цифровых речевых сигналов.

Критерий оценки защищенности аналогового речевого сигнала от утечки должен адекватно соответствовать критерию оценки защищенности цифрового речевого сигнала от утечки. Предложено критерий оценки защищенности цифровых речевых сигналов установить по вероятности ошибочного приема бита $P_{ош}$.

Используя формулу Шеннона для нормированного значения отношения сигнал/шум, определяют пропускную способность аналогового речевого сигнала. Пропускная способность гауссовского канала C_a определяется шириной полосы сигнала F(Гц) отношением мощности сигнала P_c (Вт) к мощности шума $P_ш$ (Вт) [1]. Данное отношение определено в зависимости от нормированной величине разборчивости речи.

Известно, что при малом отношении сигнал/шум $P_c<P_ш$ для аналогового сигнала из формулы Шеннона значение пропускной способности [2]:

$$C_a = F\log_2 e\cdot\frac{P_c}{P_ш} = 1{,}443\cdot F\cdot\frac{P_c}{P_ш} = 1{,}443\frac{P_c}{N_0} = 1{,}443\Delta\text{, бит/с,} \qquad (1)$$

где C_a – пропускная способность канала, бит/с, F – ширина полосы частот, Гц, $P_c/P_ш$ – отношение мощности сигнала P_c к мощности шума $P_ш$ для аналогового сигнала. $P_c/N_0=\Delta$ – нормативное значение отношения мощности сигнала P_c к спектральной плотности мощности шума N_0.

Для двоичного симметричного дискретного канала пропускная способность канала $C_ц$ вычисляется [1]:

$$C_ц = 1 + P_{ош}\log_2 P_{ош} + (1-P_{ош})\log_2(1-P_{ош}), \text{ бит/с}, \quad (2)$$

По значению пропускной способности $C_ц$ и равенству $C_ц = C_a$ из формулы (2) вычисляют вероятность ошибочного приема бита $P_{ош}$. Нормативным значением оценки защищенности цифровых речевых сигналов следует принять величину вероятности ошибочного приема бита $P_{ош}$, соответствующему нормированному значению величины разборчивости речи [3].

Особенностями каналов утечки цифровых сигналов являются их широкополосность, высокий уровень шумов и несимметричность. Это ограничивает возможности измерительных сигналов при оценке их защищенности в шумах высокого уровня.

Измерительным сигналом для оценки защищенности от утечки речевых сигналов в цифровой форме в виде битовых символов предложен и обоснован сигнал в виде последовательности прямоугольных импульсов типа меандр [4]. Измерительным сигналом для оценки защищенности от утечки модулированных речевых сигналов в цифровой форме предложен и обоснован ортогональный по частоте и квадратурный по фазе модулированный сигнал без разрыва фазы [5].

Применение таких сигналов в качестве измерительных позволило обнаруживать и восстанавливать сигнал в канале утечки информации при воздействии шумов высокого уровня. С учетом свойства несимметричности канала утечки показаны преимущества применения предложенных сигналов в качестве измерительных.

Применение предложенных методов оценки защищенности от утечки речевого сигнала в цифровой форме рекомендуется использовать для оценки защищенности технических каналов утечки речевой информации при ее преобразовании из аналоговой формы в цифровую современными системами передачи данных, а также оценки принятых мер маскирования речевых сигналов.

Список литературы

1. Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема / Под ред. Д.Л. Бураченко. СПб.: изд-во Политехн. ун-та, 2005.

2. Помехоустойчивость и эффективность систем передачи информации / Под общ. ред. А.Г. Зюко. М.: Радио и связь, 1985.

3. *Железняк В.К., Рябенко Д.С.* Способ оценки защищенности от утечки речевого сигнала / Патент РБ № 15588.

4. *Фельдбаум А.А. и др*. Теоретические основы связи и управления. М.: 1963.

5. *Железняк В.К., Дворников С.В.* Основы теории модулированных колебаний: учебное пособие. СПб.: ГУАП, 2006.

УДК 621.383.92

МНОГОКАНАЛЬНАЯ КВАНТОВАЯ СИСТЕМА СВЯЗИ ДЛЯ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

А.О. ЗЕНЕВИЧ[1], А.М. ТИМОФЕЕВ[1], А.Г. КОСАРИ[2],
А.А. ЛИПАЙ[2], Е.В. МОРОЗ[2], В.С. ТОЛКАЧЕВА[2]

[1]*Учреждение образование «Высший государственный колледж связи»*
ул. Ф. Скорины, 8/2, г. Минск, 220114, Республика Беларусь
zao@vks.belpak.by

[2]*Белорусский государственный университет информатики и радиоэлектроники*
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
TAMvks@mail.ru

Применительно к квантовым системам связи предложено устройство, реализующее многоканальную передачу конфиденциальной информации. В сравнении с одноканальными, применение многоканальных квантовых систем связи позволит увеличить скорость передачи информации таких систем за счет того, что все биты кодового слова передаются по одному оптическому волокну на разных длинах волн оптического излучения.

Ключевые слова: квантовая система связи, скорость передачи информации.

В настоящее время для защиты информации, передаваемой по волоконно-оптическим каналам связи, все чаще используются квантово-криптографические системы связи, которые обеспечивают абсолютную защищенность информации [0]. Однако квантово-криптографические системы обладают низкой скоростью передачи информации (СПИ) из-за сложной процедуры обмена данными при передаче секретного ключа (50 Кбит/с). Поэтому в работе [0] предлагается новый подход к защите информации, основанный на создании систем квантовой безопасной связи. Для защиты информации в системах квантовой безопасной связи используется квантово-механический ресурс, то есть каждый бит информации кодируется состоянием фотона. При наличии утечки информации происходит изменение состояния фотона, что обнаруживается санкционированными пользователями. Такие системы позволяют обеспечить такую же защищенность передаваемой информации, как и квантово-криптографические системы, но позволяют повысить СПИ. Для создания систем квантовой безопасной связи используются квантовые информационные системы, содержащие в качестве приемных модулей счетчики фотонов. По результатам выполненных в [0] экспериментальных исследований СПИ квантовых систем связи установлено, что наибольшее значение СПИ составляет 0,8 Мбит/с, что значительно меньше скорости передачи информации, которой обладают современные системы волоконно-оптической связи [0]. Для увеличения СПИ систем связи используется многоканальный подход, реализация которого применительно к квантовым системам связи до настоящего времени развита не в полной мере. В связи с этим целью данной работы являлось разработать многоканальную квантовую систему связи.

Структурная схема устройства, реализующего многоканальную квантовую систему связи, приведена на рис. 1.

Принцип действия устройства заключается в том, что на вход устройства поступает входная последовательность данных. При помощи формирователя слов ФС эта последовательность разбивается на слова, состоящие из i-ого числа бит (символов).

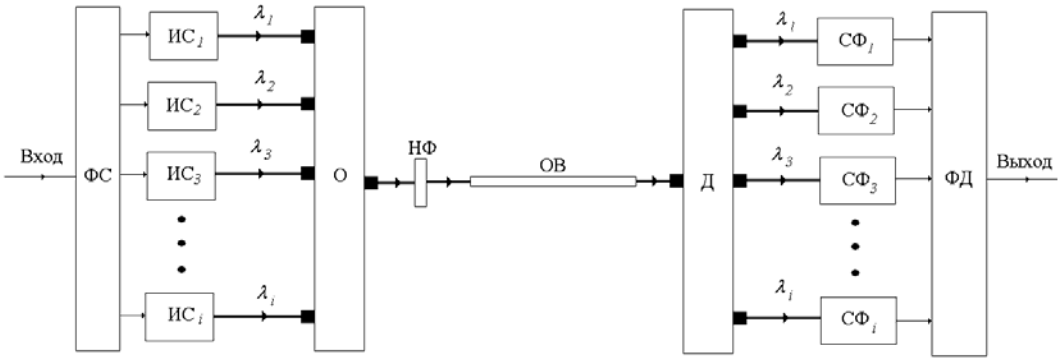


Рис. 1. Структурная схема устройства, реализующего многоканальную квантовую систему для передачи конфиденциальной информации

ФС имеет *i*-ое количество выходов, каждый из которых соединен с отдельным источником оптического излучения $ИС_1 \div ИС_i$, формирующими оптическое излучение со своей длиной волны $\lambda_1 \div \lambda_i$. Далее оптические излучения с различными длинами волн поступают на разные входы оптического смесителя О, объединяющего оптические излучения от всех источников в один оптический сигнал. Этот сигнал ослабляется при помощи нейтрального светофильтра НФ и подается в оптическое волокно ОВ, с выхода которого излучение поступает на диспергирующий элемент Д. Диспергирующий элемент осуществляет спектральную селекцию оптического излучения, поступающего на его вход. В результате на первом выходе диспергирующего элемента формируется оптическое излучение с длиной волны λ_1, на втором выходе – с длиной волны λ_2 и так далее. Оптические излучения с выходов диспергирующего элемента поступают на соответствующие счетчики фотонов $СФ_1 \div СФ_i$, которые регистрируют эти импульсы и подают на формирователь данных ФД, преобразующий данные из параллельного кода в последовательный. Такое устройство, в сравнении с одноканальным, позволяет увеличить СПИ в *i* раз, где *i* − число каналов.

Следует отметить, что основными особенностями рассмотренной многоканальной квантовой системы связи, отличающими ее от систем связи [0] со спектральным уплотнением, являются передача оптической информации маломощными оптическими сигналами, содержащими в среднем один фотон на каждый бит (символ), регистрация этих сигналов посредством счетчиков фотонов, а также возможность обеспечения за счет этого конфиденциальной связи путем введения автоматического контроля вероятности ошибки регистрации.

Таким образом, многоканальные квантовые системы связи, в сравнении с одноканальными, позволили увеличить СПИ квантовых систем связи за счет того, что все биты передаваемого кодового слова передаются по одному оптическому волокну на разных длинах волн оптического излучения.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор №Т13-018).

Список литературы

1. *Килин С.Я.* Квантовая криптография: идеи и практика. Мн. 2007.

2. *Василиу Е.В., Василиу Л.Н.* // Труды Одесского политехнического университета. 2007. вып. 2 (28). С. 1–6.

3. *Зеневич А.О., Комаров С.К., Тимофеев А.М.* // Электросвязь. 2010. № 10. С. 14–16.

4. *Дмитриев С.А. Слепов Н.Н.* Волоконно-оптическая техника: современное состояние и новые перспективы. М., 2010.