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

Литература

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

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

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ В ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

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

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

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

Литература

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

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

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

ТЕСТИРОВАНИЕ СЕТЕВЫХ СКАНЕРОВ УЯЗВИМОСТЕЙ: OPENVAS, NESSUS, RAPID7 NEXPOSE

А.Ф. Жукевич

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

Конфигурация сканирования:

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

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

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

– сканирование производилось с использованием атрибутов доступа.

Результаты сканирования:

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

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

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

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

Литература

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

МЕТОДЫ ОРГАНИЗАЦИИ КОНТРОЛЯ ДОСТУПА ПРИ ОЦЕНКЕ СЕБЕСТОИМОСТИ ИТ-ПРОЕКТОВ

А.Д. Зайков

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

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

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

Литература

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