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

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

Литература

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

ВОПРОСЫ ПРИМЕНЕНИЯ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ

Г.А. Власова, Н.А. Козырев

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

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

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

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

Литература

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

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

СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЦЕНТРАЛИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМАХ

П.Л. Волынец

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

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

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

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

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

Литература

1. Андерсон Дж. Лучшие практики внедрения SAP. 2011

2. Danielle Larocca Signoril. SAP Query Reporting

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

С.А. Ганкевич

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