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

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

Литература

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

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

СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЦЕНТРАЛИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМАХ

П.Л. Волынец

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

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

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

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

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

Литература

1. Андерсон Дж. Лучшие практики внедрения SAP. 2011

2. Danielle Larocca Signoril. SAP Query Reporting

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

С.А. Ганкевич

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

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

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

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

Литература

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

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

Д.О. Гейман

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

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