

## **Литература**

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

## **АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ НА ПЛАТФОРМЕ IOS**

Д.В. Судас

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

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

Т.О. Титовец, Е.В. Моженкова

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

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

## **Литература**

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

## **МЕХАНИЗМ ОПРЕДЕЛЕНИЯ ВЕРОЯТНЫХ СЦЕНАРИЕВ АТАКИ ИНСАЙДЕРА НА ИНФРАСТРУКТУРУ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

А.В. Федорцов

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

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

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

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

#### **Литература**

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

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

Е.И. Шалимо

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

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