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 атоматизированных 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