АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

В.О. Сидорович, А.Е. Варюшина

Практика построения современных СПИ показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений различных источников информации по общей линии связи [1].

В многоканальной СПИ по общему высоко-частотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется уплотнением каналов. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют поднесущими колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется разделением (селекцией) каналов [2].

Литература

1. Принципы многоканальной передачи информации. Элементы теории разделения сигналов [Электронный ресурс]. – 2011. – Режим доступа : http://studopedia.org/8-106652.html – Дата доступа: 26.01.2017.

2. Уплотнение информации в аналоговых системах связи [Электронный ресурс]. – 2017. – Режим доступа: http://studopedia.org/2-74270.html – Дата доступа: 11.03.2017.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИЗАЦИИ ЗДАНИЙ

Д.С. Смоляк, Т.А. Пулко

Одним из частных случаев интернет вещей (физических предметов) (IoT) являются системы автоматизации зданий, такие как системы домашней автоматизации «умный дом», позволяющие автоматизировать ряд рутинных задач и обеспечить контроль и мониторинг использования ресурсов, а также обеспечить владельцу возможность удаленного управления. При построении систем типа «умный дом», рассчитанных на широкого потребителя используются решения, использующие беспроводные протоколы передачи данных. Большое распространение на текущий момент времени получают системы, использующие беспроводные протоколы передачи данных на не лицензируемых радиочастотах, позволяющие использовать оборудование для реализации решения без дополнительных согласований, такие как ZigBee и Z-Wave. В Республике Беларусь телекоммуникационная компания Белтелеком в своей услуге «Умный дом» предлагает решения, рассчитанные на массового потребителя и основанные на беспроводном протоколе ZigBee [1]. Однако, использование беспроводных решений влечет за собой ряд угроз для потенциального потребителя. Например, исследователи из компании Qihoo360 обнаружили возможность перехвата ключей шифрования сетевых сообщений для ряда устройств [2]. Исследователями Eyal Ronen, Colin O'Flynn были обнаружены уязвимости в продукте Philips Hue, позволяющие загрузить вредоносное программное обеспечение в «умную лампочку» [3]. Таким образом, в связи с ростом применения продуктов IoT, следует подвергнуть критической оценке, представленные на рынке решения, оценить уровень их защищенности к различным атакам, а также повысить осведомленность потребителей о возможных последствиях использования небезопасных решений.

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