Разработанный модуль хорошо применять в случае связки с более производительным и дорогостоящим оборудованием, которому будут передавать информацию об активности на том или ином ресурсе.

В ходе работы были усовершенствованы системы безопасности магистральных провайдеров связи от DDoSатак. Предложенный алгоритм настройки сетевого оборудования провайдеров уровня Tier 2-3 обеспечивает быстрое взаимодействие в блокировке атакующих сетей от DDoSатак, а также позволяет проактивно реагировать на изменения в сетевой активноти.

В результате компания получила усовершенствованную магистральную сеть между центрами обработки данных с повышенным уровнем доступности, экономей входящего-исходящего трафика за счет сокращения DDoS атак, высоким уровнем утилизации оборудования за счет своевременного прекращения обработки вредоносного трафика, а также автоматизация работы с приложениями оповещения угроз, и существенное сокращение временных издержек на поиски решений и отражения DDoS атак.

Литература

1. Abliz M. Internet Denial of Service Attacks and Defense // Pittsburgh: University of Pittsburgh Technical Report [Электронныйресурс]. – Режимдоступа: http://www.cs.pitt.edu/

2. Приходько Т.А. Исследование вопросов безопасности локальных сетей на канальном уровне модели OSI [Электронный ресурс]. – Режим доступа: http://ea.donntu.org/

МОДУЛЯЦИЯ ПОЛОЖЕНИЕМ ИМПУЛЬСА В РАДИО ИДЕНТИФИКАТОРАХ ОБЪЕКТОВ

В.Т. Першин, А.Р. Буренков

Весьма перспективным в настоящее время, является использование модуляции положением импульса (Pulse Position Modulation, PPM) в радио идентификаторах объектов, представляющей собою инструмент технологии сверхширокополосной связи (Ultra Wide Band, UWB), идея которой заключается в использовании сверхширокополосного сигнала для передачи информации. В докладе представлены результаты исследования реализации метода PPM для повышения скрытности работы системы с радиочастотными идентификаторами объектов.

По виду воздействия на исходную информацию такой подход заменяет методы криптографического преобразования. Для традиционных средств связи сигналы UWB с PPM не доступны не только к приему, но даже и к определению самого факта своего существования. Поэтому модуляция положением импульса упрощает решение задачи повышения скрытности исходной информации от искажения или подслушивания ее несанкционированным пользователем. Кроме того, важно отметить, что организация криптографического процесса представляет собой значительный объем работы по выполнению многочисленных операций.

Длительность излучаемого моноимпульса может колебаться в пределах 0,2 – 2 нс, а период импульсной последовательности составляет от 10 до 1000 нс. Главные параметры, характеризующие UWB-устройства, – частота повторения коротких импульсов, средняя мощность в пересчете на 1 МГц и пиковая мощность в любой полосе шириной не менее 500 МГц. Важна также относительная ширина полосы, определяемая как отношение необходимой ширины полосы к значению центральной частоты (предполагается, что типичное значение этого параметра должно превышать 0,2).

Образование ряда независимых каналов связи может осуществляться методом временных перескоков, основанном на вводе еще одного дополнительного временного кодирования положения импульсов с помощью последовательности псевдослучайных кодов, обеспечивающих сдвиг импульсов на величины в 10 – 100 раз большие, чем дает модуляция передаваемыми данными. Для выделения сигнала в приемной части должна использоваться такая же последовательность псевдослучайных кодов. В случае применения иной

последовательности, приемник будет открываться в другие временные интервалы и приема информационных импульсов не произойдет. Применение известных ортогональных кодов для управления временными задержками импульсов позволяет создать в одной полосе до 1000 и более дуплексных каналов связи на одной станции.

ФОРМИРОВАНИЕ ГАУССОВСКИХ ИМПУЛЬСОВ ДЛЯ РАДИОЧАСТОТНЫХ РАДИО ИДЕНТИФИКАТОРОВ ОБЪЕКТОВ

В.Т. Першин, Е.Ю. Петрушеня

Обеспечение скрытности радиочастотных идентификаторов объектов с помощью технологии ультраширокополосной связи (Ultra Wide Band, UWB) требует решения задачи генерирования импульсов длительности порядка десятых долей пикосекунды. В докладе сообщается о результатах моделирования таких сигналов в системе MATLAB/SIMULINK. Приведена структурная схема разработанной в системе SIMULINK модели формирования импульса почти гауссовской формы из последовательности коротких прямоугольных импульсов. Обсуждаемая в докладе схема содержит стандартные модули Pulse generator, Transport delay, Derivative delay, Gain, Scope. Приведены результаты выполненного моделирования формирования импульсов для использования в радиочастотных идентификаторах объектов и проводится их обсуждение.

Приведены результаты экспериментального исследования генератора, собранного на диоде со ступенчатым восстановлением и уникальной схемы формирования импульса, которая создает ультраширокополосный импульс гауссовской формы. Чтобы увеличить выходную мощность передатчика, выходы двух идентичных импульсных генераторов соединяют параллельно. Генератор использует обостряющую схему, которая преобразует низкую скорость подъема во времени прямоугольного сигнала в более быстрый, превращая его в гауссовский моноцикл или более высокого порядка производный сигнал, получаемый за счет дополнительной формирующей схемы. Диоды со ступенчатым восстановлением позволяют генерировать импульсы, имеющие фронты длительностью 50…100 пс среднего уровня мощности без дополнительного усиления и с высокой скоростью повторения. Более высокие обратные напряжения приводят к увеличению времени передачи, что проявляется в увеличении длительности выходного импульса.

ПРИОРИТИЗАЦИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАКАХ

А.Н. Прузан, В.Л. Николаенко, А.В. Тихонов

Рассматривается проблема определения приоритетов обработки инцидентов информационной безопасности (ИБ) в облачных вычислениях, которая согласно руководству по обработке инцидентов компьютерной безопасности [1] является одним из важнейших этапов в процессе обработки. При ограниченных ресурсах инциденты не должны обрабатываться по принципу, «первый пришел — первый обработан» [1].

Для определения приоритетов обработки инцидентов ИБ, зафиксированных ПО для оповещения об инцидентах ZABBIX, предлагается все алерты (alert, извещение программы ZABBIX об инциденте) по своей важности разделить на 5 уровней [2]:

– уровень 1, низкий, (информация, information); отметка о таком алерте делается в специальном электронном журнале алертов низкого уровня важности;

– уровень 2, маловажный, (предупреждение, warning); при обработке такого алерта отправляется сообщение о нём на e-mail;

– уровень 3, средний (average); при обработке алерта уровня 3 отправляется сообщение о нём на e-mail и формируется заявка среднего уровня важности (average priority ticket) в программную систему HP Service Manager (HPSM);

– уровень 4, высокий (high); помимо сообщения на e-mail и формирования заявки высокой важности (high priority ticket) в систему HPSM отправляется заказ на выполнение