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

работ по устранению инцидента службам сервиса ИТ-объекта, на котором произошёл инцидент; но заказ этими службами выполняется только в их рабочее время;

– уровень 5, критический (авария, disaster); при обработке такого алерта вместе с сообщением о нём на e-mail формируется заявка критического уровня важности (critical priority ticket) в систему HPSM, но устранение инцидента службами сервиса ИТ-объекта после получения заявки выполняется в любое время суток, в том числе и в выходные дни.

Для оценки действенности предлагаемой приоритизации алертов анализируется их список за ноябрь 2014 года [2].

Литература

1. NIST special publication 800-61 Revision 2. Computer security incident handling guide.

2. *Николаенко В.А., Прузан А.Н., Сечко Г.В., Таболич Т.Г.* Опыт мониторинга инцидентов информационной безопасности в облачных вычислениях // Сб. статей III межд. заоч. НПК «Информационные системы и технологии: управление и безопасность» (декабрь 2014). – Тольятти-Русе: Поволжский гос. университет сервиса в партнёрстве с Русенским университетом «Ангел Кънчев» (Болгария), 2014. С. 209–215.

ПРИМЕНЕНИЕ VPN ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ VOIP

А.А. Антонников, С.Н. Петров

В настоящее время большую популярность приобретают различные сервисы, связанные с пакетной передачей данных по IP протоколу. Одними из наиболее популярных являются сервисы IP-телефонии, определяемые общим стеком VoIP-протоколов. Применение данной технологии позволяет снизить стоимость телефонных соединений при высоком качестве сервиса. Распространение технологии VoIP оказалось сопряжено с проблемами, связанными с защитой речевой и сигнальной информации. Так как технология передачи речевого трафика является частным сегментом пакетной передачей данных по IP протоколу, система VoIP телефонии испытывает те же угрозы, присущие обычным сетям, а также спектр угроз безопасности связанный сугубо с данным сегментом.

Рост количества и разнообразия пользовательских устройств, вызвал необходимость защиты речевого трафика от каждого конечного терминала. Обеспечение безопасности в сетевой инфраструктуре реализовано при помощи сложных программно-аппаратных комплексов, которые обеспечивают безопасность различными методами на различных уровнях. Данное решение должно быть гибким, обеспечивать устойчивое шифрование, а также быть кроссплатформенным.

Одним из наиболее подходящих решений является программный продукт с открытым исходным кодом OpenVPN. OpenVPN это open source технология, обеспечивающая надёжный криптоканал связи между пользователем и сервером. OpenVPN использует для обеспечения безопасности потока данных протоколы SSL/TLS, а, следовательно, поддерживает все возможности шифрования, аутентификации и сертификации библиотеки OpenSSL. OpenVPN является достаточно сложным при установке и настройке.

В докладе рассмотрен вариант реализации сети VoIP на основе технологии OpenVPN. Для заданной структуры телефонной сети предприятия определены основные уязвимости и угрозы информационной безопасности. Предложены варианты настройки шифрования и аутентификации.

ОПТИМИЗАЦИЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ПРЕДПРИЯТИЯ

П.А. Домино, С.Н. Петров

Ограничение доступа является важным условием соблюдения такого свойства информации, как конфиденциальность. Обязательной частью управления доступом является