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