А.А.АНТОННИКОВ[1], С.Н.ПЕТРОВ[1]

ЗАЩИТА ГОЛОСОВОГО ТРАФИКА НА БАЗЕ РАЗВЕТВЛЕННОЙ СЕТИ ПРЕДПРИЯТИЯ ООО «СЕДЬМАЯ СТЕПЕНЬ» С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПРОДУКТА OPENVPN

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

В наши дни сложно представить себе организацию, завод, учреждение образования или больницу без разветвлённой компьютерной сети. Широко используются всевозможные сервисы и технологии, реализуемые в компьютерных сетях, а также в сетях передачи данных. Одним из таких сервисов является IP-телефония.

В развитых странах IP-телефония является обыденным сервисом, который позволяет качественно и недорого осуществлять весь спектр услуг связи. По причине бурного развития данной технологии уже некоторое время возникают вопросы, связанные с безопасностью передачи данных. Существует проблема защиты такого рода данных. На рынке представлены различные технические решения, направленные на обеспечение безопасности передаваемой информации.

На базе существующей сети передачи данных (компьютерной сети) компании ООО «Седьмая степень» был осуществлен анализ основных угроз информационной безопасности и предложены меры по снижению рисков утечки конфиденциальной информации. В связи с тем, что данное предприятие имеет разветвленную структуру в разных странах, а именно 3 филиала, топология сети ориентирована на внутренние и внешние терминальные устройства. В каждом филиале существует серверное оборудование с развернутым CENTOS 7 и Open Source программным продуктом ASTERISK. Каждый из офисов связан между собой магистральным интернет-каналом передачи данных. Персонал офисов использует терминальные устройства в виде персональных компьютеров, IP-телефонов, мобильных терминалов на IOS/Android платформах. Головной офис оснащен оборудованием сопряжения, таким как голосовые шлюзы сопряжения с сетью общего пользования, шлюзы сопряжения мобильных сетей на частотах 850, 900, 1800 и 1900 МГц, а также VOIP-транки прямых международных номеров от различных интернет провайдеров. Каждое из терминальных устройств поддерживает аутентификацию пользователя.

Проанализировав спектр возможных угроз и уязвимостей сети, а также с учетом построенной модели злоумышленника, в качестве основного средства защиты был выбран open source продукт OPENVPN, обеспечивающий надежную криптозащиту и аутентификацию пользователей. Настройка и конфигурирование данного продукта является довольно трудоемким процессом и основана на клиент-серверном типе взаимодействия. Конфигурируется продукт путем создания исполнительного файла, содержащего типовые команды.

Одним из основных факторов защиты является степень закрытости передаваемой информации (речевой, текстовой, аудио-видео конференцсвязи и др.) для третьих лиц. Наибольшее распространение для обеспечения конфиденциальности информации получила криптозащита. С учетом большой популярности кроссплатформенных устройств, входящих в состав компьютерных сетей и передачи данных наиболее гибким решением является использование программных продуктов на основе протоколов шифрования SSL/TLS.

В результате мы получили распределенную VPN-сеть с надежным шифрованием и аутентификаций пользователей, без дополнительных затрат на аппаратные шифраторы и комплексы криптозащиты. Сравнительно с существующими VPN-технологиями, данное решение позволяет осуществлять удаленный доступ к терминальным устройствам без открытия портов, например, таких как UDP 5060, TCP 5061 и др. по которым ежесекундно осуществляются атаки. Следует отметить явный коммерческий эффект от такого типа решения, т.к оно не требует дополнительного оборудования и сам программный продукт является OpenSource. Основные затраты на использование лежат в плоскости инженерной настройки. Продукт OpenVPN позволил гибко выстроить политику безопасности и осуществить индивидуальную настройка каждого пользователя, использующего терминальные устройства.