УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СЕТИ ПРЕДПРИЯТИЯ

Лодис А.В., магистрант гр. 067041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С.Б. – кандидат технических наук, доцент

Распространение и внедрение информационных технологий привело к тому, что применение электронных документов вместо печатных является наиболее удобным способом документооборота, поэтому для организации его на предприятии необходимо создание защищенной сети передачи данных, а также регистрационного центра предприятия для создания и выдачи электронной цифровой подписи сотрудникам.

Целью работы является создание облика защищенной сети передачи данных и регистрационного центра предприятия, повышение защиты сети передачи данных, тем самым обеспечение информационной безопасности при издании, распространении и хранении сертификатов открытых ключей проверки электронной цифровой подписи, присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

При внедрении систем электронного документооборота на предприятии необходимо организовать и четко отладить функционирование сети передачи данных с обязательным применением основных требований по информационной безопасности, а именно обеспечить конфиденциальность, целостность и доступность информации.

Как правило у самого предприятия нет собственных ресурсов сети связи и необходимые канальные ресурсы арендуются из сети связи общего пользования у региональных и национальных операторов связи.

Используемые структурно-технологические решения по сопряжению транспортных сетей из состава собственных сетей связи с сетями в составе сетей связи общего пользования операторов связи обеспечивают связность на сетевом уровне, за счет использования единых протокольных решений на основе протоколов IPv4 и IPv6. В целях обеспечения безопасности при сопряжении собственных сетей связи с сетями связи общего пользования должны быть использованы решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе собственных сетей связи и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются в сетях связи общего пользования оператором связи.

С учетом развития угроз безопасности информации, а также способов реализации данных угроз за последнее время базовые принципы построения информационной сети претерпели существенные изменения. На рисунке 1 представлена схема взаимодействия в ведомственной информационной сети удаленных постов регистрации в региональных подразделениях с регистрационным центром в центральном узле предприятия и Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь в Национальном центре электронных услуг с применением средств межсетевого экранирования и программно-аппаратных комплексов шифрования передаваемого трафика (информации).

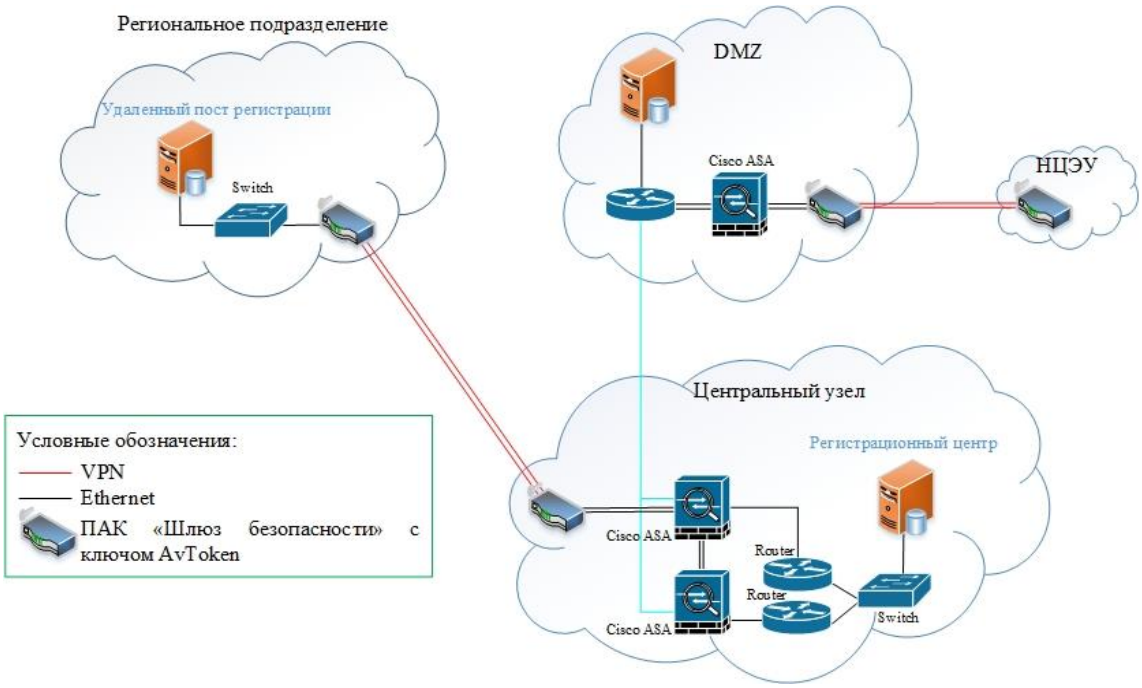

Рисунок 1. Схема сети передачи данных регистрационного центра предприятия

Для объединения локальных сетей удаленных узлов применяют технологию виртуальных частных сетей – VPN (Virtual Private Network). Данная технология предназначена для криптографической защиты данных, передаваемых по компьютерным сетям. Виртуальная частная сеть представляет собой совокупность сетевых соединений между несколькими VPN-шлюзами, на которых производится шифрование сетевого трафика.

В систему информационной сети предприятия входят программные, технические и программно-технические средства, обеспечивающие взаимодействие регистрационных центров как внутри предприятия, так и межведомственного обмена информацией.

Достоинства использования технологий виртуальных частных сетей для защиты информации в распределенных информационных сетях предприятий:

1. Сегментация информационной сети и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.
2. Использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев сети.
3. Обеспечение подконтрольности работы информационной сети и достоверная идентификация всех источников информации. При необходимости может быть обеспечена аутентификация трафика на уровне отдельных пользователей.
4. Возможность защиты всей информационной сети от крупных локальных сетей офисов до отдельных рабочих мест.
5. Масштабируемость системы защиты.

Основное предназначение регистрационного центра предприятия — это решение задач по обеспечению должностных лиц, сотрудников предприятия средствами электронной цифровой подписи Республиканского удостоверяющего центра национального центра электронных услуг.

Регистрационный центр предприятия является элементом Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг и осуществляет взаимодействие между Республиканским удостоверяющим центром и потребителями (сотрудниками предприятия, являющимися владельцами личных ключей, использующихся при выработке электронной цифровой подписи и получившими полномочия ее применять).

Основными функциями регистрационного центра предприятия являются:

проверка полноты и достоверности информации, представляемой заявителями в Республиканский удостоверяющий центр;

регистрация потребителей;

изготовление ключей электронной цифровой подписи;

запись на носители ключевой информации личных ключей;

формирование запросов в Республиканский удостоверяющий центр на выпуск сертификатов открытого ключа;

изготовление карточек открытых ключей;

изготовление учетных карточек;

формирование запросов в Республиканский удостоверяющий центр на прекращение действия (отзыв), приостановление действия сертификатов открытого ключа;

формирование запросов в Республиканский удостоверяющий центр на возобновление действия сертификатов открытого ключа;

изготовление, учет, накопление и хранение первого экземпляра карточек открытых ключей, одного экземпляра учетных карточек;

протоколирование работы регистрационного центра предприятия;

консультация потребителей по вопросам применения средств электронной цифровой подписи и др.

Таким образом с учетом функций, выполняемых регистрационным центром предприятия выдвигаемые требования по обеспечение требуемой высокой степени защиты сети передачи данных предприятия и использования оборудования межсетевого экранирования, шифрования передаваемого трафика, технологии виртуальных частных сетей являются обоснованными и необходимым условием для применения. Дальнейшая работа по исследованию данной темы будет направлена на поиск уязвимостей VPN сетей передачи данных и программно-аппаратных средств защиты сети, повышения защиты функционирования регистрационного центра предприятия.

Список использованных источников:

1. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28.12.2009 г. № 113-З.

2. Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. URL: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf;

3. Документация о программном комплексе «Шлюз безопасности виртуальный Bel VPN Gate» [Электронный ресурс]. – Режим доступа: http://s-terra.by/products/bel-vpn-gate-v.19.