ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ШЛЮЗОВ БЕЗОПАСНОСТИ В ВЕДОМСТВЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

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

Андриянов П.А., Андриянова Т.А.

Саломатин С.Б. – к.т.н.,доцент

Опыт создания и функционирования современных ведомственных телекоммуникационных систем подтвердил экономическую и техническую целесообразность формирования их на базе арендованных магистральных линий передачи (телефонных каналов общего пользования – ТКОП) и создания на их основе систем передачи данных (СПД). Современные СПД представляют собой программно-технические комплексы (ПТК), созданные на основе персональных компьютеров, высокоскоростных сетевых устройств и действующих каналов связи, в которых формирование и анализ сигналов выполняется как на аппаратном, так и на программном уровнях.

Характерной особенностью ПТК систем передачи данных является то, что в них интегрированы процессы ввода-вывода, защиты от ошибок, формирования и анализа сигналов. Кроме того, они выполняют и другие, не связанные с передачей данных, функции, такие как поиск и формирование файловых данных, компрессия и декомпрессия, защита от НСД и другие [1].

С точки зрения безопасности организуемых соединений можно выделить ряд способов: использование туннелей, шифрование, разделение потоков, аутентификация и управление доступом. При выборе конкретной технологии нужно учитывать следующие факторы:

вид передаваемого трафика (данные, голос, видео);

профиль трафика в течение суток и недели (передаются ли данные только днем или, например, ночью идет резервное копирование и сбор статистики);

иерархическую организацию площадок организации (один головной офис или структура, состоящая из головного офиса, кустовых узлов и оконечных узлов);

постоянство занимаемых площадей (собственность или аренда);

вид площадей (полноценные филиалы, пункты обслуживания клиентов или дата-центры);

организацию бизнес-процессов компании (как в плане операционной деятельности, так и временные параметры сбора информации и формирования отчетов);

требования к информационной безопасности;

общую политику организации (аренда каналов или собственные капитальные вложения) [2].

С точки зрения информационной безопасности стоит говорить об уровне конфиденциальности и ценности передаваемой информации, а также об уровне возможного ущерба в случае ее утечки, уничтожения, модификации или блокирования. Наиболее системный и общий подход состоит в том, что проводится классификация соединяемых территориально распределенных площадок организации по указанным признакам с объединением их в группы. Для каждой группы определяется оптимальный типовой вариант решения с возможностью расширения в будущем. В любом случае общая рекомендация сводится к использованию услуг сети MPLS (все основные операторы дальней связи предлагают услуги сети MPLS, а в тех регионах, где этого нет, надо использовать или выделенные каналы, или Frame Relay) и протокола IPSec. В качестве альтернативы протоколу IPSec для государственных организаций могут выступать отечественные аппаратно-программные разработки на основе алгоритмов шифрования и сертифицированного оборудования с поддержкой IPSec [2].

Защищенность соединений можно рассматривать с двух точек зрения: обеспечение защиты на технологическом уровне, за счет особенностей технологии (при этом трафик одного пользователя виртуально отделяется от трафика другого пользователя, и в нормальных условиях они не пересекаются) и обеспечение защиты с помощью шифрования трафика.

Рациональный выбор организационно-технологических и программных решений для защиты коммуникаций в территориально распределенных ведомственных информационных системах определяется несколькими факторами: архитектурой и масштабом сети, обрабатываемой в информационной сети информацией, используемой линейной и активной аппаратурой и собственно задачами обеспечения безопасности данных.

Программно-аппаратный шлюз, как средство сетевой безопасности, предназначен для обеспечения сетевой безопасности вычислительной сети любой топологии: выполняет функции шифрования, контроля целостности (криптографической защиты), а также фильтрацию как трафика подсетей, проходящего через них, так и защиту трафика самих шлюзов безопасности.

Средства сетевой информационной безопасности - это технологии виртуальных защищенных сетей (Virtual Private Network, VPN) и интегрированные с ними средства аутентификации и контроля доступа. Технологии VPN обеспечивают шифрование (конфиденциальность), электронно-цифровую подпись (целостность, имитостойкость, аутентификацию) на уровне IP-пакетов. На основе технологии VPN обеспечиваются защищенные соединения между подсетями и компьютерами. При этом компьютеры могут идентифицироваться как "обезличенные" узлы сети (по IP-адресу) и как рабочие места заданных индивидуальных пользователей (такая идентификация проводится, как правило, по сертификату пользователя). Технологии VPN предоставляют гибкость в реализации политики сетевой защиты. Для защиты могут использоваться множественные алгоритмы шифрования, сложные конфигурации туннелей и

защищенных периметров. Технологии VPN обеспечивают высокую стойкость защиты информации; при необходимости защитить сложную сетевую инфраструктуру эти технологии не имеют практической альтернативы. Технологии VPN используют средства шифрования, хэширования и электронной цифровой подписи.

Рассмотрим технологию предоставления доступа к удаленным рабочим столам Virtual Desktop Infrastructure (VDI), которая в настоящее время получила особую популярность в качестве дополнительных средств защиты от несанкционированного доступа и других внешних угроз в сфере применения ведомственных информационных ресурсов в целях создания подконтрольных виртуальных рабочих мест. С помощью технологии VDI пользователи получают доступ к информационным ресурсам своей организации и необходимому программному обеспечению.

Способы защиты VDI:

1. Защита на основе SSL VPN с дополнительной аутентификацией.
2. Защита на основе IPsec VPN с дополнительной аутентификацией.
3. IPsec VPN на специализированном терминале. Предлагаемое решение совместимо с любыми системами VDI и соответствует требованиям законодательства в области информационной безопасности. Оно позволяет сотрудникам получить защищенный доступ к инфраструктуре виртуальных рабочих столов и приложений из любой точки.

В данном сценарии сотрудники работают на терминальных станциях с оптимизированной операционной системой, находящейся на защищенном съемном носителе. Аутентификация пользователя на рабочей станции происходит до загрузки операционной системы, а после загрузки - в самом VDI приложении. Защита данных при их передаче обеспечивается встроенным в ОС IPsec VPN клиентом. Защита от вредоносного ПО реализуется с помощью замкнутой программной среды и проверки целостности при запуске.

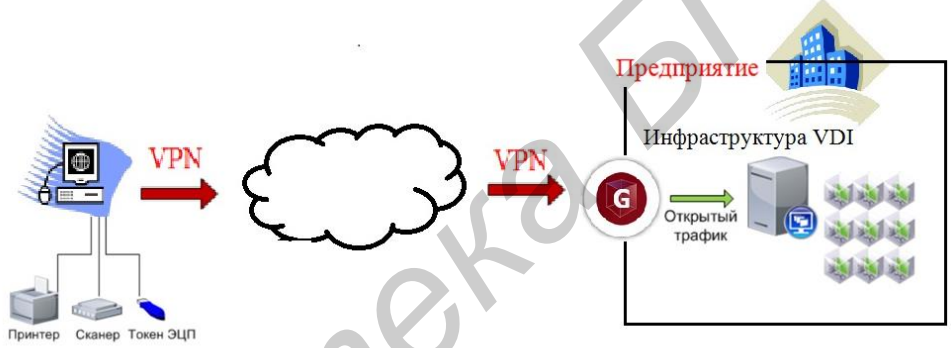

Рис. 1 - Пример защиты удаленного доступа к инфраструктуре VDI с использованием шлюзов безопасности.

Для защиты серверной части используется шлюз безопасности в виде виртуальной машины для популярных гипервизоров (VMware ESX, Citrix). Данные технологии защиты позволяют обеспечить:

Изолированное сетевое соединение с инфраструктурой VDI. Целевой трафик передается по защищенному VPN-туннелю, при этом обеспечивается конфиденциальность и целостность передаваемой информации. Остальной трафик либо запрещен, либо передается через ведомственный сервер, в зависимости от настроенных политик безопасности.

Итак, использование замкнутой программной среды и СЗН минимизирует воздействие агрессивной информационной среды на работу с важной информацией, а также снижает риски, связанные с возможными деструктивными действиями пользователей. Также можно отказаться от применения антивирусного программного обеспечения на рабочих местах пользователей и дополнительных средств защиты. Это позволяет не только сэкономить средства, но и существенно облегчить процесс эксплуатации терминалов, поскольку нет необходимости контролировать их конфигурацию и обновлять антивирусные базы данных.

Выделить какое-либо из упомянутых решений в качестве наиболее предпочтительного достаточно сложно, так как рациональная защита должна строиться с учетом характеристик информации, параметров информационной системы и уровня различных угроз.

Список использованных источников:

1. Буренин, А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А.Н. Буренин, Легков К.Е. // Наукоемкие технологии в космических исследованиях Земли. – №3. – 2015. т. 7. № 3. с. 46–61.

2. Романов С.А., Огородников Д.С., Защищенные коммуникации в территориально распределенных компаниях / Романов С.А., Огородников Д.С.// Журнал «BYTE» - №6 – 2015.