сообщении, особенно в летний период времени.

Для надежной и бесперебойной передачи данных в процессинговый центр требуется разработать резервирование каналов связи и создание таблиц маршрутизации (рисунок 1), а также обеспечить защиту передаваемых данных.

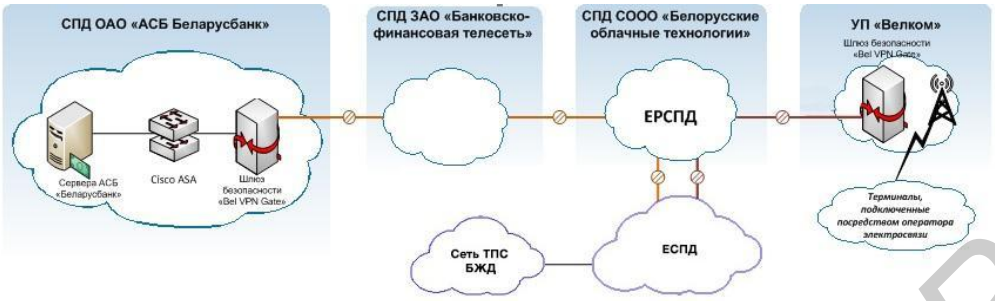

Рисунок 1 - Схема организации доступа ЕСПД Белорусской железной дороги к ОАО «АСБ Беларусбанк»

В целях организации защищенных цифровых каналов связи в единой сети передачи данных (ЕСПД) для подразделений Белорусской железной дороги, не имеющих возможности подключения по ведомственным каналам связи либо мобильных пользователей, создан ОТС VPN. В рамках ОТС VPN разработана АС VPN с использованием ведомственных и (или) арендуемых каналов передачи данных.

Построение АС VPN осуществляется по методу одного центрального узла (ЦУ) и одного или нескольких подчиненных узлов (ПУ) с минимальными затратами на аппаратно-программное оснащение пользователей и возможностью масштабирования конфигурации.

Центральный узел (ЦУ) и подчиненный узел (ПУ) АС VPN оснащаются сертифицированными в установленном порядке аппаратно-программным комплексом (АПК), предназначенными для обеспечения защиты информации при ее передаче в сетях общего пользования.

Для однозначной идентификации пользователей ОТС VPN используется отдельный УЦ VPN, который обеспечивает пользователей ОТС VPN уникальными личными ключами, предназначенными для применения в АС VPN.

Таким образом была разработана автоматизированная система, которая выполняет все функции по регистрации (аутентификации) пользователей, защите технологического трафика для передачи его из (в) ЕСПД.

Список использованных источников:

1.СТП БЧ 19.276–2013. Устройства пассажирской автоматики. Порядок технического обслуживания. – Мн.: Белорусская железная дорога, 2013. –22с.

СЕТЕВОЕ УПРАВЛЕНИЕ ПЛАТЕЖЕ-СПРАВОЧНЫМИ ТЕРМИНАЛАМИ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Ненартович Д.В.

Скудняков Ю.А. – канд.техн.наук, доцент

На предприятиях часто возникают задачи, требующие высокой доступности сетевых сервисов и данных при наличии отказоустойчивой топологии сети передачи данных. Основным используемым на практике вариантом создания отказоустойчивой конфигурации сети являются решения, основанные на применении протоколов автоматической маршрутизации.

С точки зрения протоколов маршрутизации, сеть с резервными каналами связи представляет собой отдельные подсети с несколькими возможными путями передачи данных из одной подсети в другую. В большинстве случаев администратору достаточно только включить протоколы автоматической маршрутизации, чтобы сеть "заработала". Причем переключение на другие пути передачи данных в случае повреждения каналов связи будет происходить за счет изменения таблиц маршрутизации.

Сценарий представляет собой описание двух подсетей, одна из которых SN1 защищается шлюзом безопасности GW3, а вторая подсеть SN2 защищается кластером, функции которого выполняют два шлюза безопасности GW1 и GW2. На шлюзах установлен продукт CSP VPN Gate, обеспечивающий защиту и пакетную фильтрацию трафика сети. В схему включены два роутера: Router1 и Router2.

Иллюстрация вышеописанного представлена на рисунке 1.

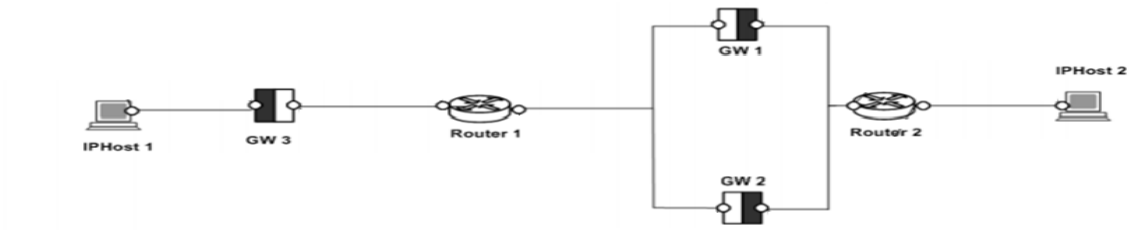

Рисунок 1 – Логика работы отказоустойчивого решения

В предложенном решении реализована следующая логика работы:

– в качестве кластера используются два шлюза безопасности CSP VPN Gate;

– шлюзы имеют различные роли – GW1 – основной шлюз безопасности, GW2 – резервный шлюз безопасности;

– кроме шлюзов безопасности определены два «надежных» устройства. На эти устройства отправляются ICMP-пакеты для диагностики работоспособности сетевых интерфейсов шлюза безопасности;

– в нормальном режиме весь трафик обрабатывается на основном шлюзе безопасности, а резервный шлюз безопасности в это время находится в режиме ожидания;

– в случае выхода из строя основного шлюза безопасности, его заменяет резервный шлюз безопасности и обрабатывает весь проходящий трафик;

– после восстановления работоспособности основного шлюза безопасности резервный шлюз переходит в режим ожидания и отдает управление основному шлюзу безопасности;

– проверка работоспособности основного и резервного шлюзов безопасности, а также действия по активации и настройке интерфейсов производятся с помощью скриптов, устанавливаемых на шлюзы безопасности.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В РЕШЕНИЯХ ПО БЕЗОПАСНОСТИ БАНКОМАТОВ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Никифоров В.В.

Шпак И.И. – канд. техн. наук, доцент

В докладе рассматриваются виды мошенничества с банкоматами. Рассматривается комплекс мер защиты конфиденциальной информации клиента, в частности IPSec, который представляет собой основанный на стандартах набор протоколов и алгоритмов защиты. Однако принимаемые меры не дают сто процентной гарантии, что злоумышленник не сможет завладеть данными.

В современном обществе устройства по обслуживанию пластиковых карт (банкоматы) пользуются всё более возрастающей популярностью. Банковские счета открываются повсеместно. Для надёжного хранения и удобства управления своими деньгами люди пользуются банковскими картами. Согласно оценкам компании Retail Banking Research Ltd, в мире установлено свыше 1,2 млн. банкоматов. Банкомат становится объектом криминальных действий мошенников.

Наиболее распространенными типами атак являются:

Заедание карточки (Cardjamming), подкачка карточки (Cardswapping), компромат по PIN-коду (CompromiseofPINnumber) , вандализм, диверсии [1].

Инновации и возможности человека растут с каждым днем. Производители банкоматов, пытаются делать все возможное для того, чтобы вся конфиденциальная информация была в сохранности. К конфиденциальным данным относиться:

1) номер держателя карты,
2) пин-код
3) CVV-код, используется для проверки подлинности карты.

Так же и сами владельцы банкоматов, а именно банки, стараются оградить клиентуру от различных видов мошенничества. Полностью избежать таких ситуаций, к сожалению, невозможно, потому как злоумышленники так же изобретают различные приспособления, устройства, находят иные способы реализации их планов.

Основные методы хищения носят технологический характер. За многолетнюю практику, в банке «Белгазпромбанк» было зафиксировано множество попыток хищения конфиденциальной информации.

Для этого было решено ввести ряд технических доработок. Так как многие АТМ находятся удаленно от