Техническое описание эквайрингового транспортного комплекса CityNet SV.3
(CITYNET SYSTEM VERSION 3)

ООО «Ситинет»
Россия, г. Москва, Ул. Берзарина, д.36, стр. 11
тел.: +7(495)-380-07-97, факс: +7(495)-730-59-59,
http: www.citynet.ru, e-mail: info@citynet.ru

Оглавление

1. Общие сведенья о системе

Универсальный коммуникационный комплекс CityNet SV.3 позволяет обеспечивать взаимодействие систем, устройств, процессов, терминалов и АТМ в разнородных коммуникационных средах (X.25,TCP/IP,RS-232). Система взаимодействия построена на одноранговых транспортно-логических сетях CityNet DUT (Date Unit Transport).

Построение таких одноранговых транспортно-логических сетей CityNet DUT (Data Unit Transport), позволяет осуществлять транспортировку сообщений по логическим узлам и интерфейсам DUT. Данная технология, кроме предоставления транспорта процессам ориентированных на сообщениях, позволяет преобразовывать логическое соединение в поток DUT сообщений и дальнейшее преобразование DUT сообщений в логическое соединение на стороне-получателе. Это позволяет избежать дорогостоящих постоянных логических соединений в X.25 или GSM сетях, заменяя их соединениями, устанавливаемыми на время передачи реальных данных, причём, от узла назначения к узлу получателю устанавливается только одно логическое соединение, даже, если транспортируются несколько логических соединений. Все логические соединения, проходящие через открытые сети, шифруются с использованием алгоритмов ГОСТ28147-89 или 3DES, что обеспечивает защищенность передаваемых данных.

Коммуникационный транспортный комплекс состоит из коммуникационного сервера CityNet SV.3 и клиентского оборудования.

Коммуникационный сервер CityNet SV.3 реализован как автоматическое устройство. Управление устройством осуществляется через консоли управления (специализированная программа, поставляемая с коммуникационным сервером). Удалённая консоль управления позволяет дистанционно наблюдать работу сервера, диагностировать и конфигурировать. Для аутентификации консолей управления используются аппаратные микропроцессорные ключи, устанавливаемые на порты (USB, LPT) как самого коммуникационного сервера, так и рабочих станций, на которые установлены консоли управления. При этом аппаратные ключи шифруют весь трафик обмена между удалённой консолью и коммуникационным сервером. Данная специфика реализации позволяет коммуникационному серверу быть неуязвимым в отношении взлома системы управления (в отличие от защиты паролем и ограничением коммуникационных адресов управления). Маршрутизация потоков данных осуществляется с помощью таблиц маршрутизации коммуникационного сервера. Все таблицы маршрутизации и другая информация конфигурации сервера, так же, хранится в закодированном аппаратным ключом виде. Серверный комплекс не является средством FireWall-й зашиты системы, а представляет средства транспортировки и шифрования данных.

Клиентское оборудование представлено комплексным маршрутизирующим оборудованием сервисного типа CityNet SV.3 Client и самостоятельными транспортными модулями MicroSV3. CityNet SV.3 Client базируется на базе персональных компьютерах с ОС Win 98, XP, Vista и защищены микропроцессорным ключом (USB, LPT), обеспечивающим шифрование передаваемого трафика и рабочих файлов приложения. Транспортные модули

MicroSV3 являются самостоятельными автоматическими устройствами, обеспечивающие взаимодействие терминальных устройств с процессинговым центром по шифрованному (ГОСТ28147-89, 3DES) виртуальному DUT каналу связи. Управление устройствами MicroSV3 и CityNet SV.3 Client осуществляется через специализированный программный комплекс с использованием шифрованных виртуальных DUT каналов.

2. Структура организация транспортной сети CityNet SV.3.

Транспортная сеть SV.3 представлена двумя уровнями:

- опорная сеть, состоящая из опорных узлов, установленных в центрах маршрутизации (Процессинговый Центр, Интернет провайдеры, Сервисных центрах)
- сеть функциональных узлов, состоящая из узлов, которые выполняют специализированные транспортные функции (платежные шлюзы, интерфейс с системой авторизации, клиентские узлы, коммутирующие шлюзы)

Основу транспортной сети составляет опорная сеть, которую образуют опорные узлы, связанные между собой постоянными логическими соединениями. Задача опорных узлов - коммутация гетерогенных логических соединений и маршрутизация DUT сообщений (Data Unit Transport - протокол, основанный на маршрутизации элемента данных с адресной информацией: узел назначения, узел источник, тип интерфейса).

Для маршрутизации DUT сообщений, опорные узлы устанавливают защищенные виртуальные логические соединения, по возможности «каждый с каждым». На основе образованных логических соединений строятся таблицы межузловой маршрутизации DUT сообщений. Построенные соединения имеют асимметричный характер (для одного узла - исходящее, для другого - входящее). Данная особенность, позволяет распределять нужным образом нагрузку между узлами.

Коммутация гетерогенных соединений, вторая функция опорных узлов, предназначена для соединения через сеть различных устройств и хостов с преобразованием протоколов (в том числе и Прикладных).

В качестве примера, можно привести подключение терминалов к клиентскому узлу, затем трансляция клиентским узлом TCP/IP соединения в DUT до следующего узла (с зашифрованной информации, актуализацией соединений - проверка маркерами на предмет целостности и готовности соединения, и т.п.). Дальнейшая трансляция с серверного узла входящего шифрованного DUT (ГОСТ28147-89, 3DES) соединения в X.25 логические соединение хосту по локальной сети.

Функциональный узел представляет собой программно-аппаратный комплекс SV.3, ориентированным на выполнение определённых прикладных задач.

Выделяется три типа функциональных узлов:

- узел системы авторизации
- клиентские узлы
- платёжный шлюз

Назначение функционального узла первого типа «узел системы авторизации», заключается в предоставлении доступа в транспортную сеть прикладным системам по DUT интерфейсам. В этом случае, прикладные системы получают возможность работать с сообщениями в формате DUT через транспортную сеть. Таким образом, узел первого типа - базовый интерфейсный узел. К данному узлу, как правило, подключаются системы авторизации для обеспечения межцентрового взаимодействия, терминальные хосты, мониторинговые системы.

Второй тип функциональных узлов «клиентские узлы», предназначен для организации подключений POS-терминалов, кассового решения и банкоматов по протоколу TCP/IP, RS-232, данный тип узлов предназначен для построения распределенной транспортной сети.

Третий тип «платёжный шлюз», предназначен для предоставления доступа к сервису платёжной системы, прикладным системам по протоколу UCFT, ABG, SAF. Узлы третьего типа иногда относят к клиентским узлам с расширенным функционалом, который обеспечивает взаимодействия сервисов с узлами авторизации.

3. Функциональные возможности и управление узлами комплекса.

3.1 Функциональные возможности узлов комплекса CityNet SV.3.

Сервер CityNet SV.3 обеспечивает выполнение следующих функций:

- маршрутизацию входящего DUT трафика
- управление узлами транспортной сети
- дешифрованного входного трафика на выходе транспортной сети
- проверка аутентификации узлов транспортной сети
- преобразование форматов данных
- контроль целостности логических DUT соединений
- взаимодействие разнородных средств передачи данных (X.25, RS-232, TCP/IP)
- обработку и преобразование дынных с использованием сервисных процессов
- резервирование логических DUT соединений
- анализ функционирования узлов сети
- геоинформационный мониторинг состояния узлов сети

Клиент CityNet SV.3 и MicroSV3 выполняют следующие функции:

- обработку входящего потока данных
- преобразование входящих потоков данных (протоколов TCP/IP, X.25, RS-232) в шифрованное DUT соединение
- посылку мониторинговых сообщений серверу CityNet SV.3
- преобразование входящего шифрованного DUT соединения со стороны сервера SV.3 в исходящее TCP/IP, RS-232, X.25
- обработку и преобразование данных с использованием сервисных процессов
- контроль целостности транслируемых потоков данных
- резервирование логических DUT соединений

3.2 Управление, защита и мониторинг устройств транспортной сети CityNet SV.3.

Узлами транспортной сети являются автономные самостоятельные управляющие модули (CityNet SV.3 Client, MicroSV3), обеспечивающие маршрутизацию, контроль целостности, шифрование (ГОСТ28147-89, 3DES) и преобразование исходящего потока данных.

Управление элементами транспортной сети включает в себя:

- конфигурирование элементом сети
- защита данных
- сервисное обслуживание
- резервирование
- мониторинг элементов транспортной сети

Конфигурирование узлов транспортной сети CityNet SV.3 предусматривает создание посредством специализированного программного обеспечения конфигурационного файла (содержащего требуемый набор параметров для функционирования определенного узла сети) и программного комплекса для удаленного доступа к оборудованию. Каждый элемент транспортной сети имеет уникальное имя NodeID (номер узла). Для каждого NodeID создаётся уникальный ключ аппаратной защиты, для шифрования передаваемых элементом данных (ГОСТ28147-89, 3DES). Программный комплекс удаленного доступа к узлу позволяет создавать шифрованный виртуально-логический канал связи для конфигурирования и управления элементом транспортной сети CityNet SV.3.

Защита данных организована, на использовании модуля безопасности узла SV.3 (Sam-модуль, микропроцессорные ключи зашиты USB, LPT). Модуль защиты представляет собой криптографическую подсистему, которая используется для организации защищенного обмена данными между пользователями (узлами) SV.3, а также между узлами и модулем управления. Зашифрованный обмен данными включает в себя два уровня защиты - шифрация межузлового трафика сессионным ключом, а также шифрацию прикладных данных от источника до получателя. Для шифрации/дешифрации данных, обмена ключами и т.д. применяются стандартизованные алгоритмы шифрования ГОСТ28147-89 и 3DES. Генерация ключей производится в специализированном программном приложении NSA, установленном на защищенном компьютере, доступ к которому разрешен только для персонала занимающегося администрированием сети узлов SV.3. Доступ к приложению регламентирован стандартом по информационной безопасности и требует от пользователей ввода индивидуальных носителей ключей аутентификации и пароля.

Сервисное обслуживание элементов транспортной сети производится по защищенным виртуальным DUT каналам связи, образованными специализированным программным обеспечением и управляемым элементом (узлом), что позволяет защитить транспортную сеть от внешнего воздействия.

Транспортная сеть, организованная на использовании оборудования CityNet SV.3, обеспечивает автономную работу всего комплекса входящих в нее устройств. Технически построенная одноранговая распределенная транспортная сеть CityNet SV.3 обеспечивает надежную и бесперебойную обработку потоков информации. Использование методов резервирования и распределения нагрузки

между серверами CityNet SV.3 позволяет снижать нагрузки на аппаратную часть оборудования, а в случае отказа избежать возможности прекращения работоспособности всего комплекса.

Взаимодействие узлов всей системы основано на организации постоянного канала связи между элементами комплекса. Контроль связи осуществляется посредством периодических посылок LifeKeep сообщений клиентским оборудованием в сторону CityNet SV.3 сервера и ожидания ответа от него. В случае отсутствия ответа на посланное LifeKeep сообщение за определенный промежуток времени, оборудование автоматически произведет смену канала связи.

Система мониторинга узлов транспортной сети реализована на базе посылки мониторинговых сообщений по защищенному DUT интерфейсу серверу CityNet SV.3 и дальнейшей их пересылке серверу геомониторинга, который преобразует полученные набор данных и заносит их в базу данных узлов. Использование сервиса мониторинга обеспечивает контроль работоспособности клиентского оборудования и своевременной реакции обслуживающего персонала на возникающие неисправности. Мониторинговые сообщения отображают текущее состояние клиентских узлов (состояние Online/Offline, уровень сигнала по GPRS, причины падения со связи, трафик, тип оператора). Вывод мониторинговых данных производится через WEB-интерфейс, визуализирующего состояний элементов транспортной сети CityNet SV.3.

4. Требования предъявляемые CityNet SV.3 Server для зашиты данных.

Безопасность использования авторизационного сервера CityNet SV.3 требует выполнения ряда положений предъявляемых системой информационной безопасности и защиты данных:

- CityNet SV.3 Server должен располагаться в специально оборудованном помещение:
  a) экранированном
  b) кондиционируемом
  c) с системой контроля доступом
- обеспечение ограниченного доступа к данным:
  a) IP-адреса/MAC-адреса
  b) приложения/сервисы
  c) учетные записи пользователей
  d) контроль и управление доступом пользователей
- ограничение доступа к CityNet SV.3 Server из внешней сети:
  a) FireWall
  b) интеллектуальные маршрутизаторы
  c) логическое зонирование сети (DMZ зоны)
  d) политика безопасности

5. Требования предъявляемые CityNet SV.3 Client для зашиты данных.

Безопасность транслируемых потоков данных через коммуникационное оборудование CityNet SV.3 Client реализуется посредством настроек OS

используемого оборудования. Существует ряд обязательных требований, накладываемый CityNet SV.3 Client для организации защиты данных:

- использование FireWall
- контроль учетных записей

6. Технические характеристики элементов CityNet.

Основные технические характеристиками CityNet SV.3 Server:

- Протоколы – X.25 Eicon, TCP/IP, RS-232
- Максимальный количество правил динамической маршрутизации - 31, 100, 1000, 2000 (зависит от версии серверного ПО)
- Максимальное число подключаемых клиентских узлов -10000
- Максимальное количество подключенных интерфейсов - 10000
- Максимальное число слушаемых TCP/IP Socket - 31, 100, 1000, 2000 (зависит от версии серверного ПО)
- Максимальный размер таблицы сервисных процессов - 31, 100, 1000 (зависит от версии серверного ПО)

Технические характеристиками CityNet SV.3 Client:

- Протоколы – X.25 Eicon, TCP/IP, RS-232
- Трансляция (параметр, отвечающий за преобразования данных на клиентском узле)
- Максимальный количество правил динамической маршрутизации - 31, 100,500,1000 (зависит от версии ПО)
- Максимальное число подключаемых клиентских узлов -10000
- Максимальное количество подключенных интерфейсов - 10000
- Максимальное число слушаемых TCP/IP Socket - 31, 100,500, 1000 (зависит от версии ПО)
- Максимальный размер таблицы сервисных процессов - 31, 100, 1000 (зависит от версии ПО)

Технические характеристики транспортного модуля MicroSV3 ARM9:

- Процессор ARM9
- Внутренняя SRAM 8 kB, внешняя 64 Mb
- LAN EMAC Ethernet 10/100, TCP
- WAN W5300 / Ethernet 10/100, TCP
- GPRS модуль Simcom с адаптером на 2 Sim-карты
- Порт RS-232
- Порт USB
- Программное обеспечение «Citynet MicroSV3 ARM9 v2.1.1»
- Количество слушаемых TCP/IP Socket - 20
- Количество одновременно поднятых TCP/IP сессий - 20

7. Установочные требования CityNet SV.3 Server к OS.

Программный комплекс CityNet SV.3 Server обеспечивает контроль, управление и защиту обрабатываемых им данных. Серверный комплекс SV.3

представляет собою вид сервисной службы, устанавливаемой в OS, обеспечивающий совместною работу встроенных сервисов операционной системы. Функционирование сервисной службы CityNet SV.3 Server требует работоспособность сетевых служб и часть прикладных сервисов:

- Сервер (Server)
- eToken Notification Service (сервис аутентификации микропроцессорного ключа Etoken)
- Смарт-карты (Smart-card service)

8. Требование предъявляемые к аппаратной части.

Технические требования предъявляемые CityNet SV.3 Server:

- Процессор не ниже Pentium 4 2GHz
- Ram не ниже 1 Gb
- HDD 2X250 Raid 1
- OS Win Server 2000/2003/2008 St.Ed x86/x64

Минимальные требования, предъявляемые к аппаратной части для CityNet SV.3 Client:

- Процессор с частотой не ниже 533 MHz
- RAM 128 Mb
- Flash 256 Mb
- OS Win 98,2000,XP Embedded

9. Комплектность оборудования.

В комплектность модуля сервера CityNet SV.3 входит:

- Аппаратный ключ защиты USB (Eutron, Rockkey, eToken)
- Драйвер аппаратного ключа зашиты
- Программный модуль Citynet SV3 Server
- Пакет документаций

Комплектность модуля CityNet SV.3 Client:

- Аппаратный ключ защиты USB, LPT (Eutron, Rockkey, eToken)
- Драйвер аппаратного ключа зашиты
- Программный модуль CityNet SV.3 Client
- Пакет документаций

В комплект транспортного модуля MicroSV3:

- Модуль MicroSV3 ARM 9
- Sam-модуль, модуль аппаратной зашиты
- Блок питания 7..25 V, 1 A
- Кроссоверный кабель
- Антенна авто
- Пакет документаций