ООО «СиЭйЭн»

Телефон: **+7 (495) 120-1515**
Факс: **+7 (495) 666-5605**
E-Mail: sales@cansec.ru
http://cansec.ru

Высокоскоростной однонаправленный шлюз **СТРОМ-1000**

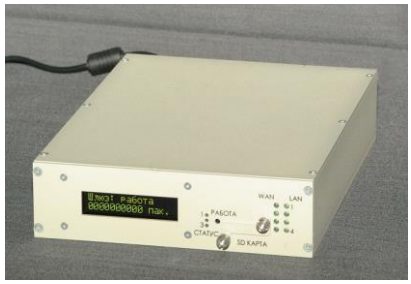
Краткое описание устройства

Высокоскоростной шлюз СТРОМ-1000 предназначен для гарантированной однонаправленной передачи информации из открытых сетей в сети, в которых циркулирует информация, составляющая государственную тайну, до 2-й категории включительно. Еще одна область использования диода данных – передача информации между сетями, при которой необходимо обеспечить целостность и доступность сети, передающей информацию. Гарантия однонаправленности передачи данных позволяет в первом случае предотвратить утечку информации из конфиденциальной сети, а во втором случае избежать возможности нежелательного внешнего воздействия на ключевые объекты и информацию, которая хранится и обрабатывается в защищаемой сети. Название Data Diode (диод данных, информационный диод) пришло из зарубежных реализаций и стало общеупотребительным для программно-аппаратных комплексов подобного класса. Оно основывается на аналогии с принципом действия соответствующего электронного элемента.

Выгоды применения

- Обеспечение конфиденциальности или целостности и доступности, в зависимости от реализуемой схемы, присоединяемого сегмента сети, гарантированные на аппаратном уровне однонаправленным характером передачи информации.
- **Единственный** аппаратно-программный комплекс, использование которого разрешено в системах, обрабатывающих и хранящих информацию, составляющую государственную тайну до 2-й категории включительно, подтвержденная заключением ФСБ России и сертификатами МО РФ.
- Простота использования и настройки, требуется минимальное начальное администрирование, дальше система может работать круглосуточно в автоматическом режиме, дополнительное участие администратора требуется если только необходимо изменить правила маршрутизации передаваемой информации.
- Оперативная поставка, как правило, на складе есть готовые к отгрузке комплексы однонаправленной передачи информации.
- Полное сопровождение в процессе эксплуатации, гарантийный срок 36 месяцев с даты поставки.

Исполнение 1.



Исполнение 2.

Основные характеристики

- Скорость передачи: до 960 Мбит/с.
- Старт: менее 5 секунд.
- Интерфейсы:
  - внешняя сеть: RJ-45, медь, витая пара, Ethernet 100/1000 BASE-T; SFP, Ethernet 1000 BASE-X;
  - внутренняя сеть: SC, многомодовая оптика, 850нм, 1000 BASE-SX.
- Конфигурирование: карта памяти.
- Поддержка до 511 внешних источников данных.
- Индикация (отображение состояния):
  - Светодиоды.
  - Матричный экран.
- Потребление: 15Вт.

- Два корпусных исполнения:
  - Исполнение 1: 1U по ГОСТ 28601.1-90 в телекоммуникационную стойку (ВхШхГ 44x483x272).
  - Исполнение 2: корпус UniCase (ВхШхГ 50x180x240).
- Категория подключаемых внутренних сетей до «совершенно секретно» включительно.
- Сокрытие структуры и топологии внутренней сети.
- В шлюзе реализован межсетевой экран, обеспечивающий фильтрацию и передачу только разрешенных IP-пакетов, заданных в таблице маршрутизации, настраиваемой в файле конфигурации.

Применение

Варианты использования высокоскоростного однонаправленного шлюза СТРОМ-1000 зависят от поставленной задачи. Условно эти задачи можно разбить на две категории: передача потоковой информации и передача файлов.

Передача потоковой информации

Такой информацией могут быть аудио- и видеопотоки, сигналы датчиков охранной сигнализации, телеметрия и т.п.
В качестве примера рассмотрим следующую задачу: необходимо передавать видеоизображение от IP-камер, установленных на неконтролируемой территории, на сервера, размещенные в категорированной сети.
В этом случае необходимо настроить источник потоковой информации на передачу данных в виде UDP/RTP-пакетов и настроить информационный диод СТРОМ-1000 под соответствующую конфигурацию сети.

Пример структуры сети для данного случая представлен на Рис.1.

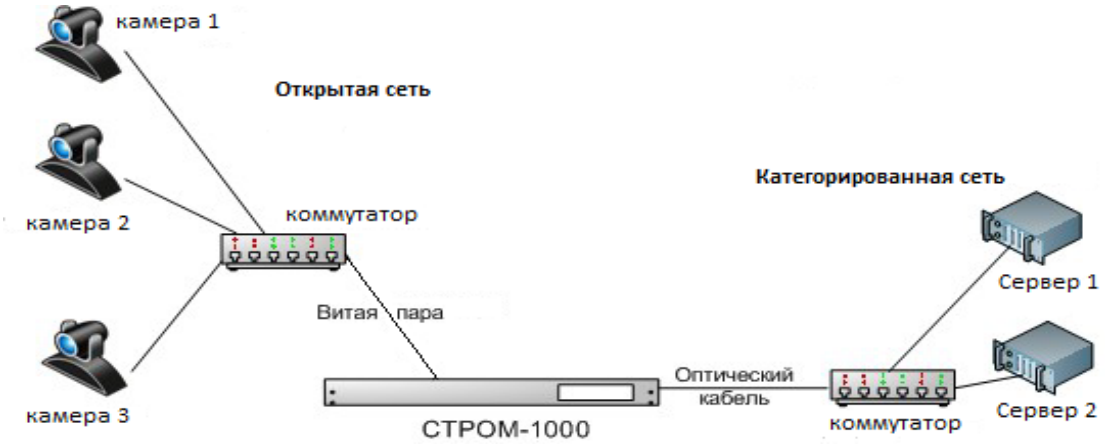


Рис.1. Передача UDP-потоков.

В данном случае работа комплекса происходит следующим образом:

1. Камеры 1 , 2, 3 настраиваются на передачу RTP-потока на определённый IP-адрес (IPdst) и порт.
2. В конфигурации СТРОМ-1000 в разделе разрешённых адресов прописываются IP-адреса камер.
3. В конфигурации указывается, с какой камеры и на какой сервер будет направлен UDP/RTP-поток.
4. Таким образом, UDP/RTP-потоки с камер собираются коммутатором и отправляются в СТРОМ-1000. Проходя через СТРОМ-1000, потоки попадают на соответствующий сервер.
5. Максимальное количество камер: 511.

Замечание

Существуют устройства, которые перед открытием потока требуют «подписаться» на этот поток. СТРОМ-1000 не выполняет функцию подписки на поток. Данная проблема решается путем установки во внешней сети сервера подписки.
В случае возникновения подобной проблемы необходимо связаться с нашей службой технической поддержкой для получения консультации и программного обеспечения сервера подписки.

Передача файлов

В качестве примера рассмотрим решение следующей задачи: необходимо провести обновление программного обеспечения компьютеров категорированной сети. Все необходимые для этого файлы были получены по каналам сети Internet. Теперь необходимо из открытой сети, имеющей подключение к сети Internet, передать эти файлы в закрытую сеть, не допустив утечки конфиденциальной информации.

Для решения подобной задачи помимо высокоскоростного однонаправленного шлюза СТРОМ-1000 необходимы два сервера с установленным специальным программным обеспечением (СПО), которое обеспечивает хранение, предоставление пользователям сетевых дисков и однонаправленную передачу файлов.

Структура сети в этом случае будет выглядеть следующим образом (Рис.2.):

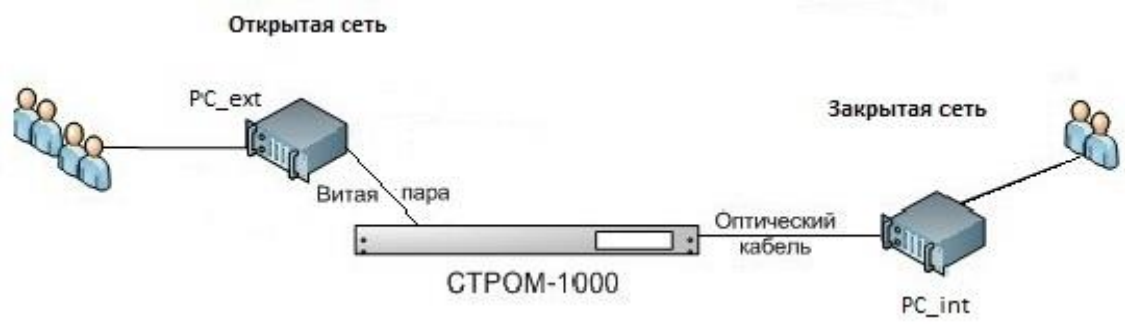


Рис.2. Передача файлов.

где PC_ext и PC_int — серверы с установленным СПО. Требования к серверам:

1. Одинаковые по производительности ПЭВМ.
2. Два сетевых интерфейса в каждой ПЭВМ.
3. Для внутреннего сервера: наличие сетевой карты с оптическим входом (1000BASE-SX, многомод, 850 нм), либо наличие оптического конвертора с аналогичными оптическими параметрами.

ВАЖНО!
Сетевая карта или оптический конвертор должны поддерживать режим работы без автопереговоров (auto-negotiation off).

4. ОС: Linux 32/64 bit, RedHat 64, Windows (от XP и выше), МСВС-3.0, МСВС-5.1.

Замечание:
Для уменьшения вероятности потери данных, не рекомендуется ставить между PC_ext и СТРОМ-1000 какое-либо активное сетевое оборудование. Также не рекомендуется использовать сетевой интерфейс PC_ext, к которому подключен СТРОМ-1000, под какие-либо другие приложения.

Функционирование программно-аппаратного комплекса однонаправленной передачи файлов.

1. На PC_ext и PC_int настроены FTP-сервера.
2. Пользователь из внешней сети заходит под своим логином на FTP-сервер PC_ext.
3. Пользователь помещает файл в свой каталог FTP-сервера.
4. СПО отправляет этот файл через СТРОМ-1000. В случае успешной отправки, файл из каталога пользователя внешнего FTP-сервера удаляется.
5. Если на PC_int файл принимается успешно, то принятый файл помещается в каталог пользователя FTP-сервера закрытой сети PC_int.
6. Пользователь заходит под своим логином на внутренний FTP-сервер PC_int и забирает помещенный туда файл.

Помимо протокола FTP, доступ пользователей также возможен по протоколу SMB.

Интерфейсы

На передней панели однонаправленного шлюза СТРОМ-1000 расположены следующие интерфейсы и средства индикации (Рис.3.):

- Разъем для чтения карты памяти (на рисунке он закрыт блокирующей пластиной).
- Светодиоды.
- LCD-дисплей.

Рис.3. Передняя панель (Исполнение 1).

На задней панели расположены следующие интерфейсы (Рис.4.):

- Разъем питания 220В.
- Разъем оптический, тип SC – для подключения к внутренней сети.
- Разъем RJ-45 – для подключения к внешней сети, витая пара.
- Разъем SFP - для подключения к внешней сети, оптический кабель.

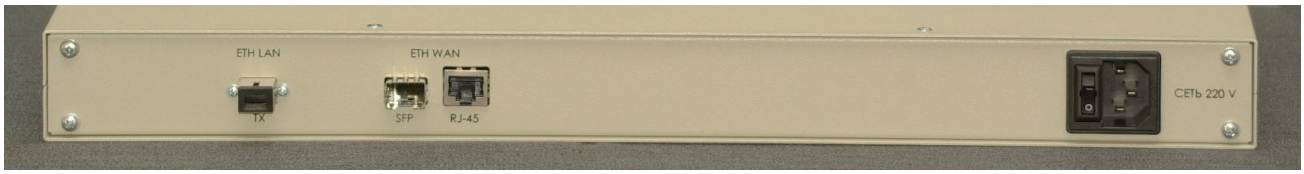


Рис.4. Задняя панель (Исполнение 1).

Габариты

Габариты Исполнения 1: В х Ш х Г – 44 х 483 х 272 мм. Габариты Исполнения 2: В х Ш х Г – 50 х 180 х 240 мм.

Конфигурирование

Конфигурирование однонаправленного шлюза СТРОМ-1000 производится с помощью конфигурационного файла, размещённого на карте памяти. Ввод конфигурации производится через считыватель SD-карт, доступ к которому ограничивается путём опломбирования (Рис.5.)

Рис.5.а. Доступ к считывателю для конфигурирования закрыт.

Рис.5.б. Доступ к считывателю для конфигурирования открыт.

Чтобы сконфигурировать высокоскоростной однонаправленный шлюз СТРОМ-1000, необходимо:

1. Включить питание СТРОМ-1000, дождаться безошибочной загрузки шлюза.
2. Снять блокирующую пластину с разъема для SD-карты.
3. Вставить SD-карту с конфигурационным файлом.
4. В случае, если конфигурационный файл на карте присутствует и соответствует установленному формату, то конфигурация применяется и запоминается в энергонезависимом ПЗУ.
5. После применения конфигурации SD-карту **нужно вытащить**, блокирующую пластину установить на место. При необходимости опечатать. **SD-карту оставлять в шлюзе не надо.**
6. Примененная конфигурация сохраняется в шлюзе даже в случае выключения питания и применяется при каждом включении.
7. Для смены конфигурации необходимо вставить в разъем карту памяти с другим конфигурационным файлом.

Конфигурационный файл

Структура и процедура получения конфигурационного файла описаны в эксплуатационной документации.

Требования к SD-карте.

- SD-карта любого объема с поддержкой режима SPI. Заметим, что в выпускаемых в последнее время SD-картах большого объема (более 8 ГБ) отсутствует поддержка SPI-режима. Такие SD-карты работать с шлюзом СТРОМ-1000 не смогут. Рекомендованный объем SD-карты — 8 Гбайт и менее.
- Возможна работа с картами micro-SD и mini-SD, установленными в соответствующие переходники.

Индикация

Индикация производится на LCD-экран и группы светодиодов.

LCD-экран отображает следующую информацию:

- Состояние устройства (работа, тестирование, ошибка).
- Процесс работы с картой памяти.
- Версии прошивок.
- Счётчик переданных во внутреннюю сеть пакетов.

Светодиоды отображают:

- Состояние линков интерфейсов.
- Наличие питания шлюза.
- Результаты тестирования при включении питания.
- Процесс работы с картой памяти.
- Аварийные ситуации.

Комплект поставки

В комплект поставки Исполнения 1 входит:

- Изделие СТРОМ-1000 Исполнение 1.
- Кабель питания 220 В.
- Паспорт изделия СТРОМ-1000.
- Диск с эксплуатационной документацией, СПО для конфигурирования, тестирования работоспособности и однонаправленной передачи файлов с описанием настройки и использования.
- Упаковка.

В комплект поставки Исполнения 2 входит:

- Изделие СТРОМ-1000 Исполнение 2.
- Источник питания 12 В.
- Паспорт изделия СТРОМ-1000.
- Диск с эксплуатационной документацией, СПО для конфигурирования, тестирования работоспособности и однонаправленной передачи файлов с описанием настройки и использования.
- Упаковка.