Руководство по эксплуатации

Teleport-1
Teleport-2

Трансляторы сухих контактов

Версия руководства 9
Версия встроенного ПО 2.0
© Форт-Телеком, Пермь 2025

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Содержание

Условные обозначения....3
Инструкция по безопасности....4
1 Назначение....6
1.1 Варианты применения....7
2 Технические характеристики....9
2.1 Teleport-1....9
2.2 Teleport-2....10
2.3 Поддерживаемые функции и протоколы....11
3 Описание....12
3.1 Внешний вид....12
3.2 Светодиодная индикация....13
3.3 Кнопка сброса настроек и перезагрузки....14
4 Монтаж и подключение....15
4.1 Монтаж Teleport-1....15
4.2 Монтаж Teleport-2....16
5 Настройка....18
5.1 Интерфейсы управления....18
5.2 Что нужно знать перед подключением....18
5.3 Управление через WEB-интерфейс....19
5.3.1 Первое подключение, быстрый старт....19
5.3.1.1 Стратегия настройки....24
5.3.2 Сетевые настройки....25
5.3.3 Настройка учётных записей пользователей....26
5.3.4 Описание устройства....27
5.3.5 Настройка языка web-интерфейса....28
5.3.6 Настройка режима трансляции....29
5.3.6.1 Настройка списка удалённых устройств....29
5.3.7 Настройка порта RS-485....31
5.3.8 Настройка цифровых входов....33
5.3.9 Настройка цифровых выходов....34
5.3.10 Настройка Modbus....36
5.3.11 Настройка режима сетевого контроллера входов/выходов....37
5.3.12 Настройка списка событий....38
5.3.13 Настройка Telnet....39
5.3.15.1 Список сообщений Syslog....44
5.3.16 Настройка SMTP....45
5.3.16.1 Пример настройки с почтовым сервером внутри локальной сети....46
5.3.16.2. Пример настройки с внешним почтовым сервером....51
5.3.17 Настройка SNMP....53
5.3.17.1 Настройка SNMP v1....53
5.3.17.2 Настройка SNMP v3....54
5.3.18 Удалённый Ping....55

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.19 Статистика 56
..... 56
5.3.19.1 Сводная информация 56
5.3.19.3 ARP таблица 57
5.3.19.5 DNS таблица 57
5.3.19.6 Системный журнал (лог) 58
5.3.20 Обновление ПО 58
5.3.21 Сохранение и восстановление настроек 60
5.3.21.1 Сохранение настроек в файл 60
5.3.21.2 Восстановление настроек из файла 61
5.3.22 Сброс настроек на заводские установки 65
5.3.23 Перезагрузка 65
5.4 Управление через Telnet 66
5.4.1 Пример настройки 68
5.4.2 Описание команд Telnet 69
5.4.3 Группа config 70
5.4.3.1 Сетевые настройки (config ipif) 70
5.4.3.2 Настройка SNMP 71
5.4.3.3 Настройка Syslog 72
5.4.3.4 Настройка SNTP 72
5.4.3.5 Настройка TFTP 72
5.4.3.6 Настройка событий 73
5.4.3.7 Настройка учетных записей пользователей 73
5.4.3.9 Настройка входов 74
5.4.3.10 Настройка выходов 75
5.4.3.11 Настройка RS485 76
5.4.3.12 Настройка Modbus 77
5.4.3.13 Настройка списка удалённых устройств 78
5.4.4 Группа show 79
5.4.4.1 Просмотр сводной информации 80
..... 80
5.4.4.2 Просмотр настроек 81
5.4.5 Обновление ПО через TFTP 85
5.4.6 Сохранение и загрузка конфигурации и лога через TFTP 87
5.4.6.1 Сохранение конфигурации 87
5.4.6.2 Восстановление конфигурации 87
5.4.6.3 Сохранение системного лога 88
5.4.7 Сохранение настроек 88
5.4.8 Перезагрузка 88
5.4.9 Выход из режима управления 88
5.4.10 Диагностические функции 89
5.4.10.1 Утилита Ping 89
6 Диагностика неисправностей 90
7 Гарантии изготовителя 92
8 Техническая поддержка 93

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Условные обозначения

В данном руководстве приняты следующие обозначения:

Обозначение	**Что означает**
	Знак «Обратите внимание».
Basic Settings → Network Settings	При описании настройки через Web-интерфейс, курсивом указывается путь к web-странице
DEFAULT	Полужирным шрифтов выделяется какой-либо значащий параметр, значение, название кнопки и т.д.
`#IPADDRESS=[192.168.0.1]`	Шрифтом Courier New выделяются параметры в файле настроек
<VALUE>	Угловые скобки заменяются на значение переменной в консольной команде
config syslog state <STATE>	Консольная команда выделяется полужирным курсивом
config syslog state enable	Результат выполнения консольной команды выделяется курсивом

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Инструкция по безопасности

Данная инструкция по безопасности рассматривает общие правила работы с оборудованием TFortis.
Для снижения риска нанесения физического вреда, поражения электрическим током и ожогов человека, а также выхода из строя оборудования, необходимо соблюдать следующие меры предосторожности:

- Твердо придерживайтесь указаний маркировки.
- Не обслуживайте устройство при отсутствии документации на него.
- Только обученный сервисный специалист может обслуживать внутренние компоненты устройства.
- При возникновении любого из следующих условий необходимо отключить устройство от электрической розетки, заменить вышедший из строя модуль или связаться с сервисной службой:
  - Повреждение кабеля электропитания, удлинителя или штепселя.
  - Попадание постороннего предмета внутрь устройства.
  - Устройство было подвержено действию воды.
  - Повреждение или падение устройства.
  - Устройство работает некорректно при точном соблюдении инструкций по эксплуатации.
- Держите устройство вдали от радиаторов и источников тепла, а также избегайте перекрытия вентиляционных отверстий, предназначенных для охлаждения.
- Не проливайте пищу или жидкости на компоненты системы, и никогда не работайте с устройством во влажной окружающей среде. Если система была подвергнута воздействию влаги, то необходимо обратиться к специалистам сервисного центра.
- Не помещайте никаких предметов в отверстия системы. Это может привести к возгоранию или электрическому разряду в связи с замыканием внутренних компонентов системы.
- Используйте данное устройство только совместно с сертифицированным оборудованием.
- Прежде чем снять корпус устройства или прикоснуться к его внутренним компонентам, необходимо отключить питание и дать устройству достаточно времени на охлаждение.
- Не используйте устройство с источниками питания, характеристики которых отличны от обозначенных на ярлыке с электрическими параметрами.
- Убедитесь, что характеристики питания подключаемых устройств соответствуют нормам, действующим в данной местности.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• Используйте только подходящие силовые кабели. Силовой кабель должен соответствовать характеристикам напряжения и тока, необходимым для данного устройства.

• Характеристики напряжения и тока кабеля должны быть больше, чем мощность, указанная на устройстве.

• Чтобы избежать удара электрическим током, при работе с устройством пользуйтесь заземленными должным образом электрическими розетками и кабелями.

• Соблюдайте характеристики кабеля-удлинителя и шины питания. Удостоверьтесь, что общий номинальный ток всех устройств, подключенных к кабелю-удлинителю или шине питания, не превышает лимит 80% номинального тока кабеля-удлинителя или шины питания.

• Для обеспечения защиты системы от внезапных кратковременных скачков электропитания используйте ограничитель напряжения, формирователь линии или источник бесперебойного питания (UPS).

SEC.RU | Короткий путь к информации Скачано с sec.ru

1 Назначение

TFortis Teleport предназначены для интеграции коммутаторов TFortis PSW с охранными системами. Блоки имеют дискретные входы и релейные выходы, порт RS-485 и порт Ethernet.

Трансляторы сухих контактов **Teleport** выполняют следующие функции:

- трансляцию состояния «сухих контактов» через Ethernet
- передачу аварийных событий от коммутаторов PSW
- удаленное управление автоматикой

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.1 Варианты применения

1. Контроль несанкционированного доступа к шкафам

Коммутаторы TFortis PSW имеют дискретные входы, к которым можно подключить любые датчики типа «сухой контакт», например герконы, концевики, для организации контроля вскрытия шкафов. Сигнал о вскрытии передаётся коммутатором на Teleport. Т.е. при срабатывании входа на коммутаторе, срабатывает соответствующий выход на блоке Teleport.

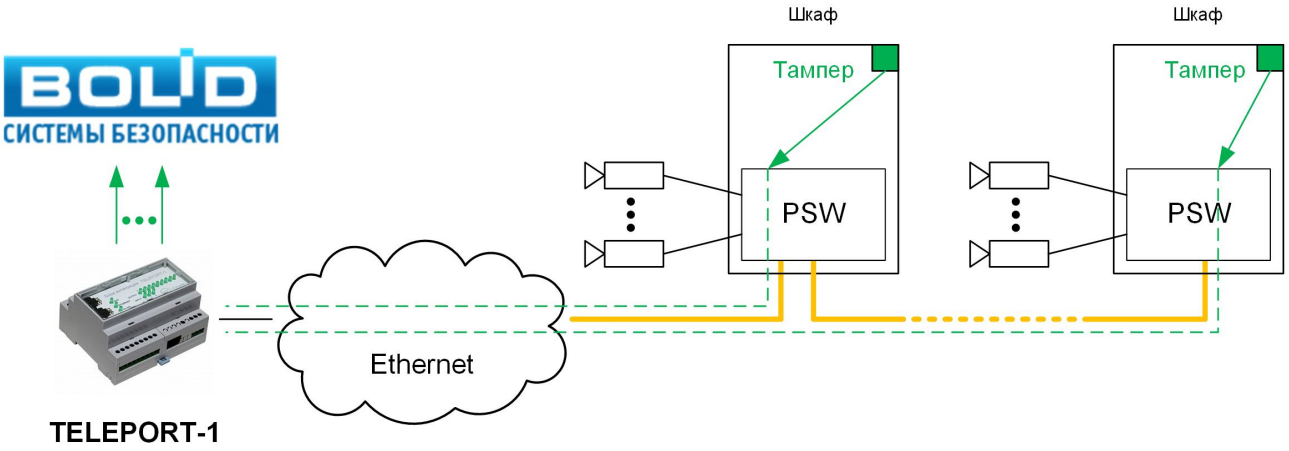


Рис 1.7 Вариант организации трансляции сигналов вскрытия шкафа от коммутаторов TFortis PSW в ИСО "Орион".

2. Удалённое управление автоматикой

Трансляцию входа одного устройства на выход другого можно использовать и для удалённого управления исполнительными механизмами. Однако, следует иметь ввиду, что встроенные выходные реле являются маломощными. Для коммутации мощной нагрузки необходимо использовать дополнительные коммутационные устройства (контакторы).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

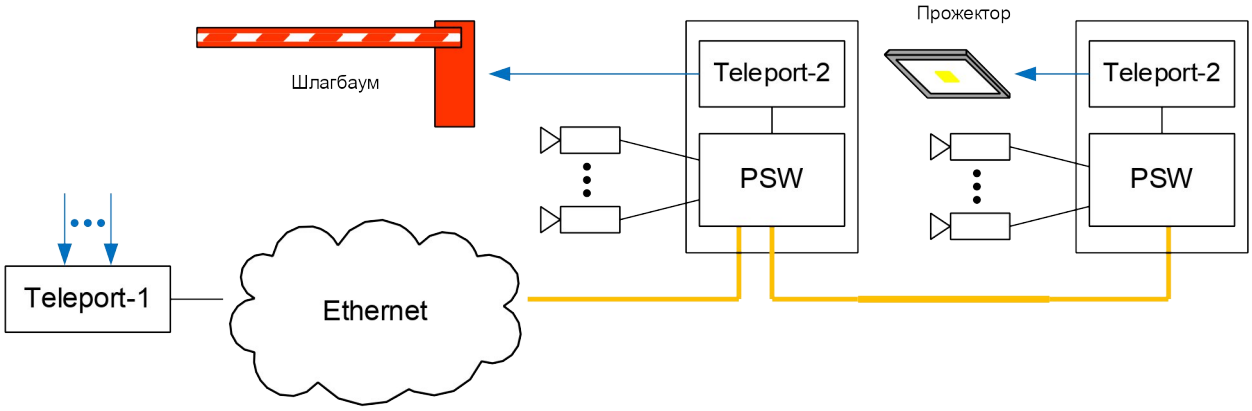


Рис. 1.8 Управление исполнительными механизмами

3. Трансляция аварийных событий от коммутаторов PSW

Коммутаторы TFortis формируют ряд событий, которые могут быть переданы на Teleport:

- Зависание камеры
- Пропало питание 220В
- Обрыв оптики и др.

И уже на стороне сервера эти события преобразуются в логические состояния выходов блока Teleport , которые можно подключить к контроллеру охраны.

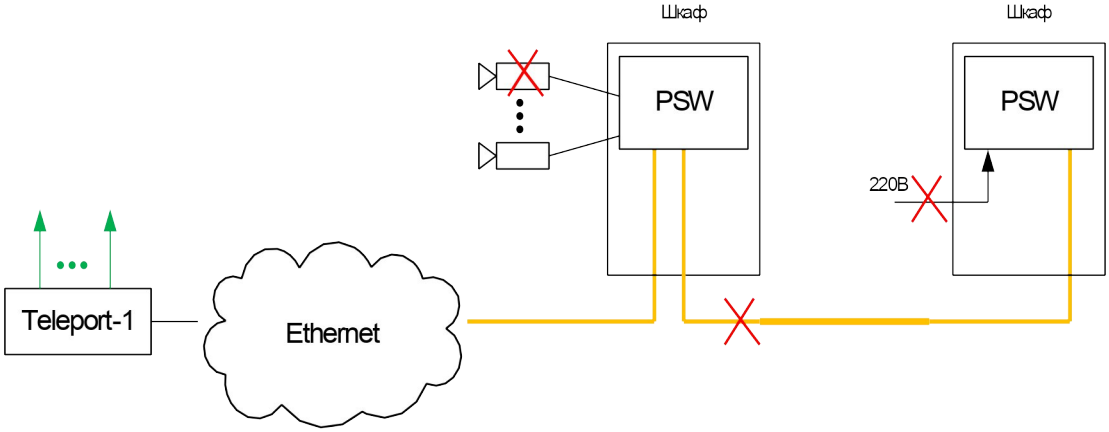


Рис. 1.9 Трансляция аварийных событий

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2 Технические характеристики

2.1 Teleport-1

Ethernet	• 10/100Base-Tx с разъемом RJ-45 — 1шт. • поддержка Auto-MDIX • поддержка управления потоком IEEE 802.3x
RS-485	• скорость до 115 200 бит/сек. • дальность до 100 м • терминирующий резистор встроенный – 120 Ом • без гальванической развязки
Входы	• количество – 3 шт. • замкнутое состояние – менее 200 Ом. • разомкнутое состояние – более 50 кОм. • без гальванической развязки
Выходы	• количество – 9 шт. • нормально разомкнутый контакт • коммутируемое напряжение – 30В • коммутируемый ток – 50мА • сопротивление канала – 10 Ом • гальваническая развязка
Питание	• напряжение питания – 12/24В (от 9В до 27В) • макс. потребляемая мощность – не более 3Вт.
Конструкция	• 106x90x58 мм (ширина 6 модулей) • масса не более 0,3 кг • крепление на DIN рейку (35 мм)
Надежность	• наработка на отказ не менее 50 000 часов
Условия эксплуатации	• температура от плюс 5 до плюс 40 °С • относительной влажности воздуха до 80 %
Хранение	• температура от минус 50 до плюс 50 °С • относительной влажности воздуха до 80 %

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2 Teleport-2

Ethernet	• 10/100Base-Tx с разъемом RJ-45 — 1шт. • поддержка Auto-MDIX • поддержка управления потоком IEEE 802.3x
RS-485	• скорость до 115 200 бит/сек. • дальность не более 100 м • терминирующий резистор встроенный – 120 Ом (с возможностью отключения) • с гальванической развязкой
Входы	• количество – 5 шт. • замкнутое состояние – менее 200 Ом. • разомкнутое состояние – более 50 кОм. • с гальванической развязкой
Выходы	• количество – 1 шт. • нормально разомкнутый контакт • коммутируемое напряжение – 250В • коммутируемый ток – 50мА • с гальванической развязкой
Питание	• PoE (IEEE802.3af Class 3 • максимальная потребляемая мощность - 13Вт • выход питания для внешних устройств: 24VDC (6Вт) с гальванической развязкой, защитой от КЗ и возможностью дистанционного управления
Конструкция	• корпус IP66 • 160x160x90 мм (без учета гермовводов) • масса не более 0,3 кг
Надежность	• наработка на отказ не менее 50 000 часов
Условия эксплуатации	• температура от минус 55 до плюс 50 °С • относительная влажность воздуха до 80 %
Хранение	• температура от минус 55 до плюс 50 °С • относительная влажности воздуха до 80 %

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.3 Поддерживаемые функции и протоколы

- Трансляция состояния входов на выходы удалённого устройства
- Поддержка до **12** удалённых устройств
- Встроенный Web-интерфейс
- Modbus-RTU, Modbus-ASCII, Modbus-TCP клиент
- Telnet
- мониторинг по SNMP v1, v3
- SNTP
- SMTP
- Syslog
- системный журнал
- DNS
- удалённый Ping
- система настройки событий информирования
- обновление ПО через TFTP и Web-интерфейс

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3 Описание

3.1 Внешний вид

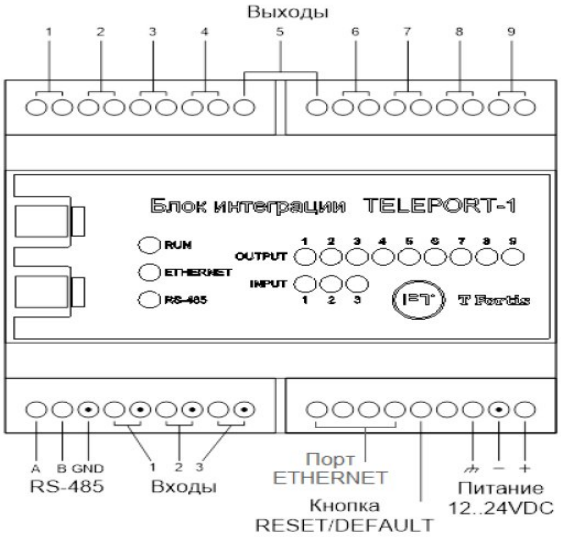


Рис.3.1. Внешний вид Teleport-1

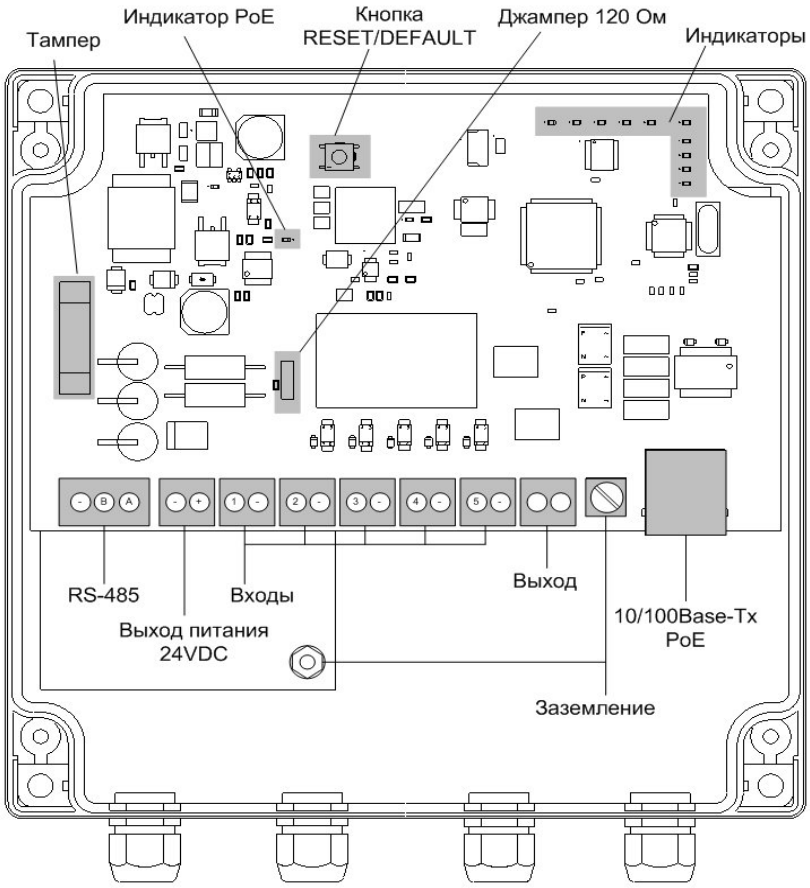


Рис.3.2. Внешний вид Teleport-2 (со снятой крышкой)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.2 Светодиодная индикация

Трансляторы сухих контактов Teleport-1 и Teleport-2 имеют светодиодную индикацию на лицевой панели (Teleport-1) или на печатной плате(Teleport-2), которая отображает работу устройства и состояния входов и выходов.

Индикатор **RUN** отображает режим работы устройства.

Индикатор **ETHERNET** совмещает индикатор линка и активности через порт Ethernet.

Индикатор **RS485** отображает активность на интерфейсе RS485.

Индикаторы **INPUT** отображают текущее состояние входов устройства. Если вход находится в замкнутом состоянии — соответствующий индикатор горит, если в разомкнутом — не горит.

Индикаторы **OUTPUT** отображают текущее состояние выходов устройства. Если вход находится в замкнутом состоянии — соответствующий индикатор горит, если в разомкнутом — не горит.

Данные индикаторы могут быть полезными в процессе настройки и наладки устройства.

Таблица 3.1 Назначение индикаторов

Состояние индикатора	**Состояние устройства**
Индикатор **RUN** мигает (интервал 4 секунды)	Устройство работает на заводских настройках.
Индикатор **RUN** мигает (интервал 1 секунда)	Устройство работает нормально, настройки отличны от заводских
Индикатор **ETHERNET** непрерывно горит	Поднят линк на интерфейсе Ethernet, но обмена данными нет
Индикатор **ETHERNET** мигает	Происходит обмен данных через Ethernet
Индикатор **RS485** мигает	Происходит обмен данных через RS485
Индикаторы **RUN** и **RS485** мигают синхронно	Диагностирована неисправность на аппаратном или программном уровне. Обратитесь в службу технической поддержки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.3 Кнопка сброса настроек и перезагрузки

БИ TFortis Teleport имеет одну кнопку сброса - **RESET**.

В **Teleport-1** кнопка утоплена внутрь корпуса (см. рис. 3.1), для того, чтобы её нажать, воспользуйтесь тонким неметаллическим предметом.

В **Teleport-2** кнопка располагается на печатной плате (см. рис. 3.2), для того, чтобы её нажать, необходимо снять крышку корпуса.

- Для перезагрузки нажмите кнопку **RESET** на 3-5 секунд.
- Для сброса настроек нажмите кнопку **RESET** на 15-20 секунд.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4 Монтаж и подключение

4.1 Монтаж Teleport-1

Трансляторы сухих контактов Teleport-1 предназначены для установки на стандартную DIN-рейку шириной 35 мм. Для установки необходимо использовать DIN-рейку длиной не менее 106мм (ширина 6 стандартных модулей). DIN-рейка располагается горизонтально.

Teleport-1 располагают в отапливаемом помещении на удалении от источников сильного нагрева или охлаждения. Поскольку устройство не имеет гальванической развязки и серьезной защиты от импульсных перенапряжений по Ethernet, входам и RS-485, рекомендуется минимизировать длину подключаемых кабельных линий. Рекомендуется использовать питание от бесперебойных источников питания с выходом 12..24В.

Рекомендуется организация заземления. Наличие заземления позволит увеличить помехоустойчивость устройства.

Подключение линий сухих контактов и Ethernet

Входы устройства не имеют гальванической развязки(как между управляющим микроконтроллером, так и между собой). Поэтому при подключении датчиков, следует иметь в виду, что все входы имеют 2 контакта, один из которых — общий. На блоке общий потенциал обозначен точкой. Контакты, обозначенные точкой «звонятся» (соединены) между собой.

Выходы устройства имеют гальваническую развязку, к ним данное требование не относится.

Для снижения влияния помех, рекомендуется снижать длину линий входов, выходов и Ethernet.

Подключения RS-485 осуществляется кабелем, типа «витая пара». Наличие линии для выравнивания потенциала (GND) является обязательным при большой протяженности линии. Терминирующие резисторы (120 ом) уже установлены внутри корпуса, установка дополнительных резисторов не требуется.

Подключение к серверу или центральному коммутатору осуществляется UTP или FTP патч-кордом.

Запрещается прокладка линий вдоль высоковольтных линий электропитания.

SEC.RU | Короткий путь к информации Скачано с sec.ru

4.2 Монтаж Teleport-2

Teleport-2 допускает установку в уличных условиях на любых металлических/неметаллических поверхностях, рядом с контроллерами охраны периметра, т.к. корпус устройства обеспечивает защиту от пыли и влаги IP66. Однако, установка рядом с коммутаторами PSW в уличных металлических шкафах с защитой не ниже IP54, позволяет увеличить удобство монтажа и обеспечивает хорошую вандалозашищенность.

Teleport-2 предусматривает крепление к задней фальш-стенке уличного шкафа TFortis CrossBox-2 и CrossBox-3 через «Монтажную панель PSW-11»

Рис.4.1. Монтаж блока в шкафу

Крепление блока к переходной пластине осуществляется винтами М4(не поставляются). Винты крепления переходной пластины поставляются в комплекте с монтажной пластиной.

Также допускается монтаж и вне шкафа. Для монтажа используются винты М4 или универсальные саморезы диаметром 4 мм.

Организация заземления

Наличие заземления обязательно. При отсутствии заземления, а также при некачественно выполненном заземлении компоненты грозозащиты не работают или работают не в полном объёме. Наличие заземления позволяет существенно повысить устойчивость устройства к электромагнитным импульсным помехам.

Заземление осуществляется через клемму заземления или шпильку заземления (рис. 3.2).

Заземление через экран FTP кабеля **не допускается**!

Сопротивление заземления **не более 4 ом**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Подключение линий сухих контактов и Ethernet

Входы и выходы устройства имеют гальваническую развязку и устойчивы к импульсным помехам. Однако, для снижения влияния помех, рекомендуется снижать длину линий входов, выходов, RS-485 и Ethernet.

Подключения RS-485 осуществляется кабелем, типа «витая пара». Наличие линии для выравнивания потенциала (GND) является обязательным. Терминирующие резисторы (120 ом) уже установлены внутри устройства, установка дополнительных резисторов не требуется. Существует возможность отключить терминирующие резисторы. По умолчанию резисторы подключены.

Подключение к PoE коммутатору осуществляется при помощи качественного уличного FTP кабеля.

Запрещается прокладка линий вдоль высоковольтных линий электропитания.

Выходы устройства не рассчитаны на коммутацию мощной нагрузки.

Герметизация вводов

Устройство поставляется с комплектом гермовводов. При установке вводов, их необходимо надёжно затянуть. Неиспользуемые вводы необходимо загерметизировать герметиком или пластиковым грибком.
Нарушения в монтаже гермовводов не гарантируют соответствие устройства классу защиты IP66.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5 Настройка

5.1 Интерфейсы управления

Трансляторы сухих контактов TFortis Teleport имеют несколько вариантов удалённого управления: WEB-интерфейс, Telnet, при помощи фирменной утилиты **TFortis Device Manager**.

WEB-интерфейс содержит наиболее полный набор контролируемых параметров, снабжённых подробными разъяснениями и краткой справкой. Интерфейс представлен на русском и английском языках. Подключение к БИ возможно при помощи обычного Web-браузера.

Telnet представляет собой альтернативную форму конфигурирования устройства посредством консольного приложения такого как Microsoft Telnet, PuTTY, Hyper Terminal и других.

SNMP используется для мониторинга состояний и параметров.

При помощи программы **TFortis Device Manager** можно осуществлять широковещательный поиск устройств и дистанционную настройку. Использование программы может быть полезным, когда неизвестны сетевые настройки Блоков интеграции Teleport, а также когда присутствует дублирование IP адресов (В случае, когда в сети присутствуют несколько устройств с одинаковыми IP адресами, стандартные методы настройки, такие как настройка через Web-интерфейс, не применимы).

5.2 Что нужно знать перед подключением

Обратите внимание!

Выходы устройства не рассчитаны на коммутацию мощной нагрузки.

Teleport-2 содержит выход 24 VDC для питания периферийных устройств.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3 Управление через WEB-интерфейс

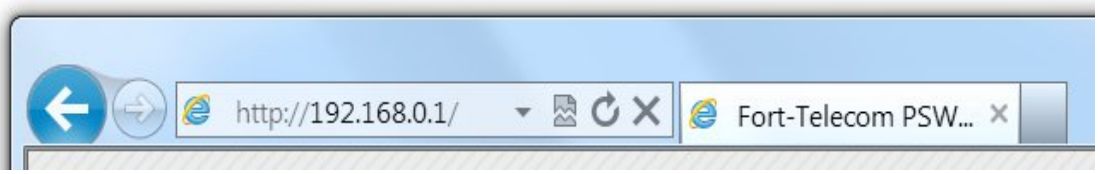
5.3.1 Первое подключение, быстрый старт

При первом включении, устройство имеет следующие сетевые настройки по умолчанию:

IP адрес:	192.168.0.1
Маска подсети:	255.255.255.0
Логин/Пароль	не заданы
DHCP клиент	выключен
Telnet	включен
SNMP	выключен

Перед подключением убедитесь, что сетевая карта компьютера находится в той же подсети, что и Teleport (192.168.0.*).

Запустите Web-браузер и в адресной строке введите IP адрес **192.168.0.1** рис



5.3.1.1)

Рис. 5.3.1.1. Подключение

После подключения, мы должны попасть на главную страницу web-интерфейса.(рис 5.3.1.2)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

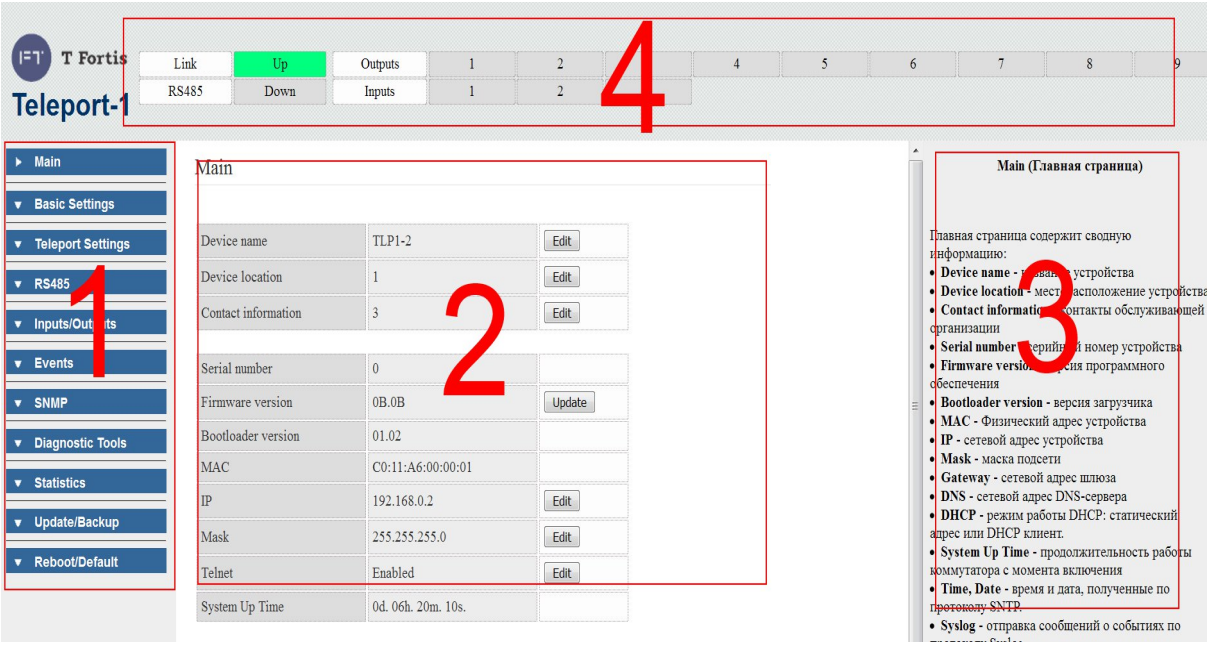


Рис. 5.3.1.2. Web-интерфейс

Web-интерфейс можно разделить на 4 зоны - фрейма, как показано на рисунке 5.3.1.2:

1 - боковое меню, через него осуществляется доступ к различным группам настройки

2 - основной фрейм, содержащий группу настроек

3 - справка по данным настройкам

4 - шапка с состоянием входов и выходов (автоматически обновляется каждые 10 секунд)

Примечание: при заводских настройках логин и пароль для доступа к web-интерфейсу не установлен, в последующем рекомендуется ограничить доступ, установив логин и пароль. При этом каждое последующие подключение к будет сопровождаться стандартным диалоговым окном аутентификации.

После подключения к web-интерфейсу, перейдём к настройке. Но перед этим мы должны чётко представлять себе карту сети, где какие блоки располагаются, и какие функции несут.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Пример настройки

Рассмотрим на примере, как на рис. 5.3.1.3.

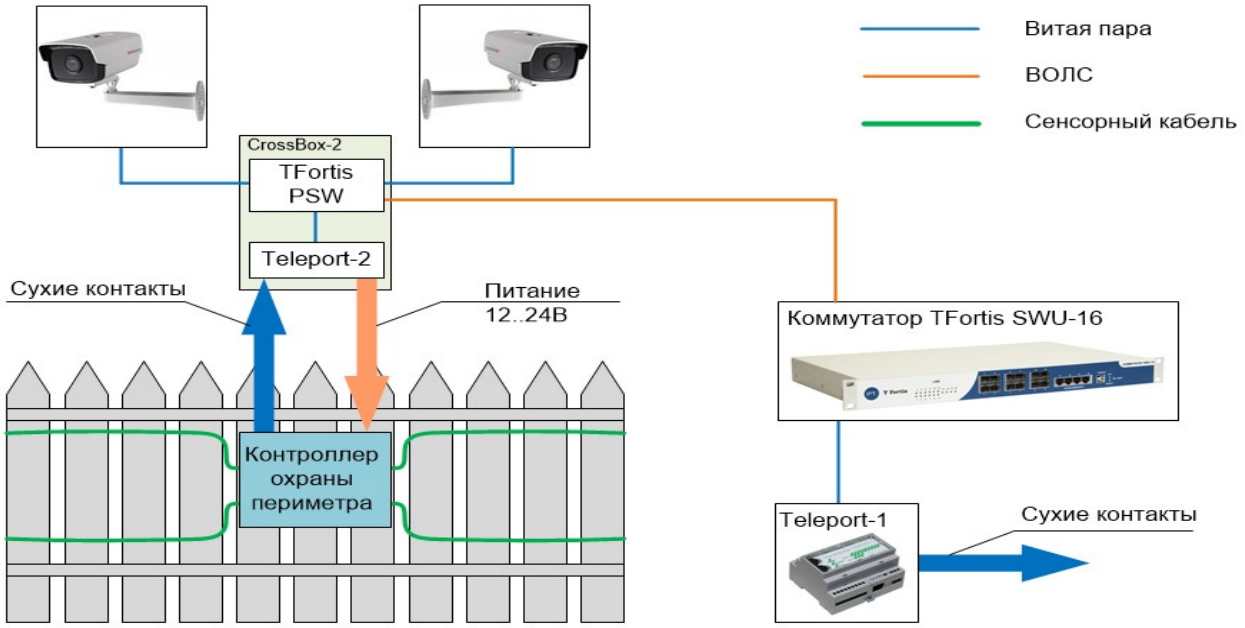


Рис. 5.3.1.3. структура системы

На данном примере рассматривается система охраны периметра, которая значительно удалена от сервера сбора и обработки информации (ССОИ). Контроллер охраны периметра осуществляет контроль за чувствительными кабельными элементами и оповещает о срабатывании через стандартный интерфейс «сухих контактов». Также по периметру расставлены камеры видеонаблюдения, подключенные к коммутатору TFortis PSW. Эта связка оборудования формирует Узел охраны. При применении такой системы мы должны соединить Сервер и Узел. Однако бывает так, что удалённость Узла от Сервера может быть очень большой. Единственным решением может стать применение оптоволоконных линий связи для сети Ethernet. А для RS-485 в таком случае можно реализовать виртуальный канал - «трубу» через Ethernet.

На устройстве Teleport-2 осуществляется преобразование «сухие контакты» → Ethernet. Данные проходят через коммутатор узла — TFortis PSW, а затем по оптике через центральный коммутатор, затем в Teleport-1, где осуществляется обратное преобразование Ethernet → «сухие контакты».

Для организации виртуального канала между двумя устройствами Teleport-1 и Teleport-2 их необходимо настроить.

В общем случае процесс настройки выглядит следующим образом:

1. Конфигурируем сетевые настройки
2. Прописываем удалённое устройство (Для Teleport-1 – это Teleport-2 и наоборот)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Настройка входов и выходов в режим парного соединения с удалённым устройством.

Сетевые настройки

В сетевых настройках Блока необходимо задать уникальный в пределах подсети IP адрес. Допустим, что Teleport-1 имеет IP 192.168.0.1, а Teleport-2 192.168.0.2. Меняем эти поля, как показано на рис. 5.3.1.4, для чего в боковом меню выбираем **Basic Settings → Network Settings**

MAC	C0 11 A6 00 00 01
IP	192 168 0 1
Mask	255 255 255 0
Gateway	255 255 255 255
DNS	255 255 255 255
DHCP Mode	Disable

Рис. 5.3.1.4 сетевые настройки устройства Teleport-1

Список удалённых устройств

Для того, чтобы Teleport-1 “знал” о Teleport-2, а Teleport-2 знал о Teleport-1 их необходимо «познакомить». Для чего на каждом устройстве существует список удалённых устройств. В него заносятся все устройства, с которыми может взаимодействовать локальное устройство.

Рассмотрим на примере Teleport-1. Для него удалённым устройством будет Teleport-2. Поэтому заходим на web-интерфейс Teleport-1, во вкладке **Teleport Settings → Remote Devices**. Как видим пока список пуст, заносим туда Teleport-2, указывая его IP адрес, тип (Teleport-2) и пользовательское описание, по которому его легче опознавать. Нажимаем **Apply**.

Remote Devices

Devices List

	Name	Type	IP Address	

Device list is empty

Add New Remote Device

Name	описание
Type	Teleport-2
IP Address	192 168 0 2

Apply

Рис. 5.3.1.5 настройка удалённых устройств Teleport-1

SEC.RU | Короткий путь к информации Скачано с sec.ru

Как мы видим на рис. 5.3.1.6, Teleport-2 добавлен в список.

Devices List

	Name	Type	IP Address	
1	описание	Teleport-2	192.168.0.2	Info Edit Delete

Рис. 5.3.1.6 список удалённых устройств Teleport-1

Аналогичную настройку производим и на web-интерфейсе Teleport-2.

Devices List

	Name	Type	IP Address	
1	описание2	Teleport-1	192.168.0.1	Info Edit Delete

Add New Remote Device

Name	
Type	Teleport-1
IP Address	

Apply

Рис. 5.3.1.7 настройка удалённых устройств Teleport-2

Нажимаем **Apply** для применения настроек. Те же самые настройки проводим и на другом устройстве.

Далее нам необходимо настроить вход 1 на Teleport-2 для трансляции его на выход 1 Teleport-1

Inputs

	Active	Description	Operation Mode	Remote Device	Remote Port	Inverse	Current State
1	☑		Pair Connection	192.168.0.1	Out 1	☐	Open

Рис. 5.3.1.8 настройка входа для трансляции на выход удалённого устройства

Аналогично настраиваем выход 1 на Teleport-1 для привязки к Teleport-1

SEC.RU | Короткий путь к информации Скачано с sec.ru

Outputs

	Description	Operation Mode	Remote Device	State	Err. State	Current State
1		Pair Connection	192.168.0.2		Last state	Open

Рис. 5.3.1.9 настройка выхода для трансляции на выход удалённого устройства

На этом настройка завершена.

5.3.1.1 Стратегия настройки

В предыдущем разделе был рассмотрен процесс настройки на конкретном примере, а весь процесс настройки можно разбить на несколько ключевых этапов.

1. **Установка сетевых настроек** (задание уникального IP адреса в пределах подсети, установка маски и шлюза).
2. **Установка логина и пароля** для ограничения доступа к настройкам.
3. **Создание списка удалённых устройств.**
4. **Настройка входов, выходов, RS-485**. Указание режимов работы, удалённых устройств.
5. **Настройка мониторинга.** Для удобства администрирования можно настроить отправку событий через протоколы Syslog, SMTP, SNMP, синхронизировать внутренние часы через протокол SNTP.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.2 Сетевые настройки

Basic Settings → Network Settings
В данном разделе указываются основные сетевые настройки блока.

MAC:	C0 11 A6 04 00 02
IP:	192 168 0 2
Mask	255 255 255 0
Gateway	255 255 255 255
DNS	255 255 255 255
DHCP Mode	Disable

Рис. 5.3.2.1 Сетевые настройки

MAC - Физический адрес устройства используется для идентификации устройства в сети. Без крайней необходимости, не рекомендуем менять MAC адрес, поскольку он гарантировано обеспечивает уникальность устройства в сети. Последние 2 байта заводского MAC адреса составляют серийный номер устройства. Заводской MAC адрес нанесен на наклейке и размещен на корпусе.

IP - Сетевой адрес устройства. При работе в пределах одной подсети необходимо обеспечить уникальность сетевого адреса.

Mask - Маска подсети

Gateway - Сетевой адрес шлюза. Если шлюз не используется, то оставьте значение по умолчанию: *255.255.255.255*

DNS - Сетевой адрес DNS ресолвера. Используется в некоторых функциях для преобразования символьного имени хоста в его сетевой адрес. Если не используется, то оставьте значение по умолчанию: *255.255.255.255*

DHCP Mode - выбор режима работы с протоколом DHCP:

1. *Disable* - DHCP отключен. БИ использует статические сетевые настройки. (IP, Mask, Gateway и др.)

2. *Client* - включене режима DHCP клиента. БИ получает сетевые настройки автоматически путем широковещательного запроса к DHCP серверу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.3 Настройка учётных записей пользователей

Basic Settings → User Accounts

В данном разделе содержатся настройки учетных записей пользователей.

User list

	User Name	Password	Access Right	
1			Admin	Edit
2				Add New User

Рис. 5.3.3.1 Список пользователей

По умолчанию единственной учетной записью является учетная запись администратора с неустановленными именем пользователя и пароля. Т.е. доступ к WEB- интерфейсу и Telnet происходит без аутентификации.

Для ограничения доступа обязательно следует создать как минимум одного пользователя с правами **Admin**. И, при необходимости одного или нескольких пользователей с правами **User**.

Разделение прав доступа осуществляется выбором поля Access Right

Add/Edit user

User Name	user
New Password	••••
Password Confirm	••••
Access Right	Admin / User

Apply Cancel

Рис. 5.3.3.2 Настройки имени пользователя и пароля

Пользователь с правами **Admin** имеет максимальные полномочия.

Пользователь с правами **User** имеет ограниченные полномочия, не может изменять настройки, имеет доступ к статистике и диагностическим инструментам (Ping).

После применения параметров, если все прошло успешно, отобразится сообщение "*Parameters accepted*" и потребуется пройти авторизацию, введя логин и пароль.

При сообщении об ошибке, попробуйте ввести данные еще раз.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание 1: Данные поля являются обязательными для заполнения. Максимальная длина - 20 символов. Язык ввода — английский, спецсимволы поддерживаются
Примечание 2: Поля регистрозависимые, т.е. есть разница между "Admin" и "admin".
Примечание 3: Поддерживается до 4 учетных записей.

5.3.4 Описание устройства

Basic Settings → Device Description

Device Name	
Device Location	
Service Company	

Рис. 5.3.4.1 Описание устройства

Device Name - Название устройства
Device Location - Расположение устройства
Service Company - Контактная информация обслуживающей компании или ответственного лица

Данные поля являются необязательными для заполнения и служат лишь для упрощения идентификации устройства. Максимальная длина записей - 64 символа при использовании английского языка и 32 символа при использовании русского.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.5 Настройка языка web-интерфейса

Basic Settings → Language

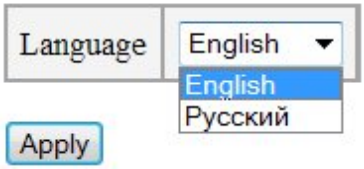


Рис. 5.3.5.1. Выбор языка

Teleport имеет возможность выбора языка для Web-интерфейса. Поддерживается 2 языка: русский и английский. По умолчанию установлен английский язык, однако его можно поменять на русский, но при этом нужно убедиться чтобы не было проблем с кодировками текста в браузере.

В Web-интерфейсе используется кодировка **UTF-8**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.6 Настройка режима трансляции

Устройства Teleport выполняют следующие режимы трансляции:

- **трансляцию «сухих контактов» через Ethernet и передачу аварийных событий от коммутаторов PSW.** В этом режиме транслируются состояния входов на блоках Teleport или входы коммутаторов TFortis на выходы других блоков Teleport. (До 32 устройств)

При трансляции RS-485 через Ethernet следует учитывать, что из-за преобразования данных неизбежно возникают задержки. Для того, чтобы не возникало сбоев в работе системы, следует учитывать это учитывать, устанавливая таймауты. Подробнее про методику расчёта таймаутов см. стр. 95.

5.3.6.1 Настройка списка удалённых устройств

Teleport Settings → Remote Devices

Devices List

	Name	Type	IP Address	
1	123	Teleport-1	192.168.0.1	Info Edit Delete

Add New Remote Device

Name	
Type	Teleport-1
IP Address	

Рис. 5.3.6.1. добавление удалённых устройств

Первым этапом в настойке связки устройств, использующихся для трансляции состояния входов типа «сухой контакт» и данных RS-485 является создание списка устройств, на которые пересылаются данные. Список удалённых устройств заполняется только в этой вкладке.

В этот список заносятся все удалённые устройства, с которыми может взаимодействовать локальное устройство. Механизмы взаимодействия (трансляции) настраиваются позже в других разделах.

SEC.RU | Короткий путь к информации Скачано с sec.ru

При добавлении нового устройства заполняются следующие поля:

Name — описание устройства, это поле можно не заполнять, но оно может помочь для дальнейшей идентификации устройства.

Type — тип удалённого устройства,

IP Address— IP адрес удалённого устройства

Нажатие кнопки **Apply** сохраняет настройки.

Кнопка **Edit** – редактирование настроек удалённого устройства, а **Delete** – удаление.

При нажатии на **Info** будет показана подробная информация об устройстве, статус соединения, число входов/выходов и др.

Remote Device Info

Name	123
Type	Teleport-1
Inputs num	3
Outputs num	9
IP Address	192.168.0.1
Connection status	Not connected
RX mngmt frames	0
TX mngmt frames	0

Refresh

Рис. 5.3.6.2. подробная информация об устройстве

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.7 Настройка порта RS-485

RS-485 → RS-485 Settings

В данном разделе производится настройка порта RS-485. Настройку можно разделить на 2 части: настройка физических параметров интерфейса и режим работы.

Настройка физических параметров интерфейса:

- **Baudrate** - скорость порта(бит в секунду)
- **Parity** - проверка на чётность: **Disable** - отключена; **Even** - Чет.;**Odd** - Нечет.
- **Data Bits** - число бит данных
- **Stop Bits** - число стоповых битов

RS-485 Settings

Baudrate	9600
Parity	Disable
Data Bits	8
Stop Bits	1

Рис. 5.3.7.1. настройка RS-485

Настройка режима работы

Operation mode

Mode	Disabled
Apply	

Disabled
Modbus RTU/ASCII Client

Рис. 5.3.7.2. настройка режима работы

Для интерфейса поддерживается клиент Modbus RTU/ASCII.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим клиента Modbus RTU/ASCII

В этом режиме Teleport является клиентом протоколов Modbus RTU или Modbus ASCII. Сама настройка протокола Modbus производится в в разделе 5.3.10 - Настройка Modbus.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.8 Настройка цифровых входов

Inputs/Outputs → Inputs

Рис.

Inputs

	Active	Description	Operation Mode	Remote Device	Remote Port	Inverse	Current State
1	☑	датчик движения	Pair Connection	123	Out 1	☐	Open
2	☑	геркон шкафа	Pair Connection	123	Out 2	☑	Open
3	☐						Open

Apply

5.3.8.1. настройка входов

Входы Teleport могут быть ретранслированы на выход другого удалённого устройства.

- **Active** - разрешение работы входа. Если галочка установлена вход становится активным и его состояние может быть ретранслировано на удалённое устройство.
- **Description** - описание входа, может быть использовано для облегчения процесса настройки.
- **Pair Connection** - режим "парного соединения", состояние входа будет транслироваться на выход удалённого устройства. На данный момент это единственный режим работы входа.
- **Remote Device** - удалённое устройство, на которое будет транслироваться состояние входа. Если Вход активен, то необходимо указать куда этот вход ретранслировать, то есть задать удалённое устройство.
- **Remote Port** - номер выхода удалённого устройства, на который будет транслироваться состояние входа
- **Inverse** - инверсия входа. На удалённое устройство будет ретранслироваться инверсное состояние входа. Например, при замыкании датчика, подключенного к этому входу, выходное реле на удалённом устройстве будет размыкаться.

Current State - текущее состояние входа:
Open - вход разомкнут, логический "0"
Short - вход замкнут, логическая "1"

Настройки применяются и сохраняются после нажатия **Apply.**

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если нет необходимости в ретрансляции входа, но необходимо каким-либо образом узнавать о состоянии входа, то для этого можно воспользоваться рядом способов:

1) получение сообщений о изменении состояния входа по протоколу Syslog, SMTP, SNMP-Traps.

2) отправкой запросов по протоколу SNMP

3) отправкой запросов по протоколу Modbus

5.3.9 Настройка цифровых выходов

Inputs/Outputs → Outputs

Outputs

	Description	Operation Mode	Remote Device	State	Err. State	Current State
1		Pair Connection	TLP-11		Open	Open
2		Pair Connection	TLP-12		Open	Open
3		Pair Connection	TLP-13		Last state	Open
4		Manual		Short		Open
5		Manual		Open		Open
6		Manual		Open		Open
7		Manual		Open		Open

Рис. 5.3.9.1. настройка выходов

Teleport содержит несколько управляемых слаботочных твердотельных реле.

Выходы поддерживают несколько режимов управления (**Operation Mode**)

1. **Pair Connection** - Режим парного соединения. В этом режиме выход используется для ретрансляции состояния входа удалённого устройства. На удалённом устройстве (с которого необходимо ретранслировать вход) вход переводится также в **Pair Connection**. Для этого режима необходимо указать удалённое устройство в поле **Remote Device**. Если удалённое устройство не указано, то выход не будет реагировать на управляющие команды. В данном режиме Выход может быть изменён только по управляющей команде от входа.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если в ходе работы пропала связь с удалённым устройством, то состояние выхода переводится в состояние **Err. State.**

2. **Manual** - Режим ручного управления. Выход может быть вручную установлен в нужное состояние через Web-интерфейс или Telnet.
   Open – выходное реле разомкнуто.
   Short – выходное реле замкнуто.
   Также в этом режиме порт может быть установлен в соответствующее состояние через протоколы SNMP, Modbus или в режиме сетевого контроллера входов/выходов.

Для мониторинга состояния выходов можно использовать несколько вариантов:

1) получение сообщений о изменении состояния выхода по протоколу Syslog, SMTP, SNMP-Traps.

2) отправкой запросов о состоянии выхода по протоколу SNMP

3) отправкой запросов о состоянии выхода по протоколу Modbus

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.10 Настройка Modbus

Modbus → Modbus Settings

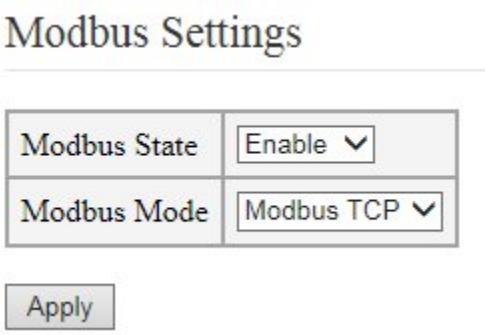


Рис. 5.3.10.1. настройка выходов

Транслятор Teleport может быть Modbus клиентом. Поддерживаются следующие режимы:

- Modbus TCP
- Modbus RTU
- Modbus ASCII

По протоколу Modbus можно считывать состояние входов и выходов и управлять выходами.

Адресное пространство для протокола Modbus

Адрес регистра	значение
00001-00009 (00001)	Состояние цифровых выходов для Teleport-1 (Teleport-2)
10001-10003 (10001-10005)	Состояние цифровых входов для Teleport-1 (Teleport-2)

Teleport поддерживает следующие функции протокола:

- (0x01) Read Coil Status – чтение цифрового выхода
- (0x02) Read Discrete Inputs — чтение цифрового входа
- (0x05) Write SingleCoil Status — запись единичного выхода
- (0x0F) Write Coil Status — запись группы выходов

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.11 Настройка режима сетевого контроллера входов/выходов

Teleport→ PLC

Teleport поддерживает функции сетевого контроллера (управление входами и выходами).

State	Disable			
UDP Port	7000			
Period	1000			
Server 1	0	0	0	0
Server 2	0	0	0	0
Server 3	0	0	0	0
Server 4	0	0	0	0

Рис. 5.3.11.1. настройка режима сетевого контроллера

State - состояние. Enable - включение поддержки функции, Disable - выключение поддержки функции.

Управление выходами осуществляется через http-запрос вида:
xx.xx.xx.xx/digitaloutput/all/value?DO0=0&DO1=1&DO2=0, где

xx.xx.xx.xx - IP адрес блока,
DO0=0 - установка выхода 0 в состояние 0(разомкнуто),
аналогично DO1=1 для выхода 1 в состояние 1(замкнуто). Аналогично и для других выходов

Получение состояния входов осуществляется периодической отправкой (с периодом Period, задаётся в мс.) UDP пакетов на порт UDP Port и адреса серверов (Server 1 - Server 4). Формат отправки соответствует формату в контроллерах Advantech ADAM6066.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.12 Настройка списка событий

Events → Event List

Teleport имеет широкие возможности по обеспечению удобства администрирования. Важную роль в этом играет механизм немедленного уведомления администратора о произошедших событиях посредством различных механизмов, таких как Syslog, SMTP (e-mail) или SNMP Trap.

Имеется возможность гибко настроить реагирование только на интересующие события и присвоить им соответствующий уровень важности (только для протокола Syslog). Уровни меняются от 0 до 7, где 0 - наивысший уровень важности.

Parametrs	State	Level
System	☑	(4) Warning
Inputs	☑	(4) Warning
Outputs	☑	(6) Informational

Рис. 5.3.12 Список событий

Общепринята следующая градация уровней:

- **(0) Emergency**: система неработоспособна
- **(1) Alert**: система требует немедленного вмешательства
- **(2) Critical**: состояние системы критическое
- **(3) Error**: сообщения о возникших ошибках
- **(4) Warning**: предупреждения о возможных проблемах
- **(5) Notice**: сообщения о нормальных, но важных событиях
- **(6) Informational**: информационные сообщения
- **(7) Debug**: отладочные сообщения

Используя такое логическое разделение уровней важности событий, на стороне сервера можно по-разному их обрабатывать. Например, сообщения о событиях с уровнем 6,7 могут просто писаться в журнал событий, а сообщения о событиях с уровнем 0-3 выводятся оператору.

Настройки разбиты на подгруппы по категориям:

- **System** - изменение состояния системы(перезагрузка, обновление, сброс на заводские установки и др.)
- **Inputs** — событие при изменении состояния входов
- **Outputs** - событие при изменении состояния выходов

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.13 Настройка Telnet

Basic Settings → Telnet

Telnet Settings

State	Enable
Option Echo	Enable

TFTP Settings

State	Enable
Port	69

Рис. 5.3.13.1. Включение Telnet и TFTP

Telnet - протокол для реализации удалённого управления сетевым оборудованием, основанный на протоколе TCP порт 23.

По умолчанию Telnet включен, по желанию его можно отключить. Логин и пароль для доступа к Telnet такие же, что используются для доступа к web-интерфейсу.

Option Echo – опция протокола Telnet, по умолчанию опция включена.

Кроме того существует возможность производить обновление прошивки через Telnet, при этом используется протокол TFTP.

Поскольку протокол TFTP не является защищенным, то он по умолчанию выключен. При необходимости можно включить, а также изменить стандартный UDP порт (69) на другой.

Более подробно конфигурирование при помощи Telnet рассмотрено в разделе 5.4.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.14 Настройка SNTP

Basic Settings → SNTP

State	Enable
Server IP address	192 168 0 81
Server Name	
Time Zone	+5
Period	10

Рис. 5.3.14.1. Настройка SNTP

SNTP (Simple Network Time Protocol) – протокол, с помощью которого блок синхронизирует свои внутренние часы с внешним сервером точного времени.

Teleport не содержит встроенных часов реального времени, поэтому для получения сведений о текущем времени необходимо использовать протокол SNTP. Применение протокола SNTP не является обязательным, основные функции БИ никак не связаны с SNTP. Однако, для упрощения администрирования Teleport поддерживает запись журнала событий в «черный ящик», отправку syslog- и e-mail- сообщений о событиях администратору сети. И в эти сообщения, при включенном протоколе SNTP, добавляется штамп времени, что в свою очередь может помочь администратору при обслуживании сети.

Параметры настройки:

State — состояние

Server IP address - IP адрес SNTP сервера

Server Name – доменное имя SNTP сервера. Если задан IP адрес сервера и доменное имя одновременно, то приоритет отдаётся IP адресу

Time Zone - часовой пояс (отклонение от UTC)

Period - период времени синхронизации с сервером.(в минутах)

Synchronize – принудительная синхронизация времени (для проверки настроек)

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.15 Настройка Syslog

Events → Syslog

Syslog — стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в IP сетях. Протокол syslog прост: при наступлении определенных событий, Teleport посылает короткое текстовое сообщение, размером меньше 1024 байт получателю сообщения. Сообщения отправляются по UDP (порт 514). Syslog используется для удобства администрирования и обеспечения информационной безопасности.

Имеется возможность гибко настроить только интересующие события и присвоить им соответствующий уровень важности. (Вкладка Events → Event List) Уровни меняются от 0 до 7, где 0 - наивысший уровень важности.

Общепринята следующая градация уровней:

- **(0) Emergency**: система неработоспособна
- **(1) Alert**: система требует немедленного вмешательства
- **(2) Critical**: состояние системы критическое
- **(3) Error**: сообщения о возникших ошибках
- **(4) Warning**: предупреждения о возможных проблемах
- **(5) Notice**: сообщения о нормальных, но важных событиях
- **(6) Informational**: информационные сообщения
- **(7) Debug**: отладочные сообщения

Используя такое логическое разделение уровней важности событий, на приемной стороне можно по-разному их обрабатывать. Например, сообщения о событиях с уровнем 6,7 могут просто писаться в журнал событий, а сообщения о событиях с уровнем 0-3 выводятся оператору.

Формат Syslog сообщения

Согласно стандарту Syslog сообщение имеет следующий формат:
<уровень важности><дата и время><IP адрес отправителя><сообщение>

Примечание: обратите внимание, что в поле <дата и время> подставляется дата и время полученные по протоколу SNTP. Если данные времени не получены или SNTP не настроен, то в поле <дата и время> подставляется время в секундах, прошедшее с момента подачи питания.

Рассмотрим это на примере. Пусть у нас дано сообщение, полученное программой Wireshark:

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
LOCAL0.WARNING:  <245>192.168.0.2 Port #4 Link Up
```

Рис. 5.3.15.1. SNTP не настроен

Как видим, время не настроено, подставлено значение с момента старта.

```
LOCAL0.WARNING:  Sep 22 10:08:43 192.168.0.2 Port #4 Link Down
```

Рис. 5.3.15.2. SNTP настроен

А теперь сообщение имеет стандартный штамп времени.

Настройка Syslog

Настройка не представляет особой сложности. Первое, что нужно сделать — это выбрать интересующие события во вкладке Events → Event List. Например, нас интересует событие изменения входов.

Parametrs	State	Level
System	☐	(4) Warning
Inputs	☑	(4) Warning
Outputs	☐	(6) Informational

Рис. 5.3.15.3. Выбираем событие

Затем во вкладке Events → Syslog Settings включаем работу с протоколом Syslog и устанавливаем IP адрес сервера, на который будут приходить сообщения.

State	Enable
Server IP address	192 168 0 104

Рис. 5.3.15.4. Настройка Syslog

Получение Syslog сообщений

После настройки на устройстве, переходим к настройке сервера.
Рассмотрим пример для ОС Windows. Существует большое число программ для работы с syslog-сообщениями. Вот некоторые из них:

- Kiwi Syslog
- Syslog Watcher
- Datagram SyslogServer Suite
- syslogbroadband
- LogZilla
- Syslog Server Free Tool

SEC.RU | Короткий путь к информации Скачано с sec.ru

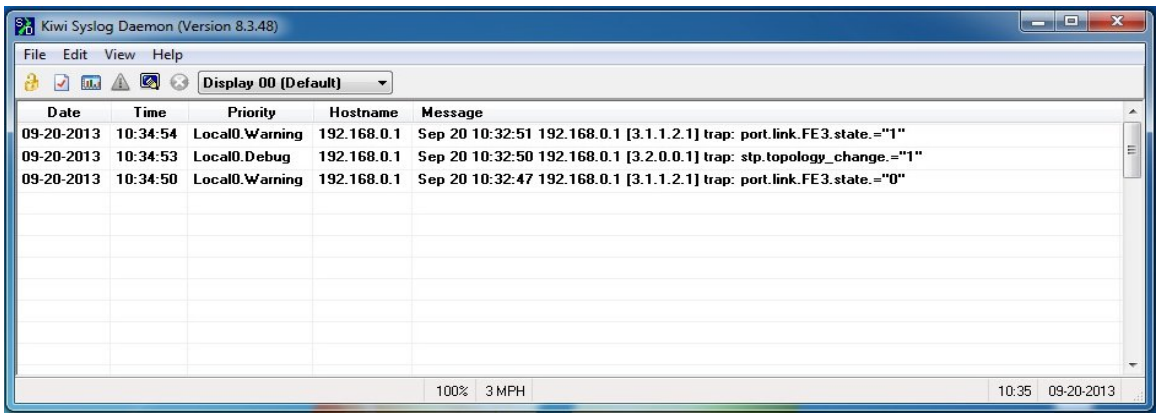
Остановим свой выбор на программе Kiwi Log Viewer - это бесплатная упрощенная версия программы Kiwi Syslog Server. Но тем не менее она удовлетворяет поставленным задачам.
Адрес для загрузки - http://www.kiwisyslog.com/downloads.aspx

Установка программы не отличается особой сложностью, единственное, в окне Chose Operating Mode установите Install as Service (В этом случае Kiwi Syslog установится как служба: будет запускаться при старте ОС и резидентно сидеть в трее)

Рис. 5.3.15.5. Установка программы Kiwi Syslog

После установки, запускайте программу. По умолчанию в главном окне будут отображаться все принятые сообщения. Эти сообщения пишутся в текстовый файл. Также есть возможность настроить пересылку на email.

Рис.



5.3.15.6. Интерфейс программы Kiwi Syslog

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.15.1 Список сообщений Syslog

Таблица 5.3.1. Список Syslog сообщений

`Web-interface authentication: Ok`	Вход на WEB-интерфейс с паролем
`Update firmware x.x.x`	Обновление ПО
`Default settings`	Сброс настроек на заводские установки
`Clear ARP cash`	Очистка ARP кэша
`Start after power reset`	Старт после снятия питания
`Start after reset`	Старт после перезагрузки
`Output 1 is changed`	Выход 1 изменил состояние
`Input 1 is changed`	Активен вход 1 (с указанием текущего состояния)
`Tamper is changed`	Сработал датчик вскрытия корпуса (для Teleport-2)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.16 Настройка SMTP

Events → SMTP

Краткий список терминов.

SMTP – (Simple Mail Transfer Protocol) протокол передачи e-mail сообщений по сети. SMTP используется для передачи сообщений на почтовый сервер. Для получения сообщений с почтового сервера клиентские приложения обычно используют протоколы POP либо IMAP.

Параметры настройки:

State — состояние SMTP
Server IP address - IP адрес почтового сервера
Server domain name - доменное имя почтового сервера
Port - номер TCP порта, через который происходит отправка писем (0 - 65534). По умолчанию 25.
Sender e-mail address - почтовый адрес отправителя. В письме отображается в поле **From**
Receiver e-mail address - почтовый адрес получателя. В письме отображается в поле **To.** Для дополнительных возможностей пользователей доступно до 3 получателей.
Subject - тема письма.
Login, Password - логин и пароль, если почтовый сервер требует процедуру аутентификации.

Если эти поля заполнены, автоматически включается механизм аутентификации с сервером. Если поля оставлены пустыми, то действует механизм без аутентификации.
БИ Teleport поддерживает методы аутентификации **AUTH PLAIN** и **AUTH LOGIN**.

По умолчанию, если указан IP адрес сервера, сообщения направляются на этот адрес. Для использования доменного имени, установите **Server IP address** в **0.0.0.0** и укажите доменное имя в поле **Server domain name**.
Примеры настройки SMTP

Существует несколько вариантов организации работы электронной почты:

- В локальной сети находится специально выделенный почтовый сервер.
- Используется внешний почтовый сервер.

У каждого варианта есть свои достоинства и недостатки. Вариант с

SEC.RU | Короткий путь к информации Скачано с sec.ru

выделенным почтовым сервером можно порекомендовать в том случае, если сеть видеонаблюдения физически отделена от сети Интернет и невозможно использовать внешние почтовые сервисы, либо в сети уже существует почтовый сервер и не требуется дополнительных усилий по созданию и поддержанию работы сервера. Использование внешних почтовых сервисов делает настройку проще и быстрее, избавляет от необходимости содержать почтовый сервер, однако в таком случае требуется постоянное подключение к сети Интернет, что не всегда может быть возможным из-за политик безопасности предприятия.

5.3.16.1 Пример настройки с почтовым сервером внутри локальной сети

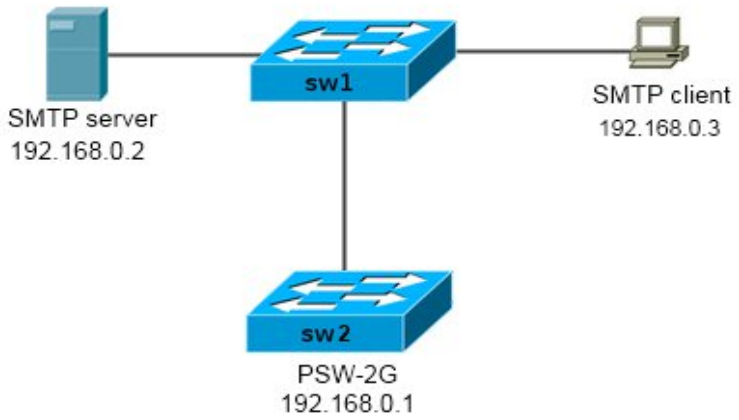


Рис. 5.3.16.1.1 Структура сети

Поставим задачу следующим образом:

Пусть требуется настроить SMTP на коммутаторе SW2 (PSW-2G) с IP 192.168.0.1 для отсылки сообщений об изменении линка на портах коммутатора PSW-2G на компьютер оператора 192.168.0.3.

Поскольку протокол SMTP не предполагает хранение сообщений и выдачу их почтовому клиенту, в сеть необходимо включить почтовый сервер (192.168.0.2).

Выберем для нашей сети доменное имя companyname.com

Для PSW-2g выберем e-mail адрес psw2g@companyname.com,

для SMTP сервера - server@companyname.com,

для клиента - client@companyname.com .

Настройка Teleport`a

Первое — это требуется указать событие, при наступлении которого будет высылаться сообщение. В нашем случае это событие изменения линка.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для этого во вкладке Events → Event List ставим галочку напротив нужного события.

trap:

Port.link	☑	(4) Warning
Port.PoE	☐	(7) Debug
STP	☐	(7) Debug

Рис. 5.3.16.1.2 Выбираем нужное событие

Теперь настроим SMTP

Переходим во вкладку Events → SMTP.

Разрешаем работу SMTP, устанавливаем IP адрес сервера, устанавливаем e-mail адрес отправителя (т.е. PSW) psw@companyname.com, устанавливаем e-mail адрес основного получателя server@companyname.com, также установим запасной адрес server2@companyname.com, куда будут дублироваться сообщения.

Заголовок письма «TFortis Teleport-1».

Поля Login и Password оставляем пустыми: мы не будем использовать аутентификацию.

SMTP server settings

State	Enable
Server IP address	192 168 0 2
Port	25
Sender e-mail address	psw2g@companyname.com
Receiver e-mail address 1	server@companyname.com
Receiver e-mail address 2	server2@companyname.com
Receiver e-mail address 3	
Subject	PSW-2G_log

Login	
Password	

Рис. 5.3.16.1.3 Настройка SMTP в Teleport

Нажимаем «Apply». Настройки применяются.

Теперь переходим к настройке почтового сервера

Существует большое число программ почтовых серверов под различные

SEC.RU | Короткий путь к информации Скачано с sec.ru

ОС и поддерживающие различные протоколы. Для нас важна поддержка SMTP и POP3.

В качестве примера почтового сервера под Windows рассмотрим Office Mail Server (https://www.box.com/oms) Это бесплатная программа с несложной настройкой.

Техническая поддержка и инструкции доступны на сайте: http://oficemailserver.livejournal.com/

Устанавливаем программу, и после запуска будет доступно главное окно:

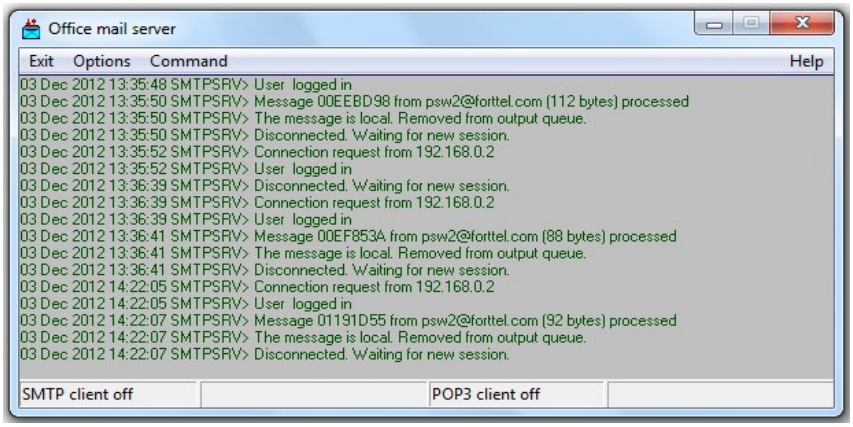


Рис. 5.3.16.1.4 Главное окно программы Office Mail Server

В меню **Options->SMTP/POP3 server options** установите
Local domain name: companyname.com
И в поле Users добавьте пользователя **client.** Затем установите тип пользователя [BOSS].

Office mail Server поддерживает следующие специализированные типы пользователей:

1. Postmaster — пользователь, ответственный за работу и сопровождение Office mail Server. Он получает специальные сообщения, формируемые системой в случае ошибки.
2. Daemon— используется для дистанционного запуска связи с внешним SMTP/POP3 сервером, для отправки и получения сообщений
3. Boss— пользователь которому попадают копии всех сообщений, отправляемых через SMTP сервер.

SEC.RU | Короткий путь к информации Скачано с sec.ru

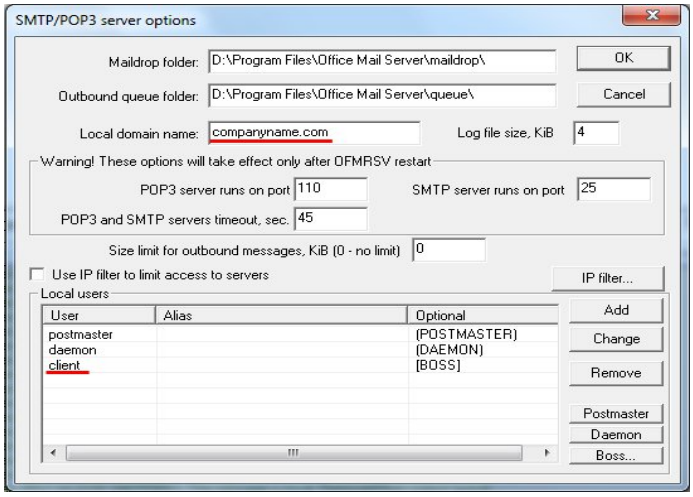
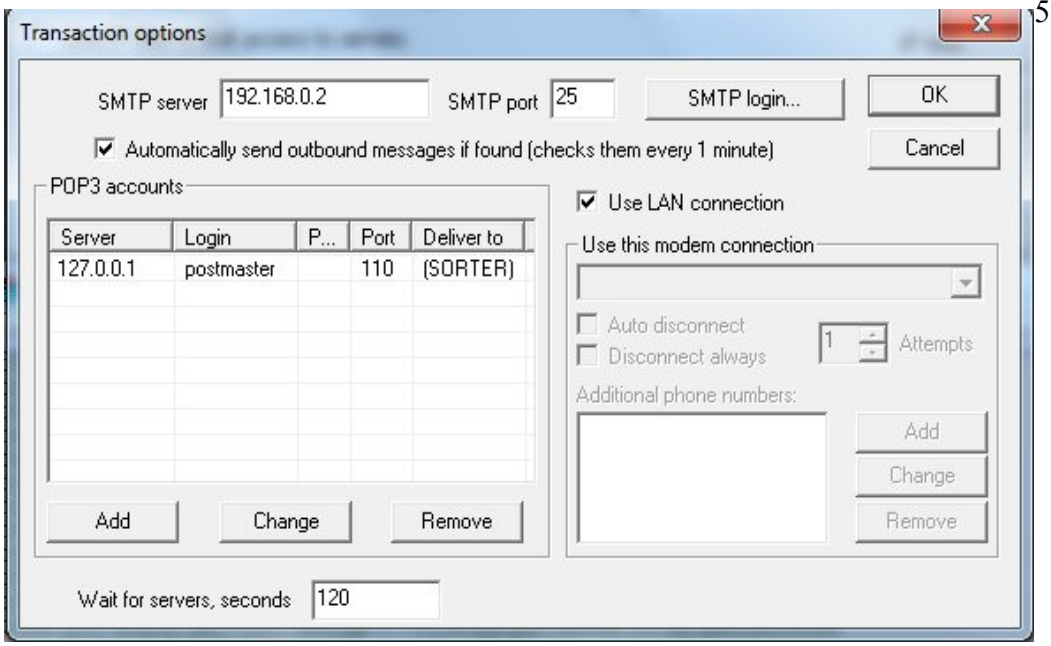


Рис. 5.3.16.1.5 Настройка программы Office Mail Server

Во вкладке **Options->Transaction options**:
Установить IP адрес сервера, установить галку «Automatically send outbound message if found», отключить авторизацию для SMTP (кнопка SMTP login...)

Рис. 5.3.16.1.6



Настройка программы Office Mail Server

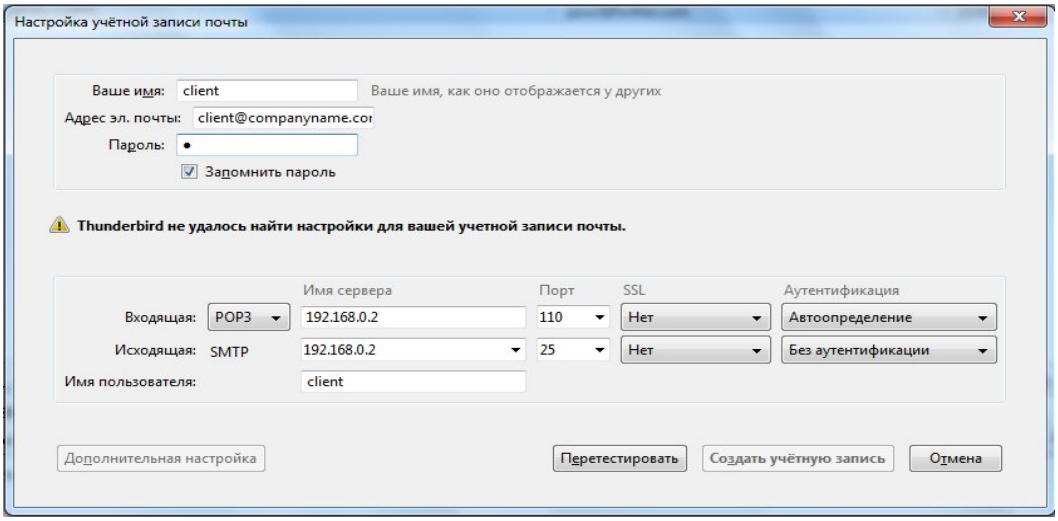
Теперь все сообщения, приходящие на сервер, будут пересылаться клиенту client@companyname.com

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Настройка клиента

Настройка клиента не представляет особых сложностей. Пример настройки на примере Mozilla Thunderbird:

Рис.



5.3.16.1.5 Настройка почтовой программы Mozilla Thunderbird

После окончания всех настроек можно зайти на Web-интерфейс на вкладку SMTP Settings и проконтролировать отправку тестового сообщения. Заполните поля Subject и Message и отправьте письмо. Если все настроено правильно, Mozilla Thunderbird уведомит о новом письме.

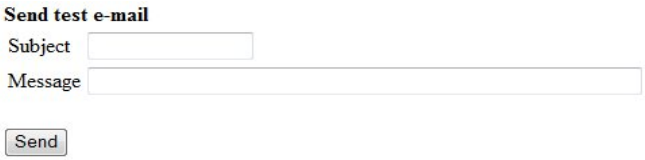


Рис. 5.3.16.1.6 Проверка тестовым сообщением

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.16.2. Пример настройки с внешним почтовым сервером

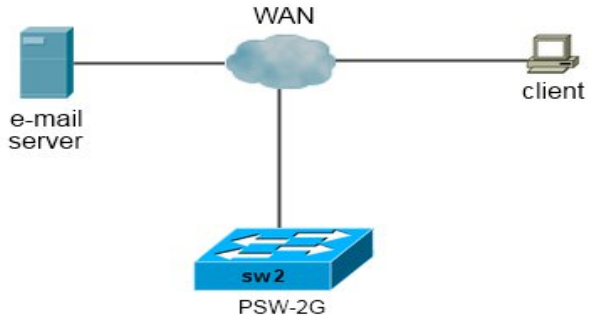


Рис. 5.3.16.2.1 примерная топология сети

В данном примере рассмотрим настройку PSW в том случае, когда используется внешний почтовый сервер.
В примере рассмотрим работу с почтовым сервисом mail.ru. С остальными сервисами работа аналогична, если они поддерживают аутентификацию AUTH PLAIN или AUTH LOGIN.

Также необходимо создать учетную запись почты. И определить настройки SMTP подключения. Для mail.ru адрес SMTP сервера: smtp.mail.ru и порт 25.

Всё, теперь можно приступать непосредственно к настройке.
Заполняем как на рисунке 5.3.12.2.2.
Адрес для отправки сообщений companyname@mail.ru,
адрес получателя пусть будет таким же, т.е. как будто бы мы отправляем письмо сами себе.
Логин: companyname@mail.ru (у mail.ru логином является сам адрес)
Пароль: password

Примечание: в данном примере мы заполнили поле **Server domain name**, а поле **Server IP address** заполнили нулями. В этом случае коммутатор получит IP адрес сервера автоматически через DNS запрос, но для этого должен быть настроен адрес DNS ресолверва. Если у нас DNS не настроен, то в этом случае необходимо было бы непосредственно указать IP адрес SMTP сервера.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

State	Enable
Server IP address	0 0 0 0
Server domain name	smtp.mail.ru
Port	25
Sender e-mail address	companyname@mail.ru
Receiver e-mail address 1	companyname@mail.ru
Receiver e-mail address 2	
Receiver e-mail address 3	
Subject	TFortis PSW-2G4F

Login	companyname@mail.ru
Password	password

Рис. 5.3.16.2.2 Настраиваем SMTP

После окончания всех настроек можно зайти на Web-интерфейс на вкладку SMTP Settings и проконтролировать отправку тестового сообщения. Заполните поля Subject и Message и отправьте письмо.

Send test e-mail

Subject

Message

Send

Рис. 5.3.15.2.3 Отправляем тестовое сообщение

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.17 Настройка SNMP

SNMP → SNMP

SNMP (Simple Network Management Protocol**)** — протокол, который используется для управления и мониторинга за сетевыми устройствами. С помощью протокола SNMP, программное обеспечение может получать доступ к информации, которая хранится на управляемых устройствах (например, на коммутаторе). На управляемых устройствах SNMP хранит информацию об устройстве, на котором он работает, в базе данных, которая называется MIB.

БИ поддерживает SNMP v1 и SNMP v3.

5.3.17.1 Настройка SNMP v1

State	Enable
Traps server IP address	192 168 0 104
Version	SNMP v1
Read Community	public
Write Community	private

Рис. 5.3.17.1 Настройка SNMP v1

- **State** - состояние.
- **Traps Server IP address** - IP адрес сервера, на который отправляются SNMP Traps.
- **Version** - версия протокола SNMP.
- **Read Community** - сообщество только для чтения, строка использующаяся для аутентификации в SNMP v1. Также **Read Community** используется для отправки SNMP Taps.
- **Write Community** - сообщество для записи, строка использующаяся для аутентификации в SNMP v1.

SNMP Traps будут посылаться только при наступлении тех событий, которые указанны во вкладке **Event List**

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.17.2 Настройка SNMP v3

SNMP v3 обеспечивает более высокий уровень безопасности по сравнению с SNMP v1.

State	Enable
Traps server IP address	192 168 0 104
Version	SNMP v3
Security Level	Auth,Priv
Engine ID	80001F888077D5CB779EA0EF4B
User Name	user
Auth Password	••••
Priv Password	••••

Рис. 5.3.17.2 Настройка SNMP v3

Для настройки SNMP v3 установите переключатель Version в положение «SNMP v3».

SNMP v3 позволяет гибко настраивать уровень безопасности.

Выбор уровня осуществляется переключателем «**Security Level**»:

- **NoAuth,NoPriv** - авторизация только по строке User Name и без шифрования. (режим аналогичен SNMP v1)
- **Auth,NoPriv** - работа с использованием авторизации по паролю Auth Password (метод HMAC-MD5-96), но без шифрования.
- **Auth,Priv** - работа с использованием авторизации по паролю Auth Password (метод HMAC-MD5-96), и с шифрованием AES-128 по ключу Priv Password.

Engine ID - идентификатор в SNMP v3. Для каждого устройства **Engine ID** уникален, он генерируется на базе MAC адреса устройства. То есть его не требуется изменять, но при необходимости можно установить собственное значение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.18 Удалённый Ping

Diagnostic Tools → Ping

Рис. 5.3.18.1 Интерфейс удаленного PING

PING — Утилита для проверки соединений в сетях на основе TCP/IP. Данная утилита отправляет 4 пакета по 32 байта на указанный IP адрес и контролирует их возвращение.

При помощи данной утилиты Вы можете «пропинговать» удалённое устройство непосредственно с web-интерфейса. Это может понадобиться для решения возникающих проблем.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.19 Статистика

Teleport предоставляет различную статистическую информацию, она может быть полезна при решении проблем с сетью и ее администрированием.

5.3.19.1 Сводная информация

Statistics → Main Statistics

В данном разделе отображается статистика по состоянию входов и выходов, RS-485 и списка подключенных устройств.

Inputs

Inputs	Current State	Changes count
1	Open	0
2	Open	0
3	Open	0

Outputs

Outputs	Current State	Changes count
1	Open	0
2	Open	0
3	Open	0
4	Open	0
5	Open	0
6	Open	0
7	Open	0
8	Open	0
9	Open	0

RS485

RX cnt	0
TX cnt	0

Remote Devices

	Name	Type	IP Address	RX mngmt frames	TX mngmt frames
1	TLP 2	Teleport-2	192.168.0.1	0	0
2	TLP1-2	Teleport-1	192.168.0.2	0	0
3	PC	Teleport-1	192.168.0.104	0	124

Рис. 5.3.19.1.1 Сводная статистика по всему устройству

Интерпретация данной таблицы позволит проверить правильность работы и настройки устройства.

Inputs – таблица текущих состояний входов, и числа изменений. Если состояние входа изменяется очень часто, а подключенное устройство не предполагает частое изменение состояния (например геркон на вскрытие шкафа), то это можно интерпретировать как неисправность датчика или переменный контакт в линии.

Outputs- таблица состояния выходов

RS-485 – счётчики порта RS-485. Если порт активен и используется, то счётчики приёма и передачи должны инкрементироваться.

Remote Devices – таблица статистики по удалённым устройствам.

Если устройство транслирует состояния своих входов на выходы удалённых устройств, то должен инкрементироваться счётчик TX mngmt frames

Если на выходы устройства транслируется состояния входов удалённых

SEC.RU | Короткий путь к информации Скачано с sec.ru

устройств, то должен инкрементироваться счётчик RX mngmt frames.

Если устройство работает в режиме трансляции RS-485, то должны инкрементироваться оба счётчика.

5.3.19.3 ARP таблица

Statistics → ARP Table

Страница содержит ARP кэш процессора, представленный в виде таблицы. В ARP таблице должны отображаться MAC адреса всех настроенных удалённых устройств, с которыми осуществляется взаимодействие.

№	IP address	MAC address
1	192.168.0.101	84:C9:B2:47:00:28
2	192.168.0.166	D0:27:88:1C:33:B5
3	192.168.0.236	20:1A:06:8A:62:89
4	192.168.0.235	9C:93:4E:18:24:7F
5	192.168.0.128	00:1A:92:67:A8:B5
6	192.168.0.79	CC:5D:4E:4C:11:AC
7	192.168.0.124	22:1B:64:EA:0F:00
8	192.168.0.8	00:1A:92:67:A8:B1
9	192.168.0.24	00:0F:EA:61:93:56
10	192.168.0.10	20:CF:30:C3:4A:C2

Рис. 5.3.18.3.1 ARP таблица

5.3.19.5 DNS таблица

Statistics → DNS Table

Вкладка содержит результат работы протокола DNS: соответствие имени хоста и его IP адреса.

№	IP address	Domain name
1	217.69.139.160	smtp.mail.ru

Рис. 5.3.19.5.1 DNS таблица

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.19.6 Системный журнал (лог)

Statistics → Log
Вкладка содержит лог работы Teleport. На одной странице выводится 10000 записей, для переключения на следующую страницу нажмите **Next**.
Для сохранения лога в txt файл, нажмите **Download log as file.**

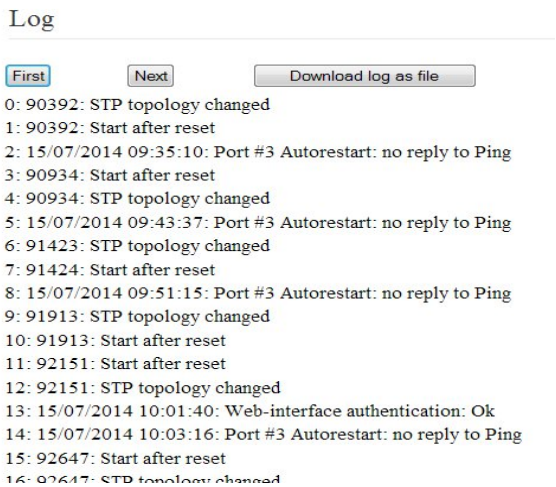


Рис. 5.3.19.6.1 Лог

5.3.20 Обновление ПО

Update/Backup → Update Firmware

Teleport поддерживает обновление ПО. Последняя версия ПО всегда доступна на сайте tforis.ru.

Для обновления ПО скачайте архив с прошивкой. Разархивируйте. Файл с прошивкой имеет расширение *.img

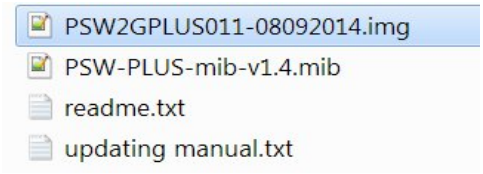
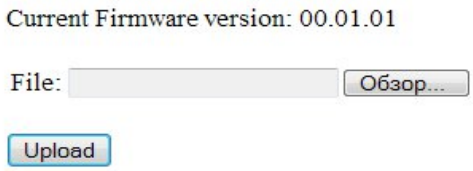


Рис. 5.3.20.1. Файл *.img

В веб-интерфейсе зайдите на вкладку **Update Firmware** и выберите файл прошивки кнопкой **Обзор**.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Рис. 5.3.20.2. Нажимаем Обзор

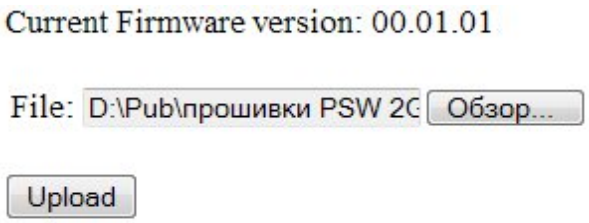


Рис. 5.3.20.3. Выбираем файл *.img

Нажмите кнопку **Upload**, дождитесь пока файл скопируется во внутреннюю память устройства.

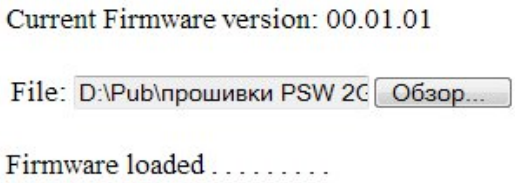


Рис. 5.3.20.4. Дожидаемся загрузки файла

После того, как файл загрузился, нажмите **Update** для обновления или **Cancel** для отмены.

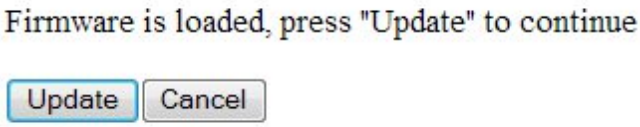


Рис. 5.3.20.5. Нажимаем Update

После нажатия Update начнется процесс обновления. При не перезагружайте Teleport и не отключайте питание.

Updating firmware, please wait

Рис. 5.3.20.6. Ждем окончания процесса прошивки

Примечание: также БИ поддерживает обновление через Telnet с внешнего TFTP сервера. Более подробно см. раздел «Управление через Telnet»

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.21 Сохранение и восстановление настроек

Update/Backup → Backup/Recovery

Трансляторы сухих контактов Teleport поддерживают возможность сохранения текущих настроек в файл конфигурации, его редактирования, а также восстановления настроек из файла.

5.3.21.1 Сохранение настроек в файл

В боковом меню выберите Update/Backup → Backup/Recovery

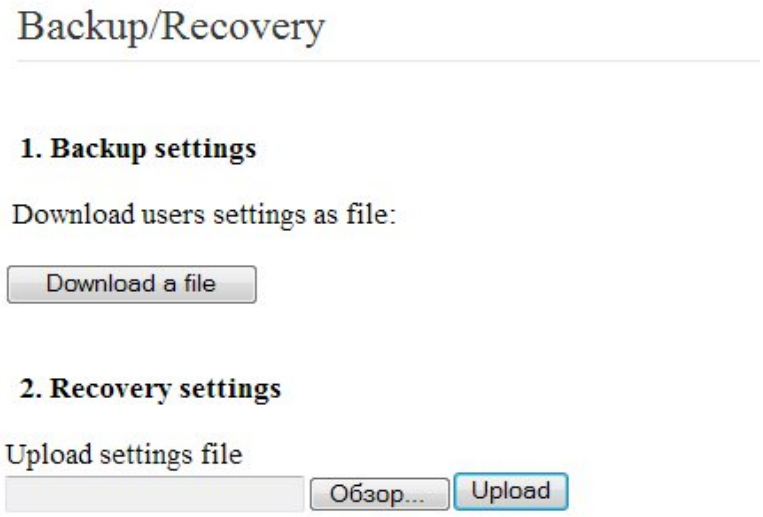


Рис. 5.3.21.1.1 Интерфейс сохранения и восстановления настроек

В пункте 1 нажмите кнопку «Download a file». Будет предложено сохранить или открыть файл, сохраняем.

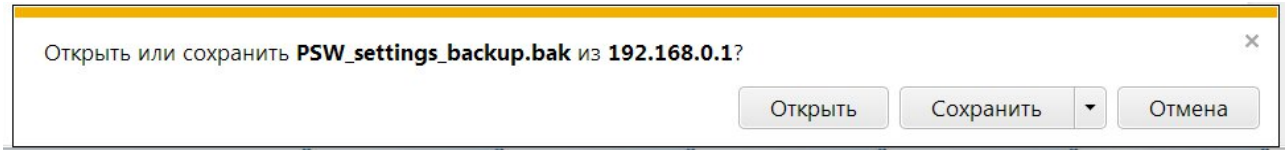


Рис. 5.3.21.1.2 Сохранение файла настроек

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.3.21.2 Восстановление настроек из файла

Если требуется восстановить ранее сохраненные настройки из файла, то во вкладке Update/Backup → Backup/Recovery выбираем в пункте 2 (Recovery settings) файл конфигурации *.bak и нажимаем «**Upload**» для загрузки.

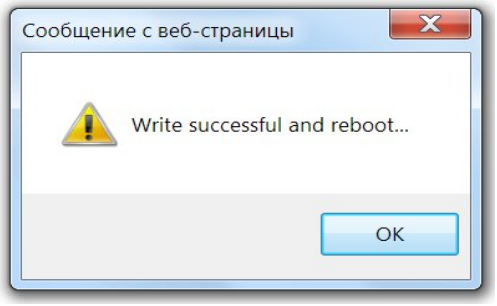


Рис. 5.3.21.2.1 Перезагрузка

После загрузки файла, устройство перезагрузится, и настройки будут применены.

5.3.21.3 Редактирование файла конфигурации

Изменение файла конфигурации может быть полезным, когда у группы устройств схожие настройки, в этом случае можно создать для этих устройств универсальный файл конфигурации и у каждого устройства менять только небольшой набор параметров, например IP адрес, а другие параметры уже будут записаны из файла конфигурации.

Файл конфигурации, генерируемый Teleport при сохранении настроек в файл, представляет собой файл с расширением *.bak с настройками в текстовом виде.

Данный файл можно открыть любым текстовым редактором. Структура записей имеет строго определенную форму записи. В общем виде она выглядит так:

#<*имя переменной*>**=[**<*значение переменной*>**]**
Например: #IPADDRESS=[192.168.0.1], где переменной IPADDRESS соответствует значение 192.168.0.1

Описание настроек с параметрами по умолчанию представлено в Таблице 5.3.2.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Таблица 5.3.2. Переменные файла конфигурации

Синтаксис команды	Описание
#IPADDRESS=[192.168.0.1]	IP адрес
#NETMASK=[255.255.255.0]	Маска подсети
#GATEWAY=[255.255.255.255]	шлюз по умолчанию
#USER_MAC=[c0:11:a6:0:0:0]	пользовательский MAC адрес
#DNS=[255.255.255.255]	IP адрес DNS сервера
#DHCPMODE=[0]	режим работы DHCP (0 — выключен, 1 — DHCP клиент)
#LANG=[0]	язык интерфейса (0-английский, 1 — русский)
#HTTP_USERNAME=[] #HTTP_PASSWD=[]	логин и пароль для учетной записи по умолчанию (права доступа **Admin**)
#USER1_USERNAME=[]	Имя пользователя
#USER1_PASSWD=[]	Пароль для учетной записи
#USER1_RULE=[0]	Права дотупа (0-учетная запись отключена, 1 — Admin, 2 – User)
#SYSTEM_NAME=[]	описание устройства
#SYSTEM_LOCATION=[]	месторасположение устройства
#SYSTEM_CONTACT=[]	контактные данные
#SMTP_STATE=[0]	включение протокола SMTP (0 – выключено, 1 — включено)
#SMTP_SERV_IP=[0.0.0.0]	IP адрес SMTP сервера
#SMTP_TO1=[]	почтовый адрес получателя 1
#SMTP_TO2=[]	почтовый адрес получателя 2
#SMTP_TO3=[]	почтовый адрес получателя 3
#SMTP_FROM=[]	почтовый адрес отправителя
#SMTP_SUBJ=[TFortis Teleport-1]	заголовок письма
#SMTP_LOGIN=[]	логин для доступа к почтовому ящику
#SMTP_PASS=[]	пароль для доступа к почтовому ящику
#SMTP_PORT=[25]	порт SMTP
#SMTP_DOMAIN_NAME=[]	доменное имя почтового сервера

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#SNTP_STATE=[0]	состояние протокола SNTP
#SNTP_SETT_SERV=[0.0.0.0]	IP адрес SNTP сервера
#SNTP_SERV_NAME=[]	Доменное имя SNTP сервера
#SNTP_TIMEZONE=[0]	часовой пояс, относительно UTC (от -12 до +13)
#SNTP_PERIOD=[10]	период синхронизации с сервером (1, 10 или 60 минут)
#SYSLOG_STATE=[0]	состояние протокола Syslog
#SYSLOG_SERV_IP=[0.0.0.0]	IP адрес Syslog сервера
#EVENT_LIST_SYSTEM_T=[7]	событие в списке EventList (7 – выключено)
#EVENT_LIST_INPUTS_T=[12]	событие в списке EventList (7 – выключено)
#EVENT_LIST_OUTPUTS_T=[12]	событие в списке EventList (7 – выключено)
#SNMP_STATE=[0]	включение SNMP (0 -выключено, 1 — включено)
#SNMP_SERVER=[0.0.0.0]	IP адрес SNMP Traps сервера
#SNMP_VERS=[0]	версия протокола SNMP (0 – SNMP v1, 3– SNMP v3)
#SNMP_COMMUNITY1=[public]	сообщество чтения
#SNMP_COMMUNITY2=[private]	сообщество записи
#SNMPV3_USER1_LEVEL=[0]	Уровень безопасности (0 — NoAuth,NoPriv, 1 – Auth,NoPriv, 2 – Auth,Priv)
#SNMPV3_USER1_USER_NAME=[]	Имя пользователя для SNMP v3
#SNMPV3_USER1_AUTH_PASS=[]	Auth Password для SNMP v3
#SNMPV3_USER1_PRIV_PASS=[]	Priv Password для SNMP v3
#SNMP3_ENGINE_ID=[]	Engine ID для SNMP v3
#TELNET_STATE=[1]	включение Telnet (0 – выключено, 1 — включено)
#TFTP_MODE=[0]	включение TFTP (0 – выключено, 1 — включено)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#TFTP_PORT=[69]	UDP порт TFTP
#SERIAL_STATE=[1]	Включение порта RS-485
#SERIAL_BAUDRATE=[9600]	Скорость порта RS-485
#SERIAL_PARITY=[0]	Чётность RS-485 (0-Disable, 1-Even, 2-Odd)
#SERIAL_DATABITS=[8]	Число бит данных
#SERIAL_STOPBITS=[1]	Число стоповых бит
#SERIAL_MODE=[0]	Режим работы порта: 0-Disable, 1 – Pair Connection
#SERIAL_REMDEV=[[1][0][0][0][0][0][0][0]]	Список удалённых устройств, для порта, работающего в режиме Pair Connection
#OUTPUT1_STATE=[0]	Состояние выхода 1 (0-short, 1-open)
#OUTPUT1_ACTION=[0]	Не используется
#OUTPUT1_MODE=[0]	Режим управления выхода: 0-Pair Connection, 1-Manual, 2-SNMP, 3-Modbus
#OUTPUT1_DESCR=[]	Описание выхода 1
#OUTPUT1_REMDEV=[0]	Удалённое устройство для выхода 1, если он работает в режиме Pair Connection
#INPUT1_STATE=[0]	Разрешение работы входа 1. 0 — вход неактивен, 1 - активен
#INPUT1_ALARM=[1]	Не используется
#INPUT1_DESCR=[]	Описание входа 1
#INPUT1_MODE=[1]	Режим работы входа 1. 1-Pair Connection
#INPUT1_REMDEV=[0]	Удалённое устройство для входа 1
#TLP1_VALID=[1]	Запись 1 в списке удалённых устройств активна
#TLP1_MODE=[0]	Не используется
#TLP1_TYPE=[0]	Тип устройства 1 в списке удалённых устройств

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#TLP1_DESCR=[]	Описание устройства 1
#TLP1_IP=[0.0.0.0]	IP адрес устройства 1
#TLP1_GATE=[0.0.0.0]	Не используется
#TLP1_MASK=[0.0.0.0]	Не используется
#TLP_NET_MODE=[0]	Не используется
#MODBUS_STATE=[1]	Состояние протокола Modbus
#MODBUS_ID=[0]	Не используется
#MODBUS_MODE=[2]	Режим работы: только 2-Modbus TCP

5.3.22 Сброс настроек на заводские установки

Reboot/Default → Factory Default

Рис. 5.3.22.1 Сброс настроек

При необходимости возможно осуществить сброс настроек на заводские установки. При этом сброс можно осуществлять выборочно:

Keep current Network settings — Сброс с сохраненим сетевых настроек: IP, MAC, Gateway,Mask

Keep current username & password — Сброс с сохранением настроек доступа: Username, Password

5.3.23 Перезагрузка

Reboot/Default → Reboot

При необходимости Teleport можно дистанционно перезагрузить.

- **Reboot CPU** - Перезагрузка только процессора.

Рис. 5.3.23.1 Перезагрузка

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4 Управление через Telnet

Telnet используется для удаленного управления оборудованием посредством командной строки. Telnet использует протокол TCP и порт 23. В TFortis Teleport по умолчанию Telnet включен. По желанию его можно выключить: в меню выбрать *Basic Settings → Telnet*

Telnet Settings

State	Enable
Option Echo	Enable

Рис. 5.4.1 Настройка Telnet

Telnet поддерживает следующие **дополнительные режимы**:

1. Сокращенные команды. Доступна возможность работы с короткими командами (не требуется вводить команду до конца).

Пример: если требуется ввести команду ***config ports 1-2 state enable***, то ее можно сократить до минимальных: ***co po 1-2 st en***

2.**Автодополнение команд.** Возможность по нажатию клавиши **TAB** дополнять введённую команду.

Пример: Если ввести **con**, нажать TAB, то команда дополнится до **config**

3. **История команд.** Доступна история введённых команд. Переключение осуществляется клавишами ВВЕРХ, ВНИЗ

Подключаться к устройству можно при помощи любой терминальной программы, в данном документе настройка будет рассмотрена на примере Microsoft Telnet. Подключаемся используя команду "*open <IP адрес>*"

```
Microsoft Telnet> open 192.168.0.1
```

После подключения потребуется ввести логин и пароль. (Логин и пароль для Telnet`а такие же, как и для доступа к WEB интерфейсу) Если логин и пароль не были заданы, то два раза подряд нажмите Enter.

```
                    TFortis Teleport
     Copyright(C) 2016 "Fort-Telecom" Ltd. All rights reserved.
User Name>
```

Примечание: если 30 раз подряд логин/пароль были введены неверно, то доступ к Telnet`у блокируется на 1 час.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Символ **#** и имя устройства означают, что аутентификация прошла успешно и Teleport перешел в режим конфигурирования. (Права доступа - **Admin**)

```
Teleport-1#
```

Если были введены логин/пароль учетной записи с ограниченными правами, то мы перейдем в режим просмотра. (Права доступа - **User**)

```
Teleport-1>
```

Список команд можно получить используя команду «?» или «help»

В качестве аргументов команд используется ряд условных обозначений:

- <IP> - IP адрес в формате **XX.XX.XX.XX**
- <STATE> - состояние, может принимать значения **enable** или **disable**
- <VALUE> - любое целое знаковое или беззнаковое число
- <STRING> - текстовая строка
- <LIST> - список в виде: **начальный элемент-конечный элемент**

  Пример: Для выходов 1,2,3 : «**1-3**» ; только для одного выхода 2 : «**2**»

Процесс настройки посредством Telnet`а происходит в несколько шагов:

1. При помощи подмножества команд из группы **config** устанавливается требуемая конфигурация
2. Эта конфигурация сохраняется в память командой **save, только после этого настройки применяются**

Обратите внимание:

Если после установки параметров устройство будет перезагружено без применения команды **save**, то настройки не сохранятся.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4.1 Пример настройки

Для примера рассмотрим процесс настройки Teleport-1.
Пусть нам требуется установить следующие настройки:

- IP адрес 192.168.0.100
- Шлюз 192.168.0.1

Итак, подключаемся к устройству, если устройство еще не было сконфигурировано, то его IP адрес 192.168.0.1 и логин и пароль для доступа не заданы.

```
Microsoft Telnet> open 192.168.0.1
```

Переходим к режиму управления

```
Teleport-1#
```

```
Teleport-1#config ipif System ipaddress 192.168.0.100
Command: config ipif System ipaddress 192.168.0.100
Success.
```

Меняем IP адрес командой **config ipif System ipaddress 192.168.0.100**

Добавляем шлюз по умолчанию: **config ipif System gateway 192.168.0.100**

Добавление нового удалённого устройства: **config teleport add 192.168.0.1**

Проверяем, что устройство добавлено: **show teleport**

```
Command: show teleport
        IP address      Type            Description
-------------------------------------------
1       192.168.0.1     Teleport-1
```

Настраиваем вход 1 для дальнейшего транслирования на выход 1 устройства Teleport-1 с IP 192.168.0.1

config inputs 1 state enable
config inputs 1 remdev 192.168.0.1
config inputs 1 remport 1

```
Teleport-1#config inputs 1 state enable
Command: config inputs 1 state enable
Success.
Teleport-1#
Teleport-1#config inputs 1 remdev 192.168.0.1
Command: config input 1 remdev 192.168.0.1
Success.
Teleport-1#
Teleport-1#config inputs 1 remport 1
Command: config input 1 remport 1
Success.
```

Всё, настройка завершена, теперь сохраняем настройки: **save**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.2 Описание команд Telnet

Трансляторы сухих контактов Teleport поддерживают следующий набор команд для Telnet:

1. Группа команд **config:**

- ipif – сетевые настройки (IP адрес, маска подсети, шлюз)
- snmp – настройка SNMP
- syslog – настройка Syslog
- sntp – настройка SNTP
- smtp – настройка SMTP
- user_account — настройка имени пользователя/пароля
- tftp — настройка TFTP
- events – настройка событий
- description – задание описания устройства.
- inputs – настройка входов платы расширения
- outputs – настройка выходов платы расширения
- rs485 – настройка RS485
- modbus – настройка Modbus
- teleport - настройка удалённых устройств

2. Группа команд **show**

- system — сводная информация об устройстве
- snmp— информация о протоколе SNMP
- syslog - информация о протоколе SYSLOG
- sntp — информация о протоколе SNTP
- smtp— информация о протоколе SMTP
- firmware— информация о текущей версии прошивки
- arpentry — ARP таблица
- tftp — информация о протоколе TFTP
- events – информация о настроенных событиях
- config – отображение всей конфигурации
- inputs – информация о входах платы расширения
- outputs – информация о выходах платы расширения
- rs485 – информация о настройке RS485
- modbus – информация о настройке Modbus
- teleport – информация о удалённых устройствах

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Обновление прошивки и загрузка конфигурации с TFTP сервера
download

4. Сохранение настроек и системного лога на TFTP сервер
upload

5. Утилита Ping
ping

6. Сохранение и применение настроек
save
7. Перезагрузка
reboot

8. Вывод справки по командам
help или **?**

9. выход из режима управления Telnet
exit

5.4.3 Группа config

5.4.3.1 Сетевые настройки (config ipif)

1. IP адрес.
   config ipif System ipaddress <IP>
   Пример: *config ipif System ipaddress 192.168.0.100*

2. Маска подсети .
   config ipif System netmask <IP>
   Пример: *config ipif System netmask 255.255.255.0*

3. Адрес шлюза
   config ipif System gateway <IP>
   Пример: *config ipif System gateway 192.168.0.1*

4. Адрес DNS сервера
   config ipif System dns <IP>
   Пример: *config ipif System dns 192.168.0.1*

5. Режим работы DHCP клиента
   config ipif System dhcp <STATE>
   Пример: *config ipif System dhcp enable – включен режим DHCP*

SEC.RU | Короткий путь к информации Скачано с sec.ru

клиента

5.4.3.2 Настройка SNMP

1. Включение SNMP
config snmp state <STATE>
Пример: *config snmp state enable*

2. IP адрес сервера (для SNMP Traps)
config snmp host <IP>
Пример: *config snmp host 192.168.0.1*

3. Строка сообщества чтения (Read Community)
config snmp read_community <STRING>
Пример: *config snmp read_community public*

4. Строка сообщества записи (Write Community)
config snmp write_community <STRING>
Пример: *config snmp write_community private*

5. Версия протокола (Поддерживается SNMPv1 и SNMPv3)
config snmp version <VALUE>
где <VALUE>: 1, 3
Пример: *config snmp version 1*

6. Уровень безопасности (Security Level) для SNMP v3
config snmp level <VALUE>
где <VALUE>:
0 - NoAuth, NoPriv
1 – Auth, NoPriv
2 – Auth, Priv
Пример: *config snmp level 2*

7. Имя пользователя для SNMP v3
config snmp user_name <STRING>
Пример: *config snmp user_name administrator*

8. Auth Password для SNMP v3 (необходим если выбран уровень безопасности Auth,NoPriv или Auth,Priv)
config snmp auth_pass <STRING>
Пример: *config snmp auth_pass test*

9. Priv Password для SNMP v3 (необходим если выбран уровень

SEC.RU | Короткий путь к информации Скачано с sec.ru

безопасности Auth,Priv)
config snmp priv_pass <STRING>
Пример: *config snmp priv_pass test*

9. Engine ID для SNMP v3, уникальный идентификатор
config snmp engine_id <STRING>
Пример: *config snmp engine_id 8000A42303C011A6050001*

5.4.3.3 Настройка Syslog

1. Включение Syslog
config syslog state <STATE>
Пример: *config syslog state enable*

2. IP адрес сервера
config syslog host <IP>
Пример: *config syslog host 192.168.0.1*

5.4.3.4 Настройка SNTP

1. Включение SNTP
config sntp state <STATE>
Пример: *config sntp state enable*

2. IP адрес SNTP сервера
config sntp primary <IP>
Пример: *config sntp primary 192.168.0.1*

3. Часовой пояс (относительно UTC)
config sntp timezone <VALUE>
Пример: *config sntp timezone +6*

5.4.3.5 Настройка TFTP

1. Включение *TFTP*

config tftp state <STATE>
Пример: *config tftp state enable*

2. настройка UDP порта (По умолчанию порт - 69)
config tftp port <NUM>
Пример: *config config tftp port 69*

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4.3.6 Настройка событий

Настраиваются те события, которые необходимо отправлять на сервер мониторинга. При использовании протокола Syslog дополнительно указывается уровень важности события.

переменная <STATE> принимает значение enable/disable

переменная <NUM> указывает уровень важности 0..7

1. события системы

config events system state <STATE> level <NUM>

Пример: *config events system state enable level 4*

2. изменения в состоянии входов
config events inputs state <STATE> level <NUM>

Пример: *config events inputs state enable level 4*

3. изменения в состоянии выходов
config events outputs state <STATE> level <NUM>

Пример: *config events outputs state enable level 4*

5.4.3.7 Настройка учетных записей пользователей

1. Создание нового пользователя
config user_account add <USERNAME> <PASSWORD> <MODE>
где **<USERNAME>** - имя пользователя (макс. 20 символов),
<PASSWORD> - пароль (макс. 20 символов),
<MODE> - уровень прав:

- **admin_rule**
- **user_rule**

Пример: *config user_account add username password admin_rule*
Создаем учетную запись администратора с именем «username» и паролем «password»

2. Редактирование данных пользователя
config user_account add <USERNAME> <PASSWORD> <MODE>
где **<USERNAME>** - имя пользователя (макс. 20 символов),
<PASSWORD> - пароль (макс. 20 символов),
<MODE> - уровень прав:

- **admin_rule**
- **user_rule**

SEC.RU | Короткий путь к информации Скачано с sec.ru

Пример: *config user_account add username password user_rule*
У созданной учетной записи «username» изменили права доступа (на User)

3. Удаление пользователя
config user_account delete <USERNAME>
где **<USERNAME>** - имя пользователя (макс. 20 символов)
Пример: *config user_account delete username*
Удалили учетную запись «username».

5.4.3.8 Настройка описания устройства

1. настройка названия устройства

config description name <STRING>

Пример: *config description name psw-2g4f*

2. настройка месторасположения устройства

config description location <STRING>

Пример: *config description location servernaya*

3. настройка контактов обслуживающей организации

config description location <STRING>

Пример: *config description company superpuper-telecom*

5.4.3.9 Настройка входов

1. разрешение работы входа
config inputs <INPUT> state <STATE>
где **<INPUT>** - номер входа,
<STATE> - состояние входа:
- enable – вход активен
- disable — вход неактивен

Пример: *config inputs 1 state enable*

2. Задание описания для входа
config inputs <INPUT> description <STRING>
где **<INPUT>** - номер входа,
<STRING> - строка, описание входа

Пример: *config inputs 1 description some_name*

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Задание удалённого устройства для входа
config inputs <INPUT> remdev <IP>
где **<INPUT>** - номер входа,
<IP> - IP адрес удалённого устройства.
Примечание: удалённое устройство необходимо изначально добавить в список (***config teleport add ..***). При добавлении устройства с неизвестным IP адресом возникнет ошибка.
Пример: *config inputs 1 remdev 192.168.0.2*

4. Задание выходного порта удалённого устройства
config inputs <INPUT> remport <NUM>
где **<INPUT>** - номер входа,
<NUM> *- номер выхода удалённого устройства, на который будет транслироваться состояние входа*
Пример: *config inputs 1 remport 5*

5. Инверсия состояния входа
config inputs <INPUT> inverse <STATE>
где **<INPUT>** - номер входа,
<STATE> *- состояние инверсии входа*

- enable – вход инвертирован
- *disable* — вход неинвертирован, нормальный режим

Пример: *config inputs 1 inverse enable*

5.4.3.10 Настройка выходов

1. Установка начального состояния выхода в режиме ручного управления
config outputs <OUTPUT> state <STATE>
где **<OUTPUT>** - номер выхода,
<STATE> - состояние выхода:

- short – замкнутое
- open — разомкнутое

Пример: *config outputs 1 state short*

2. Настройка режима управления выходом
config outputs <OUTPUT> mode <STATE>
где **<OUTPUT>** - номер выхода,
<STATE> - режим работы:

- pair – режим «Pair Connection»/«Парное соединение», на выход может транслироваться состояние входа с удалённого Teleport`a
- manual —режим ручного управления выходом.
- snmp – управления выходом возможно только через протокол

SEC.RU | Короткий путь к информации Скачано с sec.ru

SNMP
- modbus – управления выходом возможно только через протокол Modbus TCP

Пример: *config outputs 1 mode pair*

3. Установка описания для выхода
config outputs <OUTPUT> description <STRING>
где **<OUTPUT>** - номер выхода,
<STRING> - строка, описание входа
Пример: *config outputs 1 description some_name*

4. Задание удалённого устройства для выхода (если выход работает в режиме «парного соединения»)
config outputs <INPUT> remdev <IP>
где **<INPUT>** - номер выхода,
<IP> - IP адрес удалённого устройства.
Примечание: удалённое устройство необходимо изначально добавить в список (***config teleport add ..***). При добавлении устройства с неизвестным IP адресом возникнет ошибка.
Пример: *config outputs 1 remdev 192.168.0.2*

5.4.3.11 Настройка RS485

1. Скорость порта
**config rs485 baudrate
**
где **
** - скорость, выбирается из 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200
Пример: *config rs485 baudrate 9600*

2. Проверка на чётность
config rs485 parity <PARITY>
где **<PARITY>** - проверка на чётность
- disable – проверка отключена
- even — чет
- odd — нечет

Пример: *config rs485 parity even*

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Число бит данных
config rs485 databits <DATABITS>
где **<DATABITS>** - число бит данных
Пример: *config rs485 databits 7*

4. Число стоповых бит
config rs485 stopbits <STOPBITS>
где **<STOPBITS>** - число стоповых бит
Пример: *config rs485 databits 1*

5. Режим работы порта
config rs485 mode <STATE>
где ***<STATE>*** - режим работы
- disable – порт выключен
- translate – порт работает в режиме трансляции

Пример: config rs485 mode translate

6. Добавление удалённых устройств
config rs485 remdevs add <IP>
*где <**IP**> - IP адрес удалённого устройства.*
Пример: config rs485 remdevs add 192.168.0.1

7. Удаление удалённого устройства
config rs485 remdevs del <IP>
*где <**IP**> - IP адрес удалённого устройства.*
Пример: config rs485 remdevs del 192.168.0.1

5.4.3.12 Настройка Modbus

1.Состояние протокола
config modbus state <STATE>
где ***<STATE>*** - режим работы
- disable – протокол выключен
- enable – протокол включен

Пример: config modbus state enable

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4.3.13 Настройка списка удалённых устройств

1 Добавление удалённых устройств
config teleport add <IP>
*где <**IP**> - IP адрес нового удалённого устройства.*
Пример: config teleport add 192.168.0.1

2. Удаление удалённого устройства
config teleport del <IP>
*где <**IP**> - IP адрес удалённого устройства.*
Пример: config teleport del 192.168.0.1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.4 Группа show

Возможные команды:

- system — сводная информация об устройстве
- snmp— информация о протоколе SNMP
- syslog - информация о протоколе SYSLOG
- sntp — информация о протоколе SNTP
- smtp— информация о протоколе SMTP
- firmware— информация о текущей версии прошивки
- arpentry — ARP таблица
- tftp — информация о протоколе TFTP
- events – информация о настроенных событиях
- config – отображение всей конфигурации
- inputs – информация о входах платы расширения
- outputs – информация о выходах платы расширения
- rs485 – информация о настройке RS485
- modbus – информация о настройке Modbus
- teleport – информация о удалённых устройствах

Все команды в этой группе можно разделить на несколько подгрупп:

- Просмотр сводной информации
- Просмотр настроек

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.4.1 Просмотр сводной информации

1. Вывод сводной информации о устройстве и его конфигурации
show system

```
Command: show system
Device type:              TFortis Teleport-1
MAC Address:              C0:11:A6:00:00:02
IP Address:               192.168.0.2
Subnet Mask:              255.255.255.0
Default Gateway:          255.255.255.255
Firmware Version:         0B.0B.0B
Bootloader Version:       01.02
Serial Number:            2
Device Description:
Device Location:
Device Contact:
System Uptime:            0d. 8h. 26m. 51s
Syslog:                   enable
SMTP:                     disable
```

2. Вывод информации о встроенном программном обеспечении
show firmware

```
Firmware Version:         00.01.01
Bootloader Version:       01.00
```

3. Вывод ARP-таблицы
show arpentry

```
Teleport-1#show arpentry
Command: show arpentry
ARP Aging Time: 120

Interface        IP Address              MAC Address
-----------------------------------------------------
System           192.168.0.115           24:A4:3C:D4:EA:B4
System           192.168.0.16            D0:27:88:1C:2E:FC
System           192.168.0.164           24:A4:3C:D4:EA:B4
System           192.168.0.24            24:A4:3C:D4:EA:B4
System           192.168.0.15            4C:CC:6A:0D:00:B9
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.4.2 Просмотр настроек

1. Вывод информации по протоколу SNMP
show snmp

Для SNMP v1:

```
TFortis PSW-2G6F+#show snmp
Command: show snmp
SNMP State:                 enable
SNMP version:               1
SNMP Server IP:             0.0.0.0
SNMP Read community:        public
SNMP Write community:       private
```

Для SNMP v3:

```
TFortis PSW-2G6F+#show snmp
Command: show snmp
SNMP State:                 enable
SNMP version:               3
SNMP Server IP:             0.0.0.0
SNMP Engine ID:             8000A42303C011A6050001
Security Level:             Auth,Priv
User Name:                  test
Auth Password:              test
Priv Password:              test
```

2. Вывод информации по протоколу Syslog
show syslog

```
TFortis PSW-1G4F#show syslog
Syslog State:               disable
Syslog Server:              0.0.0.0
```

3. Вывод информации о настройке SNTP
show sntp

```
TFortis PSW-1G4F#show sntp
SNTP State:                 disable
SNTP Server:                0.0.0.0
Current Time:               00:00:00
Current Date:               00/00/2000
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. Вывод информации о настройке SMTP

show smtp

```
TFortis PSW-1G4F#show smtp
SMTP State:                disable
SMTP Server IP:            0.0.0.0
SMTP Server Name:
SMTP Server Port:          25
Mail Sender:
Mail Receiver 1:
Mail Receiver 2:
Mail Receiver 3:
SMTP Login:
SMTP Password:
```

5. Вывод информации о настройке TFTP

show tftp

```
TFortis PSW-1G4F#show tftp
TFTP State: Enable
TFTP Port: 69
```

6. Вывод информации о настройке списка событий

show events

```
Teleport-1#show events
Command: show events
Event List:
-----------
System                    State Enable,Level 7
Inputs                    State Enable,Level 4
Outputs                   State Enable,Level 4
```

7. Вывод полной конфигурации . (Вывод осуществляется в том же виде, что и при сохранении файла конфигурации)

show config

```
#EVENT_LIST_ACCESS_T=[12]
------Dry contact settings
#DRY_CONT0_STATE=[1]
#DRY_CONT1_STATE=[1]
#DRY_CONT1_LEVEL=[1]
#DRY_CONT2_STATE=[1]
#DRY_CONT2_LEVEL=[1]
------QoS settings
#PORT1_RATE_LIMIT_RX=[0]
#PORT2_RATE_LIMIT_RX=[0]
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

8. Информация о состоянии входов
show inputs

```
Command: show inputs
Input|State     |Active |Description|Mode|Remote Device, Port|Inverse
-----------------------------------------------------------------
1       Open    Enable  123           pair    192.168.0.1 - 9 Disable
2       Open    Disable 123           pair    192.168.0.1 - 9 Disable
3       Open    Enable                pair    192.168.0.1 - 9 Disable
```

9. Информация о состоянии выходов

```
Command: show outputs
Out|Current State|State|Description|Mode|Remote Device
-----------------------------------------------------
1       Open    Open            manual  ---
2       Open    Open            snmp    ---
3       Open    Open            pair    192.168.0.1
4       Open    Open            pair    192.168.0.1
5       Open    Open            pair    192.168.0.1
6       Open    Open            pair    192.168.0.1
7       Open    Open            pair    192.168.0.1
8       Open    Open            pair    192.168.0.1
9       Open    Open            pair    192.168.0.1
```

show outputs

10. Информация о настройке RS485
show rs485

```
Command: show rs485
Baudrate:       9600
Parity:         Even
Databits:       8
Stopbits:       1
Mode:           Translate

Remote devices:
192.168.0.1
```

11. Информация о настройке протокола Modbus
show modbus

```
Command: show modbus
Modbus TCP State: Enable
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

12. Информация о удалённых устройствах

```
Command: show teleport
        IP address      Type            Description
-----------------------------------------------
1       192.168.0.1     Teleport-1
```

show teleport

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.5 Обновление ПО через TFTP

Трансляторы сухих контактов TFortis Teleport поддерживают обновление прошивки через Telnet, использую внешний TFTP сервер.

Команда на обновление ПО:

download firmware_fromTFTP <IP> <PATH>

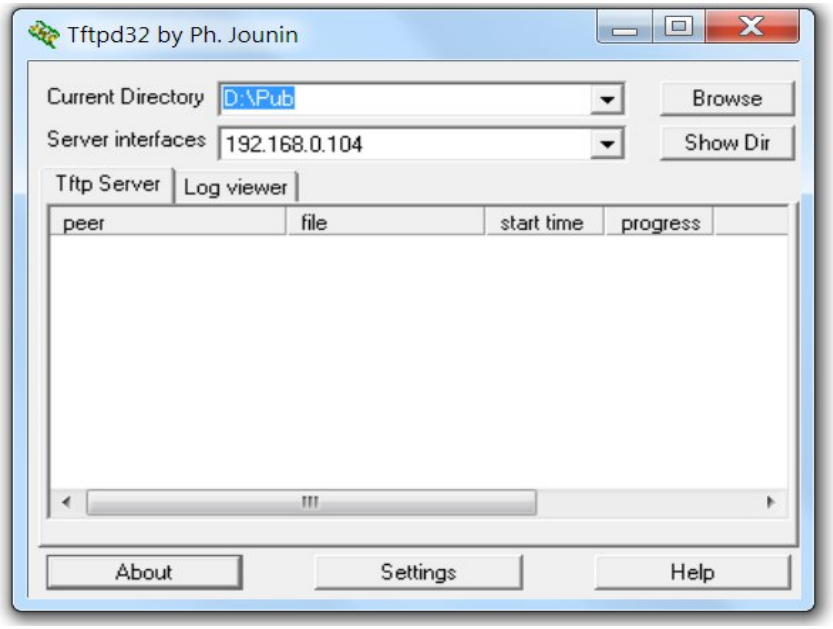
где **<IP>** - IP адрес TFTP сервера

<PATH> - путь до файла прошивки

Рассмотрим процесс обновления более подробно.

1. Во-первых необходимо убедиться, что TFTP сервер запущен, и запустить его, если не запущен. Под ОС Windows достаточно распространённым приложением является программа Tftpd32. И на примере Tftpd32 и будем рассматривать процесс обновления.
Дистрибутив доступен на сайте:
http://tftpd32.jounin.net/tftpd32.html

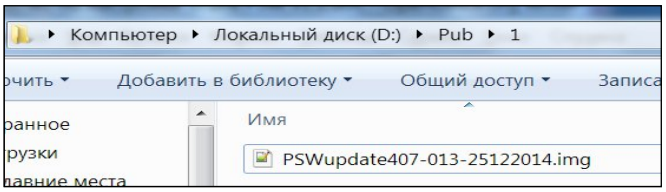
Запускаем в режиме TFTP-сервера



Как видим TFTP-сервер будет доступен по адресу 192.168.0.104, а корневая директория сервера D:\Pub

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. Помещаем файл прошивки в корневую директорию сервера



3. На стороне сервера у нас всё готово, переходим к настройкам Teleport
По умолчанию протокол TFTP отключен,
включаем его командой:
config tftp state enable

```
TFortis PSW-1G4F#config tftp state enable
TFTP config: state Enable
```

Поддержка протокола включится. Для того, чтобы сохранить в энергонезависимой памяти эту настройку выполняем команду **save**, иначе после перезагрузки эта настройка не сохранится.

```
TFortis PSW-1G4F#save
Settings saved successfully
```

Проверяем, что Teleport «видит» TFTP сервер. Для этого можно пропинговать
ping 192.168.0.104

4.

```
TFortis PSW-1G4F#ping 192.168.0.104
Ping 192.168.0.104 with 32 bytes of data
TFortis PSW-1G4F#
Reply from 192.168.0.104 bytes=32 seq=1
Reply from 192.168.0.104 bytes=32 seq=2
Reply from 192.168.0.104 bytes=32 seq=3
Reply from 192.168.0.104 bytes=32 seq=4
Ping statistics for 192.168.0.104
Packets: Sent = 4 Received = 4, Lost = 0 (0 % loss)
```

Переходим к обновлению.
Вводим команду:
download firmware_fromTFTP 192.168.0.104 1/PSWupdate407-013-25122014.img
Начнётся процесс загрузки файла во внутреннюю память, а затем и процесс обновления

SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
TFortis PSW-1G4F#download firmware_fromTFTP 192.168.0.104 1/PSWupdate407-013-251
22014.img
Download file:1/PSWupdate407-013-25122014.img
TFortis PSW-1G4F#.............................
Downloading compleat.
Updating start, wait...


Подключение к узлу утеряно.
```

После чего БИ перейдёт к обновлению ПО и перезагрузится, при этом Telnet соединение прервётся.

Процесс обновления длится около 1 минуты. После чего можно снова подключится через Telnet и проверить, версию прошивки, убедившись, что обновление прошло успешно.

```
TFortis PSW-1G4F# show firmware
Firmware Version:        00.01.03
Bootloader Version:      01.00
```

5.4.6 Сохранение и загрузка конфигурации и лога через TFTP

Teleport поддерживают возможность сохранения текущих настроек в файл конфигурации, его редактирования, а также восстановления настроек из файла.

5.4.6.1 Сохранение конфигурации

Сохранение конфигурации происходит на указанный TFTP сервер
upload cfg_toTFTP <IP> <PATH>
где **<IP>** - IP адрес TFTP сервера

<PATH> - имя и путь файла конфигурации

```
TFortis PSW-1G4F#upload cfg_toTFTP 192.168.0.104 psw_config.txt
Upload file:psw_config.txt
TFortis PSW-1G4F#
Uploading...
Uploaded compleat.
```

5.4.6.2 Восстановление конфигурации

Восстановление конфигурации происходит с указанного TFTP сервера
download cfg_fromTFTP <IP> <PATH>
где **<IP>** - IP адрес TFTP сервера

<PATH> - путь до файла конфигурации

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
TFortis PSW-1G4F#download cfg_fromTFTP 192.168.0.104 psw_config.txt
Download file:psw_config.txt
TFortis PSW-1G4F#...
Downloading compleat.
Recovery config from file, wait, reboot...
```

После того, как конфигурация будет установлена, БИ перезагрузится с новыми настройками.

5.4.6.3 Сохранение системного лога

В некоторых случаях бывает необходимо сохранить лог работы устройства для его последующего анализа.
upload log_toTFTP <IP> <PATH>
где **<IP>** - IP адрес TFTP сервера

<PATH> - путь до файла конфигурации

5.4.7 Сохранение настроек

Происходит сохранение настроек в энергонезависимую память.
Save

```
TFortis PSW-1G4F#save
Settings saved successfully
```

5.4.8 Перезагрузка

Происходит перезагрузка
reboot

```
TFortis PSW-1G4F#reboot
Rebooted....
connect closed
TFortis PSW-1G4F#

Подключение к узлу утеряно.
```

5.4.9 Выход из режима управления

Происходит выход из режима управления Telnet
exit

```
TFortis PSW-1G4F#exit
TFortis PSW-1G4F#

Подключение к узлу утеряно.
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.4.10 Диагностические функции

5.4.10.1 Утилита Ping

Позволяет «пропинговать» удаленный узел
ping <IP>
где **<IP> -** IP адрес узла
В случае если узел доступен:

```
TFortis PSW-1G4F#ping 192.168.0.104
Ping 192.168.0.104 with 32 bytes of data
TFortis PSW-1G4F#
Reply from 192.168.0.104 bytes=32 seq=1
Reply from 192.168.0.104 bytes=32 seq=2
Reply from 192.168.0.104 bytes=32 seq=3
Reply from 192.168.0.104 bytes=32 seq=4
Ping statistics for 192.168.0.104
Packets: Sent = 4 Received = 4, Lost = 0 (0 % loss)
```

Если узел недоступен:

```
TFortis PSW-1G4F#ping 192.168.0.11
Ping 192.168.0.11 with 32 bytes of data
TFortis PSW-1G4F#Ping statistics for 192.168.0.11
Packets: Sent = 4 Received = 0, Lost = 4 (100 % loss)
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

6 Диагностика неисправностей

Таблица 6. Список неисправностей и их диагностика

<table>
<tr><th>Проявление проблемы</th><th>Варианты решение проблемы</th></tr>
<tr><td>Устройство не работает, нет индикации RUN</td><td>1) Для Teleport-1:
Проверьте наличие напряжения питания
2) для Teleport-2
Проверьте подключение к PoE коммутатору, проверьте индикатор PoE Если индикатор не горит, убедитесь, что PoE коммутатор может обеспечивать питание по стандарту IEEE 802.1af по варианту A (по парам с данными: 1-2, 3-6)</td></tr>
<tr><td>Ошибки в трансляции входов/выходов</td><td>Для диагностики откройте в web-интерфейсе вкладку Statistics->Main Statistics

RS-485
<table>
<tr><td>RX cnt</td><td>1634</td></tr>
<tr><td>TX cnt</td><td>1634</td></tr>
</table>

Remote Devices
<table>
<tr><td></td><td>Name</td><td>Type</td><td>IP Address</td><td>RX mngmt frames</td><td>TX mngmt frames</td></tr>
<tr><td>1</td><td>описание</td><td>Teleport-2</td><td>192.168.0.2</td><td>1634</td><td>1634</td></tr>
</table>

1) проверить, что на интерфейс RS-485 поступают данные: поле RX cnt (число принятых пакетов на интерфейсе) должно увеличиваться при активности на интерфейсе. Если поле не меняется, проверить настройки порта RS-485, физическое подключение к порту.

2) Поля RX mngmt frames и TX mngmt frames – это счётчики принятых и отправленных управляющих UDP пакетов. Если настроена трансляция только RS-485, то счётчики RX mngmt frames и TX Cnt должны совпадать. Счётчики TX mngmt frames и RX Cnt должны совпадать. Значения RX mngmt frames и TX mngmt frames, RX cnt и TX cnt могут совпадать в том случае, когда устройство, подключенное в локальный порт RS-485 отвечает на все запросы с удалённого порта. В случае, когда используется адресный протокол, например Орион, Modbus RTU, локальное устройство может отвечать только на запросы со своим адресом, поэтому значение поля TX cnt может быть</td></tr>
</table>

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	больше, чем **RX cnt**.
	3) Для проверки связи по Ethernet между двумя устройствами нужно сравнивать счётчики **RX mngmt frames** и **TX mngmt frames.** Если счётчик **RX mngmt frames** одного устройства равен **TX mngmt frames** другого и наоборот, то считаем, что проблем в линиях Ethernet нет.
Мигает индикатор **24V**	Мигающий индикатор 24V на плате блока Teleport-2 свидетельствует о перегрузке или КЗ по выходу 24 В. Отключите мощную нагрузку от выхода.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7 Гарантии изготовителя

Гарантийный срок эксплуатации устройства - 36 месяцев с даты продажи. В гарантийное обслуживание и ремонт принимается устройство в полной комплектности.

Гарантийный ремонт не производится в следующих случаях:

- если гарантийный срок уже истек;
- при отсутствии маркировки с заводским номером на корпусе изделия, а также, если заводской номер был изменен, удален или неразборчив;
- при наличии внешних и внутренних механических повреждений (сколы, трещины, деформация, повреждение шнуров питания, разломы или трещины разъемов), следов воздействия химических веществ, агрессивных сред, жидкостей, сильных загрязнений, а также при наличии насекомых или следов их пребывания;
- из-за несоблюдения правил подключения и эксплуатации, а так же несоответствия параметров электропитания установленных руководством по эксплуатации;
- вследствие форс-мажорных обстоятельств, действий третьих лиц и других причин, независящих от изготовителя.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8 Техническая поддержка

Техническая поддержка по проектированию систем, вопросам эксплуатации и настройки оборудования оказывается:

- по телефону (время для звонков 8-00 — 16-00 по московскому времени)
  8 800 100 112 8
  +7 (342) 260 20 30
- по e-mail:
  support@tfortis.ru

Вся техническая документация доступна на сайте:
https://tfortis.ru/support/dokumentaciya-na-produkciyu/

SEC.RU | Короткий путь к информации
Скачано с sec.ru