ViPNet TLS Gateway

Руководство администратора

infotecs

© ОАО «ИнфоТеКС», 2019

ФРКЕ.00169-01 32 01

Версия продукта 1.4.0

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение ... **8**
О документе ... 9
Для кого предназначен документ ... 9
Соглашения документа ... 9
О ViPNet TLS Gateway ... 11
Исполнения ViPNet TLS Gateway ... 12
Аппаратная архитектура TLS 500 ... 12
Аппаратная архитектура TLS 1000 ... 13
Аппаратная архитектура TLS 5000 ... 14
Программная реализация TLS VA ... 16
Комплект поставки ... 17
Новые возможности версии 1.4.0 ... 18
Обратная связь ... 20

Глава 1. Общие сведения ... **21**
Назначение и основные возможности ... 22
Функциональный состав ViPNet TLS Gateway ... 24
Организация работы ViPNet TLS Gateway ... 25
Типовая схема подключения к сети вашей организации ... 29
Способы подключения пользователей к ViPNet TLS Gateway для доступа к защищаемым ресурсам ... 30
Подключение по каналу TLS с двусторонней аутентификацией ... 30
Подключение по каналу TLS с односторонней аутентификацией ... 32
Разграничение полномочий на основе ролей ... 34
Администратор с правом локального доступа ... 34
Администратор безопасности ... 35
Администратор доступа ... 36
Аудитор ... 37
Лицензирование ... 39

Глава 2. Развертывание виртуального образа ViPNet TLS Gateway ... **42**
Последовательность действий ... 43
Развертывание TLS VA ... 44
Настройка постоянного IP-адреса сетевого интерфейса ... 44
Установка и активация лицензии ... 45

Глава 3. Подготовка ViPNet TLS Gateway к эксплуатации ... 48
Последовательность действий ... 49
Требования к сертификатам для работы с ViPNet TLS Gateway ... 51
Первоначальная инициализация ViPNet TLS Gateway ... 54
Начало инициализации ... 55
Настройка часового пояса, даты и времени ... 57
Создание транспортных ключей ViPNet TLS Gateway ... 57
Настройка модуля WAF ... 57
Настройка сетевых интерфейсов ViPNet TLS Gateway ... 58
Настройка версии протокола TLS для подключения к ViPNet TLS Gateway ... 60
Получение транспортных сертификатов ViPNet TLS Gateway ... 61
Установка сертификатов и CRL ViPNet TLS Gateway ... 62
Завершение инициализации ... 63

Глава 4. Организация работы администраторов ViPNet TLS Gateway ... 65
Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway ... 66
Последовательность действий ... 66
Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway ... 68
Настройка параметров веб-браузера для подключения по протоколу TLS ... 69
Начало работы с веб-интерфейсом ... 69
Подключение к веб-интерфейсу и завершение работы с ним ... 69
Веб-интерфейс ViPNet TLS Gateway ... 70
Установка, обновление и активация лицензии через веб-интерфейс ... 73
Управление доступом администраторов к веб-интерфейсу ... 76
Добавление нового администратора ... 76
Просмотр данных об администраторах и их сертификатах ... 77
Управление ролями администратора ... 79
Изменение версии протокола TLS для подключения администраторов ... 79
Прекращение полномочий администратора ... 80

Глава 5. Организация доступа пользователей к защищаемым ресурсам ... 81
Последовательность действий ... 82
Управление параметрами доступа к ресурсам ... 83
Добавление веб-ресурса ... 83
Добавление TLS-туннеля ... 85
Изменение параметров доступа к ресурсу ... 87
Создание правил преобразования URI ресурса ... 88

Прекращение защищенного доступа к ресурсу 89
Настройка шаблона отображения пользователю страницы доступа к ресурсам 89
Изменение электронного адреса службы поддержки 91
Управление сертификатами доверенных удостоверяющих центров 92
Установление доверия к одному или нескольким удостоверяющим центрам 92
Импорт сертификата и CRL доверенного УЦ 93
Импорт списка сертификатов аккредитованных УЦ 95
Настройка адресов точек распространения CRL 97
Исключение сертификата удостоверяющего центра из списка доверенных 98
Управление доступом пользователей к ресурсам 100
Режимы доступа сертификатов пользователей 101
Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя 102
Блокирование доступа нового пользователя к ViPNet TLS Gateway и ко всем ресурсам 104
Назначение прав доступа к ресурсам по запросу пользователя 105
Правила автоматического назначения пользователям прав доступа к ресурсам 109
Настройка взаимодействия с Active Directory 109
Создание правила предоставления доступа пользователю к заданным ресурсам 112
Задание условий выполнения правила 114
Создание правила блокировки доступа пользователю к ViPNet TLS Gateway и ко всем ресурсам 117
Просмотр, редактирование и настройка порядка применения правил доступа 118
Удаление правила доступа 119
Изменение прав доступа к ресурсам существующего пользователя 119
Изменение прав доступа к ресурсам вручную 120
Применение правил автоматического предоставления доступа 121
Возобновление доступа пользователя к ViPNet TLS Gateway и к ранее запрещенным ресурсам 123
Изменение версии протокола TLS для подключения пользователей 124
Просмотр данных о пользователях и их сертификатах 124

Глава 6. Управление и настройка ViPNet TLS Gateway 126
Управление и настройка с помощью веб-интерфейса 127
Работа с журналом событий 127
Просмотр журнала событий 127
Выгрузка архива журнала событий в файл 128
Мониторинг работоспособности 129

Уровни важности событий ... 130
Оповещение о состоянии ViPNet TLS Gateway ... 130
Просмотр отчетов мониторинга ... 131
Настройка передачи данных в формате CEF ... 132
Самотестирование ... 133
Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway ... 133
Включение и выключение защиты веб-ресурсов от атак ... 135
Сетевые настройки ... 136
Настройка статических маршрутов ... 138
Диагностика сетевого окружения ... 139
Работа с транспортными сертификатами ... 141
Создание запроса на транспортный сертификат ... 142
Загрузка транспортного сертификата ... 143
Изменение назначений транспортного сертификата ... 144
Настройка подключения к защищаемым ресурсам непосредственно по их адресам ... 145
Просмотр данных о транспортных сертификатах ... 146
Настройка даты и времени ... 147
Обновление ViPNet TLS Gateway ... 148
Обновление лицензии ... 148
Обновление ПО ViPNet TLS Gateway ... 149
Обновление транспортных сертификатов ViPNet TLS Gateway ... 151
Дополнительные настройки параметров подключения к ViPNet TLS Gateway ... 151
Управление с помощью консоли Linux ... 154
Контроль целостности ПО ViPNet TLS Gateway ... 154
Выгрузка служебных журналов для диагностики работы ... 155
Повторная инициализация ViPNet TLS Gateway ... 155
Обновление и восстановление целостности ПО ViPNet TLS Gateway ... 157
Смена пароля администратора локального доступа ... 158
Перезагрузка ViPNet TLS Gateway ... 159
Выключение ViPNet TLS Gateway ... 159

Глава 7. Резервное копирование и восстановление данных ... 160
Общие сведения ... 161
Создание резервной копии данных ... 162
Сохранение резервной копии данных на внешний носитель ... 163
Восстановление данных из резервной копии после сбоев ... 165
Восстановление ViPNet TLS Gateway после аппаратного сбоя ... 165

Восстановление ViPNet TLS Gateway после программного сбоя ... 167
Запись образа ПО на USB-носитель ... 168
Установка ПО ViPNet TLS Gateway ... 169
Восстановление данных ... 170
Восстановление данных исполнения TLS VA ... 172

Глава 8. Описание интерфейса Web API ... 173
Общие сведения ... 174
Описание методов Web API ... 175
Сервис инициализации ... 175
Метод «Инициализация веб-приложения» ... 175
Сервис управления запросами на доступ к ресурсам ... 177
Метод «Отправка запроса на доступ к ресурсам» ... 177
Метод «Получение информации о запросе доступа к ресурсам для текущего пользователя» ... 178
Сервис управления защищаемыми ресурсами ... 179
Метод «Получение списка защищаемых ресурсов для пользователя» ... 179
Коды ошибок ... 182

Глава 9. Возможные неполадки и способы их устранения ... 186
Невозможно подключиться к веб-интерфейсу ViPNet TLS Gateway ... 187
Некорректное отображение иконок и меню в веб-интерфейсе ... 189
Отображается ошибка при изменении конфигурационного файла веб-сервера ... 190

Приложение A. Описание структуры сообщения в формате CEF ... 191

Приложение B. История версий ... 194
Новые возможности версии 1.3.2 ... 195
Новые возможности версии 1.3.1 ... 197
Новые возможности версии 1.3 ... 198
Новые возможности версии 1.2.1 ... 200
Новые возможности версии 1.2 ... 201
Новые возможности версии 1.1.1 ... 203
Новые возможности версии 1.1 ... 205

Приложение C. Глоссарий ... 207

Введение

О документе 9

О ViPNet TLS Gateway 11

Новые возможности версии 1.4.0 18

Обратная связь 20

О документе

Для кого предназначен документ

Документ предназначен для администраторов, отвечающих за развертывание и настройку изделия ViPNet TLS Gateway, а также за организацию защищенного удаленного подключения пользователей к веб-ресурсам и туннелируемым ресурсам корпоративной сети.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > **Подменю** > **Команда**	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, выделены красным цветом. Например:

```
команда
```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

  ```
  команда {вариант-1 | вариант-2}
  ```

О ViPNet TLS Gateway

Изделие ViPNet TLS Gateway (далее — ViPNet TLS Gateway) позволяет организовывать безопасный удаленный доступ пользователей к корпоративным информационным веб-ресурсам и туннелируемым ресурсам из любых точек мира путем создания защищенных каналов передачи данных на базе протокола TLS, обеспечивая тем самым криптографически защищенное соединение. При этом ViPNet TLS Gateway позволяет контролировать удаленный доступ пользователей к этим ресурсам.

Удаленный доступ пользователей осуществляется без их прямого обращения к адресам ресурсов за счет прохождения всего трафика через ViPNet TLS Gateway, предоставляющего функции прокси-сервера.

Пользователям для безопасного доступа к ресурсам не нужно устанавливать специальное программное обеспечение на своих компьютерах кроме сертифицированного средства криптографической защиты информации (ViPNet CSP, ViPNet PKI Client или криптопровайдера сторонних производителей).

Примечание. Подключение к туннелируемым ресурсам возможно только в программе ViPNet PKI Client версии не ниже 1.3.

ViPNet TLS Gateway выпускается в следующих исполнениях (см. Исполнения ViPNet TLS Gateway на стр. 12): TLS 500, TLS 1000, TLS 5000 и TLS VA.

ViPNet TLS Gateway в исполнениях TLS 500/1000/5000 представляет собой программно-аппаратный комплекс (далее — ПАК) на базе специализированной аппаратной платформы и программного обеспечения (далее — ПО) ViPNet TLS Gateway, которое функционирует под управлением адаптированной операционной системы (далее — ОС) Debian.

ViPNet TLS Gateway в исполнении TLS 1000 поставляется совместно с модулем Web Application Firewall (далее — WAF) производства компании Positive Technologies. Для использования модуля WAF необходима соответствующая лицензия. (см. Лицензирование на стр. 39)

Модуль WAF — самообучающийся динамический межсетевой экран, способный снижать риски атак на приложения при их появлении. Подробнее о WAF см. документ «ViPNet TLS Gateway Web Application Firewall. Руководство администратора».

ViPNet TLS Gateway в исполнении TLS VA представляет собой программную реализацию ПАК, предназначенную для развертывания в среде виртуализации (см. Программная реализация TLS VA на стр. 16).

Исполнения ViPNet TLS Gateway

Аппаратная архитектура TLS 500

Исполнение TLS 500 выпускается на базе аппаратной платформы TLS 500 Q1, в качестве которой используется сервер AquaServer T41 S24 производства ГК «Аквариус» с процессором Intel Celeron G1820.

Аппаратная платформа TLS 500 Q1 имеет следующие технические характеристики:

Таблица 3. Характеристики TLS 500 Q1

Характеристика	Описание
Форм-фактор	Сервер AquaServer T41 S24 19" Rack 1U
Размеры (ШхВхГ)	430 x 43,4 x 380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Celeron G1820
Оперативная память	От 4 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	2 порта VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 4 порта USB 2.0 2 порта USB 3.0

На передней панели TLS 500 Q1 расположены COM-порт, 2 разъема USB 2.0 и порт VGA.

Рисунок 1. Передняя панель TLS 500 Q1, TLS 1000 Q2

Остальные коммуникационные разъемы находятся на задней панели.

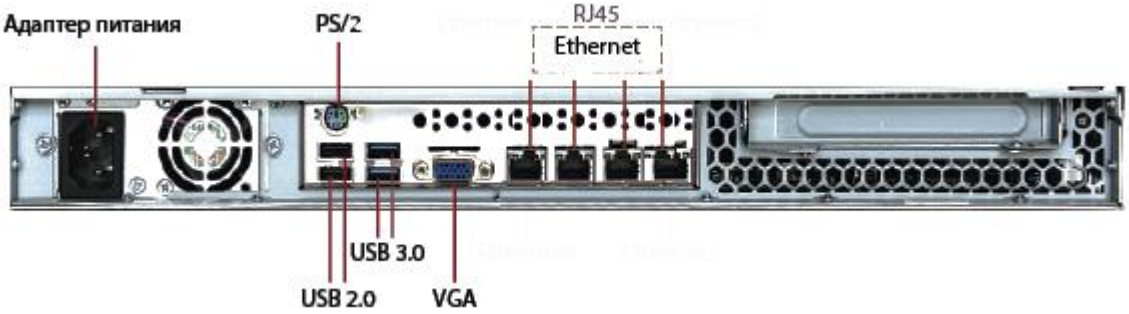

Рисунок 2. Задняя панель TLS 500 Q1, TLS 1000 Q2

Номера сетевых интерфейсов определяются в момент первого подключения сетевого кабеля к разъему сетевого порта.

Аппаратная архитектура TLS 1000

Исполнение TLS 1000 выпускается на базе аппаратной платформы TLS 1000 Q2, в качестве которой используется сервер AquaServer T41 S24 производства ГК «Аквариус» с процессором Intel Core i3-4360.

Аппаратная платформа TLS 1000 Q2 имеет следующие технические характеристики:

Таблица 4. Характеристики TLS 1000 Q2

Характеристика	Описание
Форм-фактор	Сервер AquaServer T41 S24 19” Rack 1U
Размеры (ШхВхГ)	430 x 43,4 x 380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-4360
Оперативная память	От 16 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	2 порта VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 4 порта USB 2.0 2 порта USB 3.0

Аналогично TLS 500 Q1 (на стр. 12), на передней панели TLS 1000 Q2 расположены COM-порт, 2 разъема USB 2.0 и порт VGA.

Остальные коммуникационные разъемы находятся на задней панели (на стр. 13).

Аппаратная архитектура TLS 5000

Исполнение TLS 5000 выпускается на базе аппаратной платформы TLS 5000 Q1, в качестве которой используется сервер AquaServer T51 D15 производства ГК «Аквариус».

Аппаратная платформа TLS 5000 Q1 имеет следующие технические характеристики:

Таблица 5. Характеристики TLS 5000 Q1

Характеристика	Описание
Форм-фактор	Сервер AquaServer T51 D15 — 1U в укороченном корпусе
Размеры (ШхВхГ)	444 x 44 x 383 мм
Масса	13 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100–240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Процессор	2 x Intel Xeon E5-2620v3
Оперативная память	От 24 Гбайт
Накопители	SSD от 2 Гбайт HDD от 1 Тбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP+ 10 Гбит/с 2 порта Broadcom Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 2 порта USB 3.0

На передней панели TLS 5000 Q1 расположен COM-порт RS-232.

Остальные коммуникационные разъемы находятся на задней панели:

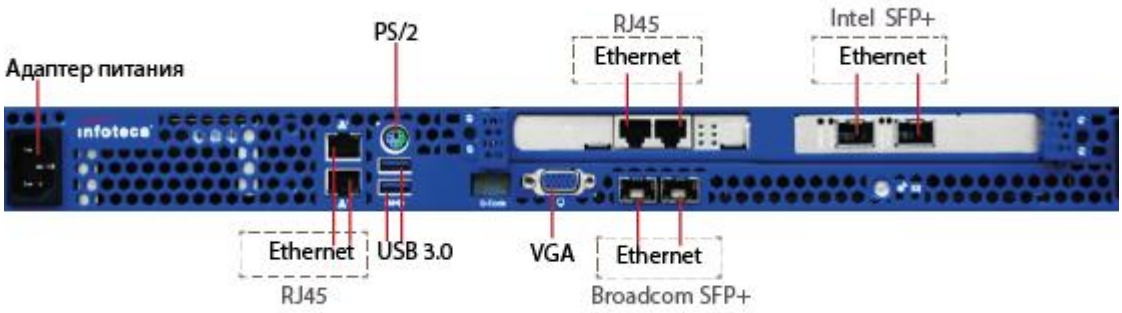

Рисунок 3. Задняя панель TLS 5000 Q1

Номера сетевых интерфейсов определяются в момент первого подключения сетевого кабеля к разъему сетевого порта.

TLS 5000 Q1 имеет двухпортовый сетевой адаптер Intel Ethernet SFP+. С адаптерами этой серии совместимы только следующие модели SFP-трансиверов:

- AFBR-709SMZ производства Avago Technologies (два трансивера этой модели входят в комплект поставки);
- E10GSFPSR производства Intel Corporation;
- E10GSFPLR производства Intel Corporation.

Коммутация 10-гигабитных сетевых портов

Исполнение TLS 5000 имеет один двухпортовый 10-гигабитный сетевой адаптер Intel Ethernet SFP+ и один двухпортовый 10-гигабитный сетевой адаптер Broadcom Ethernet SFP+.

Для подключения всех перечисленных адаптеров к сети можно использовать как SFP-трансиверы, так и кабели, напрямую подключаемые к адаптерам. Подключаемый кабель должен удовлетворять следующим требованиям:

- Любой SFP+ пассивный медный кабель, соответствующий требованиям спецификаций SFF-8431 v4.1 и SFF-8472 v10.4.
- Идентификатор по спецификации SFF-8472 должен иметь значение 03h (SFP или SFP Plus). Вы можете проверить это значение у изготовителя кабеля.
- Максимальная длина кабеля — 7 метров.

Примечание. Нельзя использовать кабель прямого подключения для соединения с гигабитным коммутатором, к которому можно подключать SFP-модули. При таком подключении 10-гигабитные сетевые адаптеры поддерживают только скорость, равную 1 Гбит.

Корпорация Intel производит пассивные медные кабели прямого подключения различной длины, которые полностью совместимы с 10-гигабитными сетевыми адаптерами, используемыми в исполнении TLS 5000. В таблице ниже приведена информация, которая поможет вам приобрести нужный кабель.

Таблица 6. Коды продукции для заказа кабелей прямого подключения

Название продукции	Код продукции
Intel Ethernet SFP+ твинаксиальный кабель, 1 метр	XDACBL1M
Intel Ethernet SFP+ твинаксиальный кабель, 3 метра	XDACBL3M
Intel Ethernet SFP+ твинаксиальный кабель, 5 метров	XDACBL5M

Программная реализация TLS VA

Исполнение TLS VA является программной реализацией ViPNet TLS Gateway и предназначено для развертывания в среде виртуализации.

TLS VA работает на следующих платформах виртуализации:

- Для файла `*.ova`:
  - Oracle VM VirtualBox 5.0, 5.1, 5.2;
  - VMware vSphere ESXi 6.0, 6.5, 6.7;
  - VMware Workstation 14, 15.

Внимание! В связи с тем, что расширение `*.ova` является форматом стандарта OVF (Open Virtualization Format), оно может быть развернуто на любой современной платформе виртуализации. Однако работоспособность в этом случае не гарантируется.

- Для файла `*.qcow2` поддерживаются платформы виртуализации, основанные на Kernel Virtual Machine (KVM).

Внимание! Развертывании образа `*.qcow2` возможно только при использовании IDE-контроллера жесткого диска.

Виртуальная машина, на которой развернуто исполнение TLS VA, должна быть сконфигурирована следующим образом:

- количество ядер процессора — не менее 2;
- объем оперативной памяти — не менее 8 Гбайт;
- количество портов Ethernet 10/100/1000 Мбит/с — не менее 3;
- накопители — не менее 50 Гбайт.

Внимание! На одно логическое ядро процессора должно приходиться не менее 4 Гбайт оперативной памяти.

Если вы планируете устанавливать доверие к аккредитованным УЦ с помощью списка аккредитованных УЦ https://e-trust.gosuslugi.ru/CA в формате Trust-service Status List (TSL) (см.

глоссарий, стр. 208), часть параметров виртуальной машины должны быть сконфигурированы следующим образом:

- количество ядер процессора — не менее 8;
- объем оперативной памяти — не менее 32 Гбайт.

Внимание! Для обеспечения стабильной работы ViPNet TLS Gateway необходимо поддерживать высокую производительность дискового устройства, используемого виртуальной машиной, для выполнения операций чтения/записи. Например, для поддержания высокой скорости операций чтения/записи на диск для платформ виртуализации VMware вы можете использовать рекомендации на сайте VMware https://kb.vmware.com/s/article/1008885.

Комплект поставки

В комплект поставки ViPNet TLS Gateway входят следующие компоненты:

- ViPNet TLS Gateway в одном из следующих исполнений:
  - TLS 500 на базе аппаратной платформы TLS 500 Q1 (см. Аппаратная архитектура TLS 500 на стр. 12).
  - TLS 1000 на базе аппаратной платформы TLS 1000 Q2 (см. Аппаратная архитектура TLS 1000 на стр. 13).
  - TLS 5000 на базе аппаратной платформы TLS 5000 Q1 (см. Аппаратная архитектура TLS 5000 на стр. 14).
  - TLS VA для развертывания в среде виртуализации. Поставляется в виде файлов с образом виртуальной машины `*.ova` и `*.qcow2`.
- Файл с неактивированной базовой лицензией (только для исполнения TLS VA).
- Документация в формате PDF:
  - «ViPNet TLS Gateway. Руководство администратора».
  - «ViPNet TLS Gateway. Руководство пользователя».
  - «ViPNet TLS Gateway Web Application Firewall. Руководство администратора» (только для исполнения TLS 1000).
  - «ViPNet TLS Gateway. Лицензионные соглашения на компоненты сторонних производителей».

Новые возможности версии 1.4.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.4.0 по сравнению с версией 1.3.2. Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 194).

- **Изменения в транспортных сертификатах ViPNet TLS Gateway**
  - Снято ограничение на использование одного транспортного сертификата для обеспечения одного типа доступа

    В предыдущей версии ViPNet TLS Gateway для обеспечения одного типа доступа (администраторов, пользователей с односторонней или двусторонней аутентификацией) использовался один транспортный сертификат. Это было неудобно, если вам, например, не требуется подключение пользователей с двусторонней аутентификацией. В новой версии вы можете использовать один транспортный сертификат для обеспечения одного, двух или трех типов доступа.
  - Снято ограничение на обязательную загрузку транспортных сертификатов для всех типов доступа при проведении первоначальной инициализации

    В предыдущей версии при проведении первоначальной инициализации нужно было обязательно добавлять транспортные сертификаты для обеспечения всех типов доступа (администраторов, пользователей с односторонней или двусторонней аутентификацией). В новой версии при проведении первоначальной инициализации можно добавить только сертификат для обеспечения доступа администраторов, а остальные транспортные сертификаты добавить позднее через веб-интерфейс (см. Работа с транспортными сертификатами на стр. 141).
  - На главную страницу добавлен раздел **Транспортные сертификаты**, предназначенный для управления транспортными сертификатами (см. Работа с транспортными сертификатами на стр. 141).
- **Расширен список алгоритмов для установки защищенных TLS-соединений**

  В новой версии для обеспечения подключения пользователей к ViPNet TLS Gateway помимо сертификатов, сформированных по алгоритмам ГОСТ, могут использоваться сертификаты, сформированные по алгоритмам RSA и ECDSA.
- **Добавлена возможность активации лицензии при отсутствии доступа в Интернет на ViPNet TLS Gateway**

  Теперь вы можете активировать лицензию ViPNet TLS Gateway по электронной почте с помощью файла запроса (см. Установка, обновление и активация лицензии через веб-интерфейс на стр. 73). Это полезно, если ваш ViPNet TLS Gateway установлен в закрытой сети и не имеет доступа в Интернет.
- **Изменения в настройках даты и времени**

  В предыдущей версии вы могли настраивать дату и время только через консоль Linux в процессе первоначальной и повторной инициализации ViPNet TLS Gateway. В новой версии вы

можете настраивать дату и время с помощью веб-интерфейса вручную или синхронизировать с внешними NTP-серверами (см. Настройка даты и времени на стр. 147). В раздел **Система** добавлена вкладка **Дата и время** (см. Настройка даты и времени на стр. 147).

- **Добавлена возможность подключения к защищаемым ресурсам непосредственно по их адресам**

  В предыдущей версии для подключения к защищаемым ресурсам пользователи сначала подключались к ViPNet TLS Gateway и выбирали нужный ресурс из списка доступных или использовали адреса в формате `https://<Адрес ViPNet TLS Gateway для подключения пользователей:порт>/<суффикс подключения>`. В новой версии вы можете настроить ViPNet TLS Gateway таким образом, что пользователи смогут подключаться к защищаемым ресурсам непосредственно по их адресам. Подробнее см. раздел. Настройка подключения к защищаемым ресурсам непосредственно по их адресам (на стр. 145).

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php.

1

Общие сведения

Назначение и основные возможности 22

Функциональный состав ViPNet TLS Gateway 24

Организация работы ViPNet TLS Gateway 25

Типовая схема подключения к сети вашей организации 29

Способы подключения пользователей к ViPNet TLS Gateway для доступа к защищаемым ресурсам 30

Разграничение полномочий на основе ролей 34

Лицензирование 39

Назначение и основные возможности

ViPNet TLS Gateway предназначен для организации удаленного подключения пользователей к корпоративным веб-ресурсам сети и туннелируемым ресурсам по защищенному каналу с помощью односторонней или двусторонней аутентификации по протоколу TLS (см. Способы подключения пользователей к ViPNet TLS Gateway для доступа к защищаемым ресурсам на стр. 30).

ViPNet TLS Gateway обеспечивает контроль удаленного доступа пользователей к корпоративным ресурсам (далее — защищаемым ресурсам) за счет использования следующих механизмов:

- Для установки защищенного TLS-соединения при подключении администраторов к ViPNet TLS Gateway используются ключи ключи электронной подписи и соответствующие им сертификаты, сформированные по алгоритмам ГОСТ.
- Для установки защищенного TLS-соединения при подключении пользователей к ViPNet TLS Gateway используются ключи электронной подписи и соответствующие им сертификаты, сформированные по алгоритмам ГОСТ, RSA или ECDSA.
- Для каждого защищаемого ресурса на ViPNet TLS Gateway администратором настраивается алгоритм шифрования и разрешенный тип подключения пользователя: с помощью односторонней или двусторонней аутентификации по протоколу TLS.
- Пользователям, подключающимся по защищенному каналу TLS с двусторонней аутентификацией, на ViPNet TLS Gateway администратором назначаются права доступа к каждому защищаемому ресурсу (с типом подключения пользователя с помощью двусторонней аутентификации по протоколу TLS).
- При удаленном подключении по защищенному каналу TLS пользователи не имеют прямого доступа к защищаемым ресурсам, поскольку весь трафик проходит через ViPNet TLS Gateway. ViPNet TLS Gateway перенаправляет запросы пользователей защищаемым ресурсам, а полученные от защищаемых ресурсов ответы перенаправляет обратно пользователям. Перенаправление запросов выполняется автоматически в соответствии с настройками доступа пользователей к защищаемым ресурсам, которые произвел администратор.
- Обеспечивается возможность идентификации пользователей на защищаемых веб-ресурсах. В HTTP/HTTPS-запросах, которые ViPNet TLS Gateway перенаправляет от пользователей защищаемым ресурсам, содержится серийный номер сертификата `TlsGateway-Client-Cert-SN` и имя издателя сертификата `TlsGateway-Client-Cert-Issuer-DN`.
- Обеспечивается контроль целостности передаваемой информации.
- Обеспечивается оперативный контроль работоспособности ViPNet TLS Gateway.
- Все действия, производимые на ViPNet TLS Gateway администраторами, фиксируются в журнале событий.

Для реализации своих функций ViPNet TLS Gateway предоставляет вам следующие основные возможности:

- Разграничение полномочий на основе ролей (на стр. 34).
- Управление доступом администраторов к веб-интерфейсу (на стр. 76).
- Управление параметрами доступа к ресурсам (на стр. 83).
- Управление сертификатами доверенных удостоверяющих центров (на стр. 92). Поддерживается возможность загрузки и обновления доверенных списков сертификатов аккредитованных удостоверяющих центров в формате Trust-service Status List (TSL) (см. глоссарий, стр. 208).
- Управление доступом пользователей к ресурсам (на стр. 100).
- Работа с журналом событий (на стр. 127).
- Мониторинг работоспособности (на стр. 129).
- Обновление транспортных сертификатов ViPNet TLS Gateway (на стр. 151).
- Обновление ПО ViPNet TLS Gateway (на стр. 149).
- Резервное копирование и восстановление данных (на стр. 160).
- Управление и настройка ViPNet TLS Gateway (на стр. 126).
- Включение и выключение защиты веб-ресурсов от атак (на стр. 135) (только для исполнения TLS 1000 с модулем WAF).
- Настройка модуля WAF (только для исполнения TLS 1000 с модулем WAF). Подробнее см. документ «ViPNet TLS Gateway Web Application Firewall. Руководство администратора».

Функциональный состав ViPNet TLS Gateway

В состав ViPNet TLS Gateway входят следующие функциональные компоненты:

- Сервер ViPNet TLS Gateway — представляет собой аппаратную или виртуальную (для исполнения TLS VA) платформу со специализированным программным обеспечением ViPNet TLS Gateway, функционирующим под управлением адаптированной ОС Debian. Обеспечивает основные возможности ViPNet TLS Gateway (см. Назначение и основные возможности на стр. 22).
- Рабочее место администратора ViPNet TLS Gateway — представляет собой персональный компьютер заказчика с веб-браузером (см. Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway на стр. 68), подключающийся к серверу ViPNet TLS Gateway по протоколу TLS с двусторонней аутентификацией. С рабочего места администратора ViPNet TLS Gateway производится подключение к веб-интерфейсу сервера ViPNet TLS Gateway для управления защищаемыми ресурсами, доступом администраторов и пользователей, а также других действий согласно назначенной роли (см. Разграничение полномочий на основе ролей на стр. 34).

Общая схема организации работы ViPNet TLS Gateway представлена в разделе Организация работы ViPNet TLS Gateway (на стр. 25).

Организация работы ViPNet TLS Gateway

Общая схема организации работы ViPNet TLS Gateway представлена ниже.

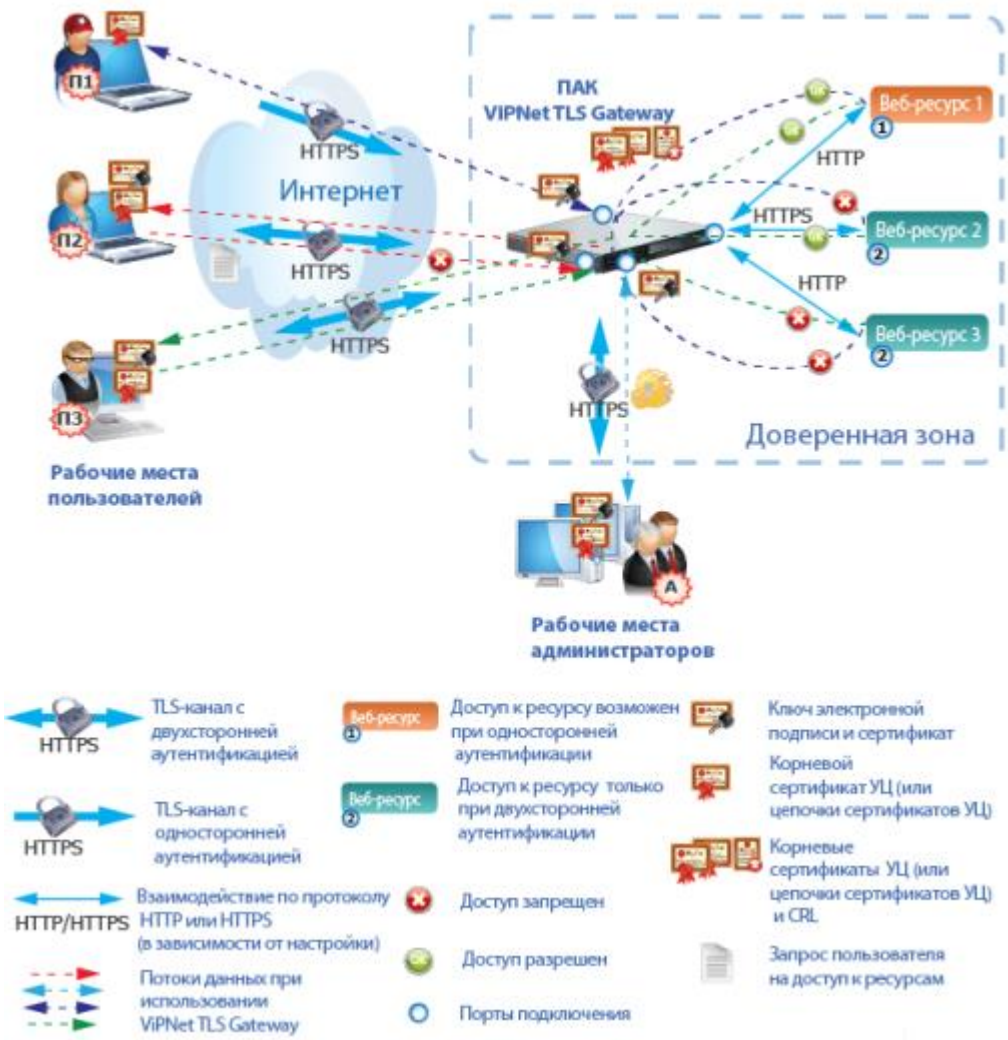

Рисунок 4. Пример схемы работы ViPNet TLS Gateway

Для организации безопасного удаленного HTTPS-доступа пользователей к корпоративным информационным ресурсам и осуществления контроля этого доступа должны быть выполнены следующие условия:

- ViPNet TLS Gateway развернут (см. Типовая схема подключения к сети вашей организации на стр. 29) и настроен в доверенной зоне корпоративной сети (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).

  Для защищенного подключения администраторов, пользователей по TLS-каналу с односторонней аутентификацией и пользователей по TLS-каналу с двусторонней

аутентификацией на ViPNet TLS Gateway должны быть настроены сетевые интерфейсы. Это могут быть разные сетевые интерфейсы ViPNet TLS Gateway с отличающимися IP-адресами или один сетевой интерфейс, но с разными портами подключения. Также должен быть выбран сетевой интерфейс для подключения ViPNet TLS Gateway к ресурсам корпоративной сети для осуществления функций прокси-сервера.

Для установления защищенного TLS-соединения между ViPNet TLS Gateway и рабочими местами пользователей (администраторов) на ViPNet TLS Gateway должны использоваться ключи электронной подписи и соответствующие им сертификаты (далее — транспортные ключи и транспортные сертификаты). Для каждого типа подключения может использоваться как отдельный транспортный ключ и соответствующий транспортный сертификат ViPNet TLS Gateway: сертификат для подключения администраторов, сертификат для подключения пользователей по TLS-каналу с односторонней аутентификацией, сертификат для подключения пользователей по TLS-каналу с двусторонней аутентификацией, так и один общий. Транспортные сертификаты используются для проверки подлинности ViPNet TLS Gateway при подключении к нему администраторов и пользователей. Набор транспортных ключей и первоначальные запросы на транспортные сертификаты формируются в процессе первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). По этим запросам администратором сертифицированного удостоверяющего центра (далее — УЦ) должны быть изданы транспортные сертификаты (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51). После чего эти сертификаты должны быть загружены на ViPNet TLS Gateway. Также при первоначальной инициализации необходимо установить доверие к УЦ, где изданы транспортные сертификаты. Для этого должны быть загружены корневой сертификат УЦ (см. глоссарий, стр. 210), в котором изданы транспортные сертификаты, а также список аннулированных сертификатов (см. глоссарий, стр. 211) УЦ.

Внимание! Если сертификат УЦ не является корневым, то должны быть последовательно загружены сертификаты всех УЦ, образующие цепочку доверия к сертификатам (см. глоссарий, стр. 211), начиная с корневого сертификата (см. глоссарий, стр. 210), а также список аннулированных сертификатов (см. глоссарий, стр. 211) каждого УЦ цепочки.

- Выделены несколько сотрудников вашей организации и назначены необходимые роли администрирования ViPNet TLS Gateway, разграничивающие обязанности сотрудников по администрированию (см. Разграничение полномочий на основе ролей на стр. 34). Рабочие места этих сотрудников (далее — администраторов) подключены к интерфейсу управления ViPNet TLS Gateway по защищенному каналу с двусторонней аутентификацией по протоколу TLS (см. Организация работы администраторов ViPNet TLS Gateway на стр. 65).

  Для установки защищенного соединения и аутентификации администратора на его рабочем месте, с которого будет происходить подключение, должны использоваться ключи электронной подписи и соответствующий им сертификат. Их использование обеспечивает криптографически защищенное соединение. При этом низкоуровневые криптографические функции может выполнять криптопровайдер ViPNet CSP, ViPNet PKI Client или криптопровайдер сторонних производителей. Одну из этих программ необходимо установить на компьютере администратора. Сертификат администратора (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51) должен быть издан в том же УЦ, что и транспортные сертификаты ViPNet TLS Gateway. Сертификат администратора, а также корневой

сертификат УЦ, в котором издан сертификат администратора (или сертификаты всех УЦ, образующие цепочку доверия к сертификатам (см. глоссарий, стр. 211) этого УЦ), должны быть установлены на компьютере администратора в системное хранилище.

- На ViPNet TLS Gateway добавлены защищаемые ресурсы и произведены настройки параметров доступа к ним (см. Добавление веб-ресурса на стр. 83).
- Удаленный доступ пользователей к защищаемым ресурсам сети должен осуществляться через ViPNet TLS Gateway по защищенному каналу TLS с двусторонней или односторонней аутентификацией (см. Способы подключения пользователей к ViPNet TLS Gateway для доступа к защищаемым ресурсам на стр. 30). На ViPNet TLS Gateway должны быть произведены необходимые настройки доступа пользователей к защищаемым ресурсам (см. Управление доступом пользователей к ресурсам на стр. 100).

В результате пользователи при подключении к ViPNet TLS Gateway по защищенному каналу TLS будут получать доступ к защищаемым ресурсам в соответствии с типом подключения и разрешением на подключение к ресурсам (только при двусторонней аутентификации), выданным администратором.

Также при подключении по защищенному каналу TLS с двусторонней аутентификацией пользователи смогут отправить запрос на получение доступа к необходимым защищаемым ресурсам. После чего администратор обработает запрос и по каждому запрашиваемому ресурсу примет решение, предоставить доступ пользователю или нет.

Например, на вышеуказанной схеме на ViPNet TLS Gateway добавлены три ресурса и произведены следующие настройки параметров доступа к ним:

- Для веб-ресурса 1 выбран тип подключения пользователей **Односторонняя аутентификация по протоколу TLS**. К этому ресурсу смогут получить доступ все пользователи, подключающиеся к ViPNet TLS Gateway с односторонней аутентификацией, а также пользователи, которым не запрещен доступ к ViPNet TLS Gateway, подключающиеся с двусторонней аутентификацией.
- Для веб-ресурса 2 и веб-ресурса 3 выбран тип подключения пользователей **Двусторонняя аутентификация по протоколу TLS**. К этим ресурсам смогут получить доступ пользователи, подключающиеся к ViPNet TLS Gateway с двусторонней аутентификацией, если администратор доступа разрешил к ним доступ.
- Доступ к веб-ресурсу 2 со стороны ViPNet TLS Gateway для перенаправления запросов пользователей возможен только по протоколу HTTPS. В связи с чем в настройках параметров доступа этого ресурса протокол HTTPS выбран для доступа ViPNet TLS Gateway к веб-ресурсу 2.

Пользователи П1, П2, П3 подключаются к ViPNet TLS Gateway для доступа к ресурсам, используя разные типы аутентификации:

- Пользователь П1 подключается к ViPNet TLS Gateway по каналу TLS с односторонней аутентификацией и получает доступ к веб-ресурсу 1. Остальные ресурсы ему недоступны.
- Пользователи П2 и П3 подключаются по каналу TLS с двусторонней аутентификацией. Пользователь П2 отправил запрос на доступ к ресурсам 2 и 3. Администратор доступа обработал запрос (тем самым добавив сертификат пользователя на ViPNet TLS Gateway) и

полностью запретил пользователю П2 доступ к ViPNet TLS Gateway (следовательно, и ко всем ресурсам). В результате все ресурсы пользователю недоступны.

- Сертификат пользователя П3 администратор доступа заранее добавил на ViPNet TLS Gateway, а также разрешил доступ к веб-ресурсу 2 и запретил доступ к веб-ресурсу 3. В результате у пользователя П2 есть доступ к ресурсу 2, а ресурс 3 ему недоступен. При этом пользователь П3 будет иметь доступ и к веб-ресурсу 1.

Если в вашей организации нет удостоверяющего центра, для получения необходимых сертификатов вы можете обратиться в ОАО «ИнфоТеКС» (см. Обратная связь на стр. 20).

Типовая схема подключения к сети вашей организации

Типовая схема подключения ViPNet TLS Gateway к корпоративной сети представлена на рисунке ниже.

Рисунок 5. Схема подключения ViPNet TLS Gateway

Чтобы обеспечить удаленное подключение пользователей к веб-ресурсам корпоративной сети, должны быть выполнены следующие настройки (предполагается, что сетевые настройки соответствуют представленным на схеме):

1. На маршрутизаторе 1, расположенном на границе корпоративной сети, настроены правила трансляции IP-адресов (NAT) из внешней сети (Интернет) во внутреннюю (корпоративную) по портам, заданным на ViPNet TLS Gateway для разных типов подключения (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).
2. На ViPNet TLS Gateway заданы:
   - шлюз по умолчанию на внутренний адрес маршрутизатора 1 (см. Сетевые настройки на стр. 136);
   - статические маршруты к подсетям расположения веб-ресурсов (см. Настройка статических маршрутов на стр. 138).

Способы подключения пользователей к ViPNet TLS Gateway для доступа к защищаемым ресурсам

Удаленный доступ пользователей к защищаемым ресурсам осуществляется через ViPNet TLS Gateway по защищенному каналу TLS. При этом аутентификация пользователя может производиться одним из следующих способов:

- Двусторонняя аутентификация (см. Подключение по каналу TLS с двусторонней аутентификацией на стр. 30).
- Односторонняя аутентификация (см. Подключение по каналу TLS с односторонней аутентификацией на стр. 32).

Подключение по каналу TLS с двусторонней аутентификацией

Для установки защищенного соединения по протоколу TLS и двусторонней аутентификации пользователя на его рабочем месте, с которого будет происходить подключение к ViPNet TLS Gateway, должны использоваться ключи электронной подписи и соответствующий им сертификат. Их использование обеспечивает криптографически защищенное соединение. При этом низкоуровневые криптографические функции может выполнять криптопровайдер ViPNet CSP, ViPNet PKI Client или криптопровайдер сторонних производителей, который необходимо установить на компьютере пользователя.

Сертификаты пользователей могут быть изданы в любом сертифицированном УЦ. На ViPNet TLS Gateway должно быть установлено доверие к УЦ, где изданы сертификаты пользователей (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92). Администратор доступа должен добавить сертификат пользователя на ViPNet TLS Gateway и явно разрешить или запретить пользователю доступ к каждому ресурсу (вручную или по запросу пользователя), для которых на ViPNet TLS Gateway настроена возможность получения доступа при двусторонней аутентификации. Пользователям также будут доступны те ресурсы, для которых на ViPNet TLS Gateway настроена возможность получения доступа по каналу TLS с односторонней аутентификацией.

Доступ пользователя к ресурсам по каналу TLS с двусторонней аутентификацией возможен при наличии у него следующих сертификатов:

- Сертификата пользователя (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51).
- Сертификата УЦ, в котором издан сертификат пользователя.
- Сертификата УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway.
- Если какой-либо из вышеуказанных сертификатов УЦ не является корневым, то потребуются сертификаты всех УЦ, образующие цепочку доверия к сертификатам УЦ, выпустившим сертификаты (пользователя и ViPNet TLS Gateway) (см. глоссарий, стр. 211).

Все сертификаты должны быть действительными (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51) и установлены на компьютере пользователя в системное хранилище ОС.

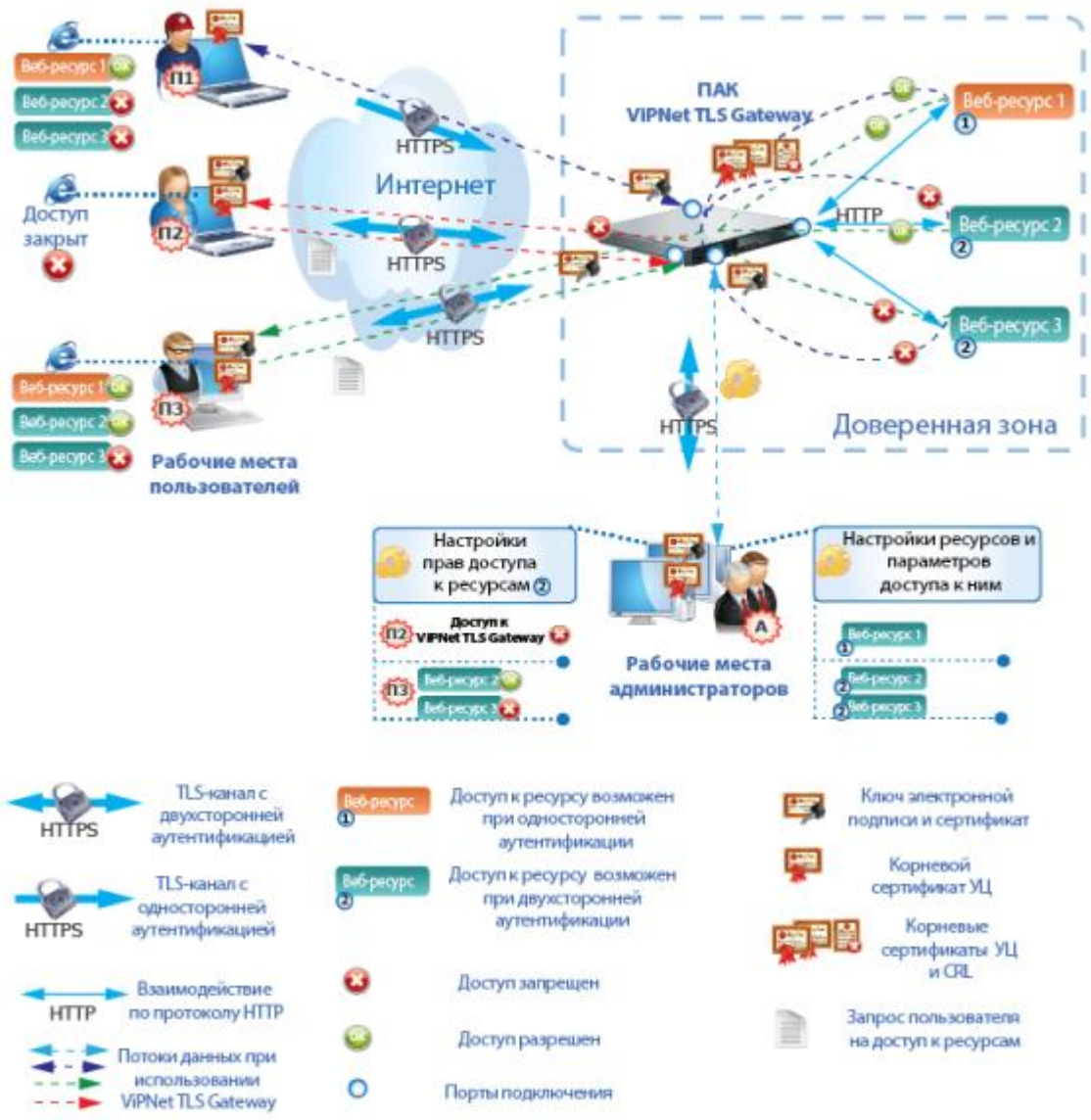

Рисунок 6. Пример подключения по каналу TLS с двусторонней аутентификацией

При подключении пользователей к ViPNet TLS Gateway с использованием двусторонней аутентификации по протоколу TLS производятся следующие проверки:

- Со стороны пользователя проверяется транспортный сертификат ViPNet TLS Gateway (см. глоссарий, стр. 211) и IP-адрес (или DNS-имя) интерфейса подключения по TLS-каналу с двусторонней аутентификацией, прописанные в данном сертификате. Действительность транспортного сертификата (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51) проверяется с помощью корневого сертификата УЦ, в котором издан транспортный сертификат ViPNet TLS Gateway, установленного на компьютере пользователя или с помощью цепочки доверия к сертификату (см. глоссарий, стр. 211).
- Со стороны ViPNet TLS Gateway проверяется:
  - Действительность сертификата пользователя (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51).

    Внимание! Чтобы успешно проводилась проверка действительности сертификатов по времени, время на ViPNet TLS Gateway и в УЦ должно быть синхронизировано.
  - Наличие сертификата пользователя в списке разрешенных сертификатов пользователей.
  - Что установлено доверие к УЦ, где изданы сертификаты пользователей (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92).

При успешной аутентификации будет установлено защищенное взаимодействие и отобразится главная страница ViPNet TLS Gateway со списком доступных защищаемых ресурсов (если есть) и кнопкой запроса необходимых ресурсов.

Подключение по каналу TLS с односторонней аутентификацией

Для доступа пользователя к ресурсам по каналу TLS с односторонней аутентификацией достаточно иметь только действительный корневой сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway. Если сертификат УЦ не является корневыми, то потребуются сертификаты всех УЦ, образующие цепочку доверия к сертификатам (см. глоссарий, стр. 211). Пользователям будут доступны только те ресурсы, для которых на ViPNet TLS Gateway настроена возможность получения доступа при односторонней аутентификации. Доступ к этим ресурсам не разграничивается.

Все сертификаты должны быть установлены на компьютере пользователя в системное хранилище ОС.

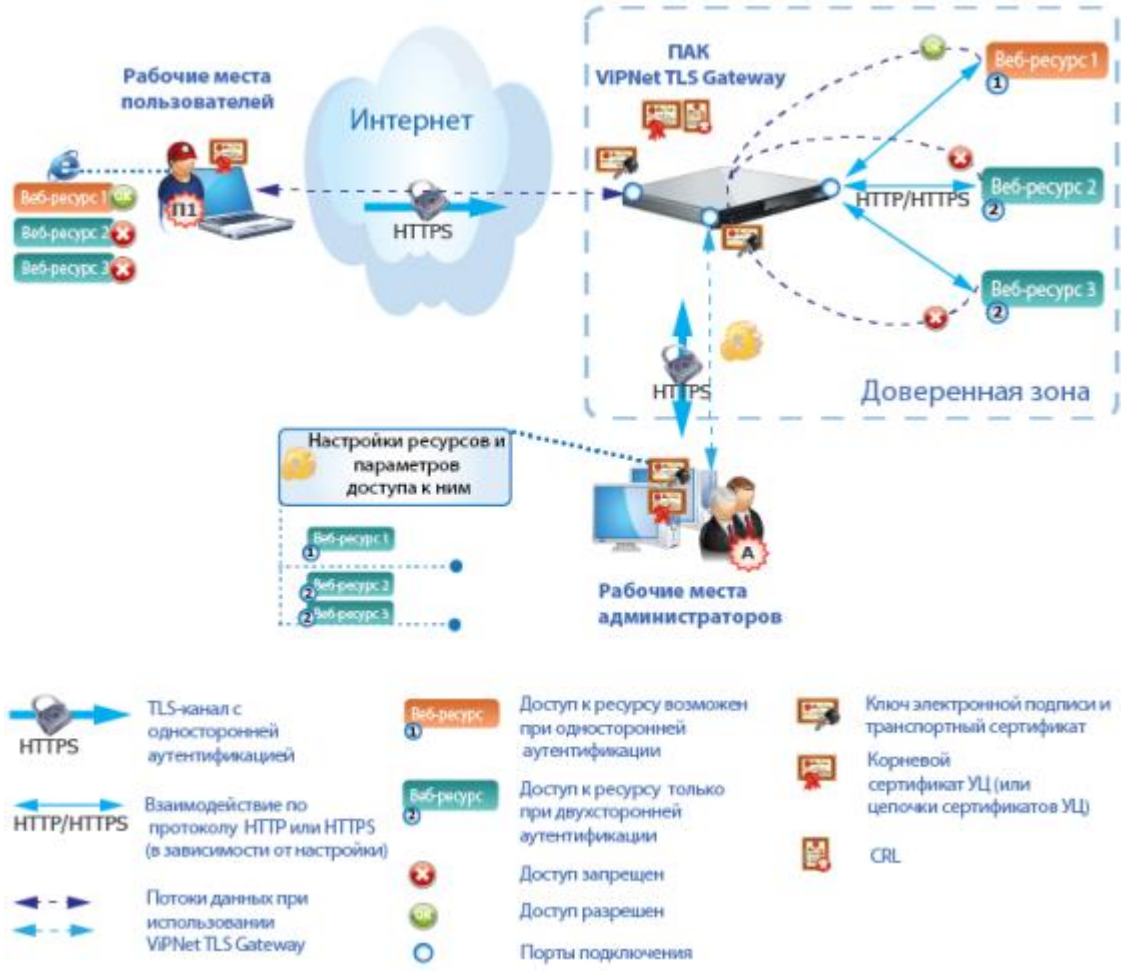

Рисунок 7. Пример подключения по каналу TLS с односторонней аутентификацией

При подключении пользователей к ViPNet TLS Gateway с использованием односторонней аутентификации по протоколу TLS со стороны пользователя проверяется транспортный сертификат ViPNet TLS Gateway (см. глоссарий, стр. 211) и IP-адрес (или DNS-имя) интерфейса подключения по TLS-каналу с односторонней аутентификацией, прописанные в данном сертификате.

Действительность транспортного сертификата (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51) проверяется с помощью корневого сертификата УЦ, в котором издан транспортный сертификат ViPNet TLS Gateway, установленного на компьютере пользователя или с помощью цепочки доверия к сертификату (см. глоссарий, стр. 211).

При успешной аутентификации будет установлено защищенное взаимодействие и отобразится главная страница ViPNet TLS Gateway со списком доступных защищаемых ресурсов (если они есть).

Разграничение полномочий на основе ролей

Управление ViPNet TLS Gateway реализовано с помощью ролевой модели доступа, которая обеспечивает разграничение полномочий администраторов. Роли определяют действия администраторов, доступные им при управлении ViPNet TLS Gateway.

В ViPNet TLS Gateway существуют следующие роли администраторов:

- Администратор с правом локального доступа (на стр. 34). Роль предназначена для выполнения действий в консоли Linux.
- Роли управления с помощью веб-интерфейса ViPNet TLS Gateway:
  - Администратор безопасности (на стр. 35).
  - Администратор доступа (на стр. 36).
  - Аудитор (на стр. 37).

Все роли управления с помощью веб-интерфейса ViPNet TLS Gateway назначаются администраторам при загрузке их сертификатов на ViPNet TLS Gateway. При первичной инициализации ViPNet TLS Gateway администратором с правом локального доступа должен быть загружен сертификат администратора, которому будет назначена роль администратора безопасности. Другим администраторам роли назначаются администратором безопасности в веб-интерфейсе ViPNet TLS Gateway.

Примечание. Ключи электронной подписи и соответствующие им сертификаты администраторов должны быть сформированы только по алгоритмам ГОСТ.

Каждый администратор может иметь одну или несколько ролей управления с помощью веб-интерфейса ViPNet TLS Gateway. При необходимости можно добавить сертификаты нескольких администраторов и назначить им одинаковые роли управления с помощью веб-интерфейса ViPNet TLS Gateway.

Администратор с правом локального доступа

Администратор с правом локального доступа может управлять ViPNet TLS Gateway только посредством консоли Linux. Ему доступны следующие действия:

- Развертывание виртуального образа ViPNet TLS Gateway (на стр. 42).
- Первоначальная инициализация ViPNet TLS Gateway (на стр. 54).

- Повторная инициализация в случае возникновения проблем при удаленном управлении (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).
- Восстановление данных из резервной копии в случае сбоев (см. Восстановление данных из резервной копии после сбоев на стр. 165).

Администратор с правом локального доступа не имеет доступа к веб-интерфейсу. Администратором с правом локального доступа назначается уполномоченный сотрудник организационными мерами.

Администратор безопасности

Администратор безопасности отвечает за управление доступом других администраторов к веб-интерфейсу ViPNet TLS Gateway.

Список всех действий, которые может выполнять администратор безопасности, приведен в таблице ниже.

Таблица 7. Доступные действия администратора безопасности

Действие	Ссылка
Управление доступом администраторов к веб-интерфейсу ViPNet TLS Gateway	• Управление доступом администраторов к веб-интерфейсу (на стр. 76)
Управление настройками ViPNet TLS Gateway	• Обновление транспортных сертификатов ViPNet TLS Gateway (на стр. 151) • Установление доверия к одному или нескольким удостоверяющим центрам (на стр. 92) • Настройка адресов точек распространения CRL (на стр. 97) • Исключение сертификата удостоверяющего центра из списка доверенных (на стр. 98) • Сетевые настройки (на стр. 136)
Просмотр списка сертификатов пользователей	• Просмотр данных о пользователях и их сертификатах (на стр. 124)
Просмотр списка ресурсов	• Управление параметрами доступа к ресурсам (на стр. 83) (только просмотр)

Действие	Ссылка
Мониторинг ViPNet TLS Gateway и просмотр журнала событий	• Уровни важности событий (на стр. 130) • Оповещение о состоянии ViPNet TLS Gateway (на стр. 130) • Просмотр отчетов мониторинга (на стр. 131) • Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway (на стр. 133) • Запуск процедуры самотестирования (см. Самотестирование на стр. 133) • Просмотр журнала событий (на стр. 127)
Изменение версии протокола TLS для подключения администраторов и пользователей	• Изменение версии протокола TLS для подключения администраторов (на стр. 79) • Изменение версии протокола TLS для подключения пользователей (на стр. 124)

Администратор доступа

Администратор доступа отвечает за управление доступом пользователей к веб-ресурсам, а также за управление параметрами веб-ресурсов.

Список всех действий, которые может выполнять администратор доступа, приведен в таблице ниже.

Таблица 8. Доступные действия администратора доступа

Действие	Ссылка
Управление доступом пользователей к корпоративным ресурсам	• Назначение прав доступа к ресурсам по запросу пользователя (на стр. 105) • Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя (на стр. 102) • Изменение прав доступа к ресурсам существующего пользователя (на стр. 119) • Просмотр данных о пользователях и их сертификатах (на стр. 124)
Управление правилами предоставления доступа пользователям к ресурсам	• Правила автоматического назначения пользователям прав доступа к ресурсам (на стр. 109)
Управление настройками доступа к ресурсам	• Добавление веб-ресурса (на стр. 83) • Добавление TLS-туннеля (на стр. 85) • Изменение параметров доступа к ресурсу (на стр. 87) • Прекращение защищенного доступа к

Действие	Ссылка
	ресурсу (на стр. 89) • Настройка шаблона отображения пользователю страницы доступа к ресурсам (на стр. 89)
Установка и активация лицензии	• Обновление и активация лицензии (см. Обновление лицензии на стр. 148)
Управление сетевыми настройками	• Сетевые настройки (на стр. 136)
Резервное копирование данных	• Создание резервной копии данных (на стр. 162) • Сохранение резервной копии данных на внешний носитель (на стр. 163)
Мониторинг ViPNet TLS Gateway и просмотр журнала событий	• Уровни важности событий (на стр. 130) • Оповещение о состоянии ViPNet TLS Gateway (на стр. 130) • Просмотр отчетов мониторинга (на стр. 131) • Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway (на стр. 133) • Запуск процедуры самотестирования (см. Самотестирование на стр. 133) • Просмотр журнала событий (на стр. 127)
Просмотр списка сертификатов администраторов	• Просмотр данных об администраторах и их сертификатах (на стр. 77)
Обновление ПО ViPNet TLS Gateway	• Загрузка и запуск обновления ПО ViPNet TLS Gateway (см. Обновление ПО ViPNet TLS Gateway на стр. 149)
Настройка модуля WAF (для исполнения TLS 1000 с модулем WAF (см. Аппаратная архитектура TLS 1000 на стр. 13))	• Включение и выключение защиты веб-ресурсов от атак (на стр. 135) • документ «ViPNet TLS Gateway Web Application Firewall. Руководство администратора»
Тонкая настройка параметров подключения пользователей к защищаемым ресурсам	• Дополнительные настройки ViPNet TLS Gateway (см. Дополнительные настройки параметров подключения к ViPNet TLS Gateway на стр. 151)

Аудитор

Аудитор отвечает за просмотр и архивацию журнала событий.

Список всех действий, которые может выполнять аудитор, приведен в таблице ниже.

Таблица 9. Доступные действия аудитора

Действие	Ссылка
Мониторинг ViPNet TLS Gateway и просмотр журнала событий	• Уровни важности событий (на стр. 130) • Оповещение о состоянии ViPNet TLS Gateway (на стр. 130) • Просмотр отчетов мониторинга (на стр. 131) • Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway (на стр. 133) • Просмотр журнала событий (на стр. 127)
Скачивание архивов журнала событий	• Выгрузка архива журнала событий в файл (на стр. 128)
Просмотр списка ресурсов	• Управление параметрами доступа к ресурсам (на стр. 83) (только просмотр)
Просмотр списка сертификатов администраторов и пользователей	• Просмотр данных об администраторах и их сертификатах (на стр. 77) • Просмотр данных о пользователях и их сертификатах (на стр. 124)

Лицензирование

Лицензия дает вам право на использование изделия ViPNet TLS Gateway и подтверждает, что используемое изделие является легальным и поддерживается производителем.

Внимание! Вы не имеете права копировать и переносить ПО ViPNet TLS Gateway на другие аппаратные или виртуальные платформы. Попытка клонирования ViPNet TLS Gateway является нарушением лицензии.

Файл лицензии содержит следующую информацию:

- Вариант исполнения ViPNet TLS Gateway.
- Максимальная версия ПО ViPNet TLS Gateway, до которой возможно обновление.
- Срок действия лицензии.
- Разрешение на использование модуля Web Application Firewall (только для исполнения TLS 1000).
- Максимальное количество действительных сертификатов пользователей, которые можно добавить на ViPNet TLS Gateway.
- Максимальное количество одновременных подключений по протоколу TLS с односторонней аутентификацией к веб-ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения. По истечении этого срока пользователи не смогут подключаться к веб-ресурсам по протоколу TLS с односторонней аутентификацией, а все существующие соединения будут разорваны.
- Максимальное количество одновременных подключений по протоколу TLS с односторонней аутентификацией к туннелируемым ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения. По истечении этого срока пользователи не смогут подключаться к туннелируемым ресурсам по протоколу TLS с односторонней аутентификацией, а все существующие соединения будут разорваны.
- Максимальное количество одновременных подключений по протоколу TLS с двусторонней аутентификацией к веб-ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения. По истечении этого срока пользователи не смогут подключаться к веб-ресурсам по протоколу TLS с двусторонней аутентификацией, а все существующие соединения будут разорваны.

Внимание! При обновлении до версии 1.3.1 и выше требуется файл лицензии, который содержит информацию о максимальном количестве одновременных подключений по протоколу TLS с односторонней и двусторонней аутентификацией. В противном случае пользователи не смогут подключаться к защищаемым веб-ресурсам и туннелируемым ресурсам.

При истечении срока действия лицензии блокируется доступ пользователей к защищаемым ресурсам по протоколу TLS. Для возможности обновления лицензии останется доступ к ViPNet TLS Gateway всех ранее подключенных администраторов.

При покупке аппаратного исполнения ViPNet TLS Gateway на нем уже установлена и активирована лицензия.

В комплект поставки программного исполнения TLS VA входит неактивированная лицензия. В процессе развертывания виртуального образа ее необходимо установить и активировать (см. Установка и активация лицензии на стр. 45).

При необходимости изменить или расширить параметры лицензии вы можете обратиться в отдел продаж ОАО «ИнфоТеКС».

По истечении срока действия лицензии ее необходимо обновить (см. Обновление лицензии на стр. 148).

Если в процессе эксплуатации ViPNet TLS Gateway вы изменили конфигурацию используемой аппаратной платформы (или виртуальной машины), лицензия может стать недействительной и для продолжения работы потребуется ее повторная активация (см. Обновление лицензии на стр. 148). Такая ситуация возможна при существенных изменениях в конфигурации аппаратной платформы (или виртуальной машины). Изменения считаются существенными, если конфигурация изменилась более чем на 50%. В таблице ниже приведен список возможных изменений конфигурации и их процентное влияние на существенность.

Таблица 10. Список возможных изменений конфигурации и влияние на существенность

Изменения	Влияние на существенность
Замена процессора, изменение количества процессоров или включение/отключение режима hyper-threading	40%
Замена сетевого интерфейса или изменение количества сетевых интерфейсов	20%
Замена жесткого диска или повторная разбивка жесткого диска на разделы	20%
Изменение количества оперативной памяти	20%

Примечание. Изменения разных типов (из разных строк таблицы) суммируются, и тем самым существенность изменений конфигурации увеличивается в соответствии с процентами оказываемого влияния.

Изменения конфигурации одного и того же типа (из одной строки таблицы) не суммируются.

Если произошли существенные изменения конфигурации аппаратной платформы (или виртуальной машины), то будет требоваться повторная активация лицензии (см. Обновление лицензии на стр. 148).

Совет. Рекомендуем не изменять конфигурацию используемой аппаратной платформы (или виртуальной машины) без крайней необходимости. Перед изменением конфигурации обязательно сохраните резервную копию (см. Сохранение резервной копии данных на внешний носитель на стр. 163).

2

Развертывание виртуального образа ViPNet TLS Gateway

Последовательность действий 43

Развертывание TLS VA 44

Установка и активация лицензии 45

Последовательность действий

Для развертывания исполнения TLS VA на платформе виртуализации вам потребуется файл с образом виртуальной машины с расширением `*.ova` или `*.qcow2` и файл с базовой лицензией, входящие в комплект поставки. Чтобы развернуть TLS VA на платформе виртуализации, выполните все действия, приведенные в таблице ниже.

Таблица 11. Порядок развертывания TLS VA

	Действие	Ссылка
☐	Разверните виртуальный образ TLS VA	Развертывание TLS VA (на стр. 44)
☐	Установите и активируйте лицензию	Установка и активация лицензии (на стр. 45)
☐	Выполните подготовку ViPNet TLS Gateway к эксплуатации	Подготовка ViPNet TLS Gateway к эксплуатации (на стр. 48)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Развертывание TLS VA

Чтобы развернуть исполнение TLS VA на платформе виртуализации, выполните следующие действия:

Примечание. Описание развертывания TLS VA приведено на примере файла с расширением `*.ova` на платформе виртуализации VMware Workstation. Развертывание на других платформах виртуализации производится аналогичным образом.

---

1 В главном окне программы VMware Workstation в меню **File** выберите пункт **Open** и укажите путь к файлу с расширением `*.ova`, содержащему образ виртуальной машины.

2 В окне **Import Virtual Machine** при необходимости измените имя виртуальной машины и нажмите кнопку **Import**.

3 Дождитесь завершения процесса импорта и создания виртуальной машины с указанным именем.

4 Запустите виртуальную машину, щелкнув ссылку **Power on this virtual machine**. Запустится установка ПО ViPNet TLS Gateway.

5 Дождитесь завершения установки и сконфигурируйте виртуальную машину согласно системным требованиям из раздела Программная реализация TLS VA (на стр. 16).

Если необходимо, измените параметры сетевых интерфейсов виртуальной машины. Далее установите и активируйте лицензию ViPNet TLS Gateway (см. Установка и активация лицензии на стр. 45).

Настройка постоянного IP-адреса сетевого интерфейса

Если в процессе первоначальной инициализации или восстановления вам необходимо назначить постоянный IP-адрес для сетевого интерфейса ViPNet TLS Gateway, после выбора соответствующей настройки выполните следующие действия:

1 В строке **Enter a new ip for interface <название интерфейса>** введите IP-адрес сетевого интерфейса. Например, `10.10.10.10`.

2 В строке **Enter a new netmask for interface <название интерфейса>** введите маску сети. Например, `255.255.255.0`.

3 В строке **Enter a new default gateway** введите IP-адрес шлюза по умолчанию.

Если сетевые настройки заданы правильно, сеть будет успешно сконфигурирована и отобразится шаг указания пути к файлу с лицензией.

Установка и активация лицензии

Для работы ViPNet TLS Gateway нужно установить и активировать лицензию.

Установить и активировать лицензию можно следующими способами:

- Через консоль Linux в процессе развертывания TLS VA. Активация лицензии производится автоматически через Интернет в режиме реального времени. Для активации необходимо обеспечить доступ одного из сетевых интерфейсов ViPNet TLS Gateway в Интернет.
- С помощью веб-интерфейса после развертывания TLS VA (см. Установка, обновление и активация лицензии через веб-интерфейс на стр. 73). Активация лицензии может производится через Интернет или вручную с помощью файла запроса.

Перед началом лицензирования ViPNet TLS Gateway запишите на USB-носитель файл с базовой лицензией.

Примечание. USB-носитель должен быть предварительно отформатирован в одну из следующих файловых систем: ext2, ext3, ext4 или FAT32.

Чтобы произвести лицензирование ViPNet TLS Gateway, выполните следующие действия:

1 Запустите ViPNet TLS Gateway (если он еще не запущен) и дождитесь завершения загрузки.

2 Подключите к виртуальной машине USB-носитель с лицензией.

3 На экране появится консоль Linux с приглашением ввести имя учетной записи администратора с правом локального доступа ViPNet TLS Gateway. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.

Примечание. После ввода в командной строке любой команды или последовательности символов для их применения и выполнения необходимо нажимать клавишу **Enter**. В дальнейшем этот шаг подразумевается, но его описание будет опущено.

4 В строке **Password** введите технологический пароль `vipnet`. На экране процесс ввода пароля не отображается.

5 Чтобы установить и активировать лицензию в строке **Do you want to skip TLS Gateway license activation** введите `n`. Если вы хотите установить и активировать лицензию позднее с помощью веб-интерфейса, введите `y` и перейдите к шагу 9.

6 Выберите сетевой интерфейс, через который будет настроен доступ в Интернет для активации лицензии. Для этого подключите сетевой кабель к разъему одного из сетевых портов ViPNet TLS Gateway. На экране появится информация о включении соответствующего сетевого интерфейса с определенным номером (например, информация о включившемся сетевом интерфейсе eth1 будет выглядеть следующим образом: Interface eth1 is UP). Далее в строке **Select network interface for activate license** введите порядковый номер этого интерфейса.

Примечание. Для исполнения TLS VA просто укажите порядковый номер нужного сетевого интерфейса из предложенного нумерованного списка.

7 Произведите настройки этого сетевого интерфейса для доступа к Интернету одним из следующих способов:

- Чтобы получить IP-адрес от DHCP-сервера, в строке **Do you want to use static ip for network interface <название интерфейса>** введите `n` и далее выберите один из следующих способов получения IP-адресов DNS-серверов:
  - Для автоматического получения IP-адресов DNS-серверов в строке **Do you want to use dns servers from dhcp** введите `y`.
  - Для указания IP-адресов DNS-серверов вручную введите `n` и далее в строке **Enter a new DNS servers** введите IP-адреса DNS-серверов. При вводе нескольких значений адресов разделяйте их символом `;` без пробелов. Например, `10.10.10.01;10.10.10.11`. Далее проверьте правильность введенного IP-адреса и, если все верно, в строке **Do you want to select a new DNS servers** введите `n`.
- Если вы хотите задать постоянный IP-адрес интерфейса, в строке **Do you want to use static ip to network interface <название интерфейса>** введите `y` и произведите соответствующие настройки (см. Настройка постоянного IP-адреса сетевого интерфейса на стр. 44).

8 В строке **Enter full path to license file** введите полный путь к файлу с лицензией. Например, если файл с лицензией находится в файле `license.itcslic` в корне USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/license.itcslic`.

Примечание. При вводе путей к файлам соблюдайте регистр букв в названиях каталогов и файлов.

Также работает стандартное в Linux автодополнение команд с помощью нажатия клавиши **Tab**.

Все введенные в текущем сеансе работы консоли Linux команды запоминаются. При необходимости повторного ввода команд для выбора нужных команд из истории можно использовать клавиши со стрелками вверх и вниз.

Запустится процесс активации лицензии. После успешной активации появится соответствующее сообщение.

9 Запустится процесс расчета контрольных комбинаций ОС и ViPNet TLS Gateway. На экране появится информация о номере версии установленного ПО ViPNet TLS Gateway и значения контрольных комбинаций ОС и ViPNet TLS Gateway в строках **TLS Gateway OS checksum is** и **TLS Gateway software checksum is** соответственно. Проверьте, что контрольные комбинации совпадают с имеющимися у вас и нажмите клавишу **Enter** для продолжения.

10 Подтвердите завершение настроек. Для этого в строке **Do you want to complete the factory settings** введите `y`.

11 Откажитесь от выключения ViPNet TLS Gateway. Для этого в строке **Shutdown system** введите `n`.

В результате на ViPNet TLS Gateway будет установлена и активирована лицензия. Далее выполните подготовку к эксплуатации ViPNet TLS Gateway (см. Подготовка ViPNet TLS Gateway к эксплуатации на стр. 48).

3

Подготовка ViPNet TLS Gateway к эксплуатации

Последовательность действий 49

Требования к сертификатам для работы с ViPNet TLS Gateway 51

Первоначальная инициализация ViPNet TLS Gateway 54

Последовательность действий

Перед подготовкой ViPNet TLS Gateway к эксплуатации выполните следующие действия:

- Установите аппаратную платформу с ViPNet TLS Gateway или компьютер с развернутым виртуальным образом TLS VA в специальное помещение, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа в соответствии с требованиями безопасности вашей организации.
- Распределите сотрудникам вашей организации роли для управления ViPNet TLS Gateway (см. Разграничение полномочий на основе ролей на стр. 34).

Для подготовки к эксплуатации ViPNet TLS Gateway выполните все действия из приведенного ниже списка.

Таблица 12. Последовательность действий по подготовке ViPNet TLS Gateway к эксплуатации

	Действие	Ссылка
☐	На рабочем месте администратора безопасности создайте запрос на сертификат администратора с помощью программы ViPNet CSP, ViPNet PKI Client или стандартных средств криптопровайдеров сторонних производителей. Передайте его администратору удостоверяющего центра для издания сертификата	См. документ «ViPNet CSP. Руководство пользователя» См. документ «ViPNet PKI Client. Руководство администратора» См. документацию к соответствующим средствам Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway (на стр. 68) Требования к сертификатам для работы с ViPNet TLS Gateway (на стр. 51)
☐	На рабочем месте администратора безопасности установите полученный сертификат администратора, а также корневой сертификат удостоверяющего центра в системное хранилище с помощью программы ViPNet CSP, ViPNet PKI Client или стандартных средств операционной системы. Если сертификат удостоверяющего центра не является корневым, то должны быть загружены сертификаты всех УЦ, образующие цепочку доверия к сертификатам (см. глоссарий, стр. 211)	См. документ «ViPNet CSP. Руководство пользователя» См. документ «ViPNet PKI Client. Руководство администратора» См. документацию к соответствующим средствам
☐	На ViPNet TLS Gateway выполните первоначальную инициализацию	Первоначальная инициализация ViPNet TLS Gateway (на стр. 54)

	Действие	Ссылка
☐	На рабочем месте администратора безопасности настройте параметры веб-браузера для защищенного подключения по протоколу TLS и подключитесь к веб-интерфейсу ViPNet TLS Gateway	Настройка параметров веб-браузера для подключения по протоколу TLS (на стр. 69) Подключение к веб-интерфейсу и завершение работы с ним (на стр. 69)
☐	Организуйте защищенное подключение по протоколу TLS рабочего места сотрудника, которому назначены полномочия администратора доступа	Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway (на стр. 66)
☐	На рабочем месте администратора доступа подключитесь к веб-интерфейсу ViPNet TLS Gateway и установите лицензию с дополнительными функциями при ее наличии	Обновление и активация лицензии (см. Обновление лицензии на стр. 148)
☐	Настройте статические маршруты, если схема подключения ViPNet TLS Gateway в вашей сети предполагает такие настройки	Настройка статических маршрутов (на стр. 138)
☐	Организуйте доступ пользователей к защищаемым ресурсам вашей сети	Организация доступа пользователей к защищаемым ресурсам (на стр. 81)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Требования к сертификатам для работы с ViPNet TLS Gateway

Для взаимодействия администраторов и пользователей (при подключении по каналу TLS с двусторонней аутентификацией) с ViPNet TLS Gateway каждая сторона должна иметь сертификаты (администратора, пользователя, транспортные сертификаты соответственно) (см. Организация работы ViPNet TLS Gateway на стр. 25).

Сертификаты должны удовлетворять следующим требованиям:

- Сертификаты изданы в сертифицированном удостоверяющем центре (по требованиям к средствам УЦ по классу КС3, например, в ПО ViPNet Удостоверяющий центр).
- Формат сертификата: X.509.
- Назначение сертификата: подпись и шифрование.
- Алгоритм подписи:
  - Сертификаты администраторов и транспортные сертификаты для обеспечения доступа администраторов — ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.
  - Сертификаты пользователей и транспортные сертификаты для обеспечения доступа пользователей — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, RSA или ECDSA.
- Транспортные сертификаты ViPNet TLS Gateway должны иметь расширение «Расширенное использование ключа» с назначением ключа «Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)». Сертификаты администраторов и пользователей должны иметь расширение «Расширенное использование ключа» с назначением ключа «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)».
- Сертификат должен быть действительным:
  - Срок действия сертификата наступил и не истек.
  - Сертификат не находится в списке аннулированных сертификатов доверенного удостоверяющего центра (см. глоссарий, стр. 211).
  - Цепочка доверия к сертификату (см. глоссарий, стр. 211) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.
- Файл с сертификатом может иметь одно из следующих расширений: `*.cer`, `*.crt` или `*.pem`.
- Ограничения на максимальную длину строковых полей сертификатов представлены в таблице ниже.

Таблица 13. Ограничения на строковые поля сертификатов

Имя поля	Обозначение и описание	Ограничение
	Обязательные поля	
Subject.CN	Наименование (общее имя субъекта)	до 64 символов
Subject.O	Организация	до 1024 символов
Subject.SNILS	СНИЛС — для корневых сертификатов УЦ это поле не обязательное	11 цифр
Issuer.CN	Выпущен (общее имя издателя) — для корневых сертификатов УЦ это поле необязательное	до 64 символов
Valid from	Действителен с	дата
Valid to	Действителен до	дата
	Необязательные поля	
Subject.SN	Фамилия (фамилия уполномоченного лица, получающего сертификат). Может совпадать с Subject.CN	до 40 символов
Subject.GN	Имя и отчество (уполномоченного лица)	до 64 символов
Subject.T	Должность (уполномоченного лица)	до 64 символов
Subject.OU	Подразделение	до 64 символов
Subject.STREET	Улица (название улицы, номер дома)	до 30 символов
Subject.L	Город (населенный пункт)	до 128 символов
Subject.S	Код субъекта РФ (код и название субъекта федерации согласно классификатору КЛАДР)	до 128 символов
Subject.C	Страна (двухсимвольный код страны)	2 символа
Subject.E	Адрес электронной почты	до 255 символов
Subject.INN	ИНН	10-12 цифр
Subject.OGRN	ОГРН	13 цифр

Также на ViPNet TLS Gateway должны быть загружены корневые сертификаты УЦ (или цепочки доверия к сертификатам (см. глоссарий, стр. 211) УЦ) и соответствующие действительные CRL (см. глоссарий, стр. 211) УЦ, в которых изданы сертификаты администраторов, пользователей и транспортные сертификаты ViPNet TLS Gateway.

Суммарный размер всех файлов CRL, которые добавлены на ViPNet TLS Gateway, в зависимости от используемой аппаратной платформы не должен превышать следующих значений:

- Для TLS 500 — 12 Мб;
- Для TLS 1000 — 18 Мб;

- Для TLS 5000 — 22 Мб;
- Для TLS VA — 85 Мб (при настройках виртуальной машины, рекомендуемых для работы с TSL-файлом (см. Программная реализация TLS VA на стр. 16).

Первоначальная инициализация ViPNet TLS Gateway

Первоначальная инициализация производится уполномоченным сотрудником вашей организации, которому назначена роль администратора с правом локального доступа. Действия производятся в консоли Linux с помощью мастера инициализации.

Для проведения первоначальной инициализации вам потребуется USB-носитель, отформатированный в одну из следующих файловых систем: ext2, ext3, ext4 или FAT32. На него нужно будет записать полученные у администратора вашего удостоверяющего центра:

- транспортные сертификаты ViPNet TLS Gateway (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51);
- корневой сертификат УЦ и соответствующий CRL (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51);
- если транспортные сертификаты ViPNet TLS Gateway изданы не в корневом УЦ, сертификаты УЦ из цепочки доверия к сертификатам (см. глоссарий, стр. 211) и соответствующие CRL;
- сертификат администратора, которому будет назначена роль администратора безопасности ViPNet TLS Gateway.

Внимание! Убедитесь, что вы знаете, какому уровню иерархии издателей сертификатов из цепочки доверия принадлежат полученные сертификаты УЦ и соответствующие CRL. В процессе первоначальной инициализации загрузку этих сертификатов необходимо будет произвести строго в определенном порядке, начиная с корневого сертификата УЦ и соответствующего CRL и далее последовательно до последнего уровня иерархии цепочки доверия.

Примечание. USB-носитель должен быть предварительно отформатирован в одну из следующих файловых систем: ext2, ext3, ext4 или FAT32.

Информация о произведенных действиях фиксируется в журнале событий (см. Работа с журналом событий на стр. 127), который можно просмотреть по завершении инициализации, подключившись к веб-интерфейсу ViPNet TLS Gateway.

Для проведения первоначальной инициализации выполните действия из приведенной ниже таблицы в предложенном порядке.

Таблица 14. Порядок проведения первичной инициализации ViPNet TLS Gateway

	Действие	Ссылка
☐	Инициируйте процедуру первоначальной инициализации ViPNet TLS Gateway	Начало инициализации (на стр. 55)
☐	Укажите часовой пояс дату и время	Настройка часового пояса, даты и времени (на стр. 57)
☐	Создайте транспортные ключи ViPNet TLS Gateway	Создание транспортных ключей ViPNet TLS Gateway (на стр. 57)
☐	Если вы используете исполнение TLS 1000 и ваш файл лицензии разрешает использование модуля WAF, настройте модуль WAF	Настройка модуля WAF (на стр. 57)
☐	Задайте сетевые настройки ViPNet TLS Gateway	Настройка сетевых интерфейсов ViPNet TLS Gateway (на стр. 58)
☐	Задайте версии протокола TLS для подключения администраторов и пользователей к ViPNet TLS Gateway	Настройка версии протокола TLS для подключения к ViPNet TLS Gateway (на стр. 60)
☐	Задайте параметры и сформируйте запросы на транспортные сертификаты. Затем передайте файлы запросов в УЦ и дождитесь получения сертификатов	Получение транспортных сертификатов ViPNet TLS Gateway (на стр. 61)
☐	Установите корневой сертификат УЦ, сертификаты УЦ из цепочки доверия, CRL УЦ, транспортные сертификаты ViPNet TLS Gateway и сертификат администратора безопасности	Установка сертификатов и CRL ViPNet TLS Gateway (на стр. 62)
☐	Завершите первоначальную инициализацию ViPNet TLS Gateway	Завершение инициализации (на стр. 63)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Начало инициализации

Первоначальная инициализация производится в консоли Linux с помощью мастера инициализации, который запускается автоматически после авторизации на ViPNet TLS Gateway.

При работе с мастером инициализации используются следующие клавиши:

- **Tab** — стандартное в ОС Linux автодополнение команд.
- «стрелка вверх», «стрелка вниз» — выбор нужных команд из истории.

- **Enter** — необходимо нажимать после ввода любой команды или последовательности символов для их выполнения и применения. В дальнейшем этот шаг подразумевается, но его описание будет опущено.

Примечание. В случае перезагрузки ViPNet TLS Gateway в процессе первоначальной инициализации будет предложено пропустить каждый из ранее пройденных шагов. Если вы уверены, что настройки были заданы верно, в строке **Skip** для каждого ранее пройденного шага введите `y`. Шаг будет пропущен.

Чтобы запустить первоначальную инициализацию ViPNet TLS Gateway, выполните следующие действия:

1 Если вы проводите инициализацию аппаратного исполнения ViPNet TLS Gateway:

1.1 Подключите аппаратную платформу ViPNet TLS Gateway к электропитанию.

Внимание! На данном этапе не следует подключать сетевые кабели к сетевым портам ViPNet TLS Gateway. Подключите сетевые кабели в момент настройки сетевых интерфейсов (см. Настройка сетевых интерфейсов ViPNet TLS Gateway на стр. 58).

1.2 Подключите к аппаратной платформе монитор и клавиатуру.

2 Запустите ViPNet TLS Gateway и дождитесь завершения загрузки.

3 Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и в строке **Password** введите технологический пароль `vipnet`. На экране процесс ввода пароля не отображается.

4 Измените пароль учетной записи администратора с правом локального доступа. Для этого в строке **Enter new password** введите пароль и в строке **Repeat password** подтвердите пароль.

Длина пароля должна быть не менее 8 и не более 31 символа включительно.

В пароле должны использоваться символы только из следующих категорий:

- прописные и строчные буквы английского алфавита A-Z, a-z;
- цифры 0-9.

Внимание! Если вы забудете новый пароль, восстановить его будет невозможно. Чтобы продолжить работу с ViPNet TLS Gateway, вам нужно будет обратиться в ОАО «ИнфоТеКС».

---

5 Откажитесь от восстановления ViPNet TLS Gateway. Для этого в строке **Do you want to restore a TLS-Gateway backup** введите `n`. Запустится режим инициализации. Следуйте указаниям мастера.

Настройка часового пояса, даты и времени

Следующие шаги предназначены для настройки часового пояса, текущих даты и времени. Часовой пояс должен соответствовать географическому положению ViPNet TLS Gateway.

Чтобы настроить часовой пояс, дату и время ViPNet TLS Gateway, выполните следующие действия:

1. В строке выбора континента введите номер континента из представленного списка. Например, для выбора континента «Европа» введите `8`.
2. В строке выбора страны введите номер страны расположения ViPNet TLS Gateway из представленного списка. Например, для выбора страны «Россия» введите `39`.
3. В строке выбора часового пояса введите номер часового пояса расположения ViPNet TLS Gateway из представленного списка. Например, для выбора часового пояса «Москва» введите `2`.
4. Проверьте, что в строке **Local time is now** дата и время отображаются корректно, затем в строке подтверждения **Please enter Yes or No** введите `y`.
5. В случае необходимости в строке **Enter a new date** вы можете ввести другие дату и время в формате `Год-месяц-день часы:минуты:секунды`. Например, `2018-06-14 14:15:15`. Если изменять дату и время не требуется, нажмите клавишу **Enter**.

Создание транспортных ключей ViPNet TLS Gateway

Чтобы создать транспортные ключи ViPNet TLS Gateway, после появления на экране сообщения биометрического датчика случайных чисел (электронной рулетки) **Press different keys** нажимайте произвольные клавиши на клавиатуре для работы электронной рулетки до появления сообщения **Done**. Запустится процесс создания транспортных ключей ViPNet TLS Gateway. Процесс создания транспортных ключей зависит от исполнения ViPNet TLS Gateway и может занять продолжительное время. Обязательно дождитесь окончания процесса создания ключей, не прерывая его. Пока создаются ключи, не нажимайте никакие клавиши. После завершения создания ключей появится информация об этом.

Настройка модуля WAF

Если вы используете исполнение TLS 1000 и ваш файл лицензии разрешает использование модуля WAF, настройте модуль WAF. Для этого:

1. В строке **TLS Gateway is configured to work with PT AF. Do you want to setup WAF module** введите `y`.
2. Пропустите шаг с указанием пути к файлу с образом виртуальной машины с WAF. Для этого в строке **Skip** введите `y`.

3 Настройте внутренние диапазоны адресов модуля WAF. Чтобы оставить значения внутренних диапазонов адресов по умолчанию, в строке **Use default networks <диапазон адресов WAN и MGMT> for WAN and MGMT interfaces and <диапазон адресов LAN> for LAN interface during WAF configuration** введите `y`. Чтобы изменить значения, заданные по умолчанию, введите `n` и выполните следующие действия:

Внимание! Диапазон внутренних адресов модуля WAF не должен конфликтовать с IP-адресами внутренней (корпоративной) сети.

3.1 В строке **Enter network for WAN and MGMT interfaces (mask /24 will apply automatically)** введите IP-адрес для задания внутреннего диапазона адресов интерфейса для внешних подключений и интерфейса управления. Маска подсети задается автоматически — 24, изменить ее нельзя.

3.2 В строке **Enter network for LAN interface (mask /24 will apply automatically)** введите IP-адрес для задания внутреннего диапазона адресов интерфейса для подключения по локальной сети. Маска подсети задается автоматически — 24, изменить ее нельзя.

4 Пропустите шаг с получением отпечатка файла лицензии модуля WAF.

5 Пропустите шаг с установкой лицензии на модуль WAF.

6 Откажитесь от перехода к консоли модуля WAF. Для этого в строке **Connect to WAF console for debug and WAF update load** введите `n`.

7 Для включения модуля WAF в строке **Do you want to enable WAF** введите `y`.

Настройка сетевых интерфейсов ViPNet TLS Gateway

Следующие шаги предназначены для настройки подключения к ViPNet TLS Gateway (подключения к ViPNet TLS Gateway администраторов, пользователей по TLS-каналу с двусторонней аутентификацией, пользователей по TLS-каналу с односторонней аутентификацией и подключения ViPNet TLS Gateway к защищаемым ресурсам для осуществления функций прокси-сервера).

Для разных типов подключения вы можете настроить как разные сетевые интерфейсы, так и один. При настройке разных сетевых интерфейсов укажите уникальные IP-адреса для каждого интерфейса. В случае использования одного сетевого интерфейса для разных типов подключения необходимо указать уникальные номера портов. Вы можете использовать любые номера портов кроме значений из диапазона 40000-50000, поскольку они зарезервированы для работы ViPNet TLS Gateway в режиме перенаправления запросов от пользователей к ресурсу с использованием выделенного порта.

Чтобы настроить сетевые параметры, выполните следующие действия:

1 Укажите номер порта подключения администраторов к ViPNet TLS Gateway по протоколу TLS для выполнения функций управления. Для этого в строке **Type the port for Administration web**

interface введите номер порта или оставьте значение по умолчанию (443), указанное в скобках, просто нажав клавишу **Enter**.

2 Выберите сетевой интерфейс, который будет выполнять функции интерфейса для подключения администраторов. После появления строки **Choose network interface for Administration web interface** и нумерованного списка всех существующих сетевых интерфейсов ViPNet TLS Gateway определите номер сетевого интерфейса, который будет использоваться для подключения к ViPNet TLS Gateway администраторов. Для этого подключите сетевой кабель к разъему сетевого порта ViPNet TLS Gateway, который будет использоваться для настраиваемого типа подключения, и посмотрите информацию о номере включившегося сетевого интерфейса (например, информация о включившемся сетевом интерфейсе eth1 будет выглядеть следующим образом: Interface eth1 is UP). Порядковый номер именно этого интерфейса укажите в строке **Choose network interface for Administration web interface**.

Примечание. Для исполнения TLS VA здесь и ниже на аналогичных шагах просто укажите порядковый номер нужного сетевого интерфейса из предложенного нумерованного списка.

---

3 Укажите номер порта подключения пользователей к ViPNet TLS Gateway по TLS-каналу с двусторонней аутентификацией. Для этого в строке **Type the port for two-way TLS web interface** введите номер порта или оставьте значение по умолчанию (443).

4 Выберите сетевой интерфейс, который будет выполнять функции интерфейса подключения пользователей к ViPNet TLS Gateway по TLS-каналу с двусторонней аутентификацией. Если вы хотите указать ранее выбранный сетевой интерфейс, в строке **Choose network interface for two-way TLS web interface** введите порядковый номер нужного интерфейса. Если вы хотите выбрать сетевой интерфейс, отличный от ранее выбранного интерфейса, подключите сетевой кабель и введите определившийся номер интерфейса.

5 Укажите номер порта подключения пользователей к ViPNet TLS Gateway по TLS-каналу с односторонней аутентификацией. Для этого в строке **Type the port for one-way TLS web interface** введите номер порта или оставьте значение по умолчанию (443), указанное в скобках.

6 Выберите сетевой интерфейс, который будет выполнять функции интерфейса подключения пользователей к ViPNet TLS Gateway по TLS-каналу с односторонней аутентификацией по аналогии с предыдущим шагом. В строке **Choose network interface for one-way TLS web interface** введите порядковый номер нужного интерфейса.

7 Аналогичным способом выберите сетевой интерфейс, который будет выполнять функции интерфейса подключения ViPNet TLS Gateway к защищаемым ресурсам для осуществления функций прокси-сервера. В строке **Select network interface for access to proxied resources** введите порядковый номер нужного интерфейса.

8 В следующих последовательно появляющихся строках введите IP-адреса и маски тех сетевых интерфейсов ViPNet TLS Gateway, которые вы выбрали на предыдущих шагах. Для этого в строках **Enter ip address** и **Enter netmask**, для каждого сетевого интерфейса, введите его IP-адрес (например, `10.10.10.10`) и маску сети (например, `255.255.255.0`). Чтобы оставить значение маски по умолчанию (255.255.255.0), указанное в скобках, нажмите клавишу **Enter**.

Внимание! IP-адрес и маска сети будут запрошены только для тех сетевых интерфейсов, которые на предыдущих шагах были выбраны вами в качестве интерфейсов подключения разных типов (**Administration web interface**, **two-way TLS web interface**, **one-way TLS web interface** и **Interface for access to proxied resources**).

9 В строке **Enter a default gateway** введите IP-адрес шлюза по умолчанию.

10 В строке **Enter a new DNS servers** введите IP-адреса DNS-серверов или оставьте значение по умолчанию, указанное в скобках, нажав клавишу **Enter**. При вводе нескольких значений адресов разделяйте их символом `;` без пробелов. Например, `10.10.10.01;10.10.10.11`.

Примечание. Модуль WAF будет работать только с первыми тремя DNS-серверами из этого списка.

11 Проверьте правильность введенного IP-адреса и в строке **Do you want to select a new DNS servers** введите `n`.

12 Если сетевые настройки заданы правильно, появится сообщение об успешном конфигурировании сети (Network settings configured).

Настройка версии протокола TLS для подключения к ViPNet TLS Gateway

Следующие шаги предназначены для настройки версии протокола TLS для подключения к ViPNet TLS Gateway (подключения к ViPNet TLS Gateway администраторов, пользователей по TLS-каналу с двусторонней аутентификацией, пользователей по TLS-каналу с односторонней аутентификацией).

Для всех типов подключения вы можете настроить как разные версии протокола TLS, так и одинаковые. После первоначальной инициализации вы сможете изменить эти настройки через веб-интерфейс (см. разделы Изменение версии протокола TLS для подключения администраторов (на стр. 79) и Изменение версии протокола TLS для подключения пользователей (на стр. 124)).

Чтобы настроить версии протокола TLS, введите его порядковый номер или номера, разделенные запятой без пробела, в следующих строках:

1 **Enter the TLS protocols version number separated by commas for admin access** — для подключения администраторов.

2 **Enter the TLS protocols version number separated by commas for users twoside access** — для подключения пользователей с двусторонней аутентификацией.

3 **Enter the TLS protocols version number separated by commas for users oneside access** — для подключения пользователей с односторонней аутентификацией.

Получение транспортных сертификатов ViPNet TLS Gateway

Чтобы задать параметры и получить транспортные сертификаты ViPNet TLS Gateway, выполните следующие действия:

1 Для каждого сетевого интерфейса в строках **Enter alternative IP addresses or/and domain names for network interface <название интерфейса> with ip address <IP-адрес интерфейса>** введите дополнительные IP-адреса или DNS-имена сетевого интерфейса или пропустите этот шаг, просто нажав клавишу **Enter**. При вводе нескольких значений разделяйте их символом `;` без пробелов. Например, `dnsname1.com;dnsname2.com`.

2 Укажите, какой алгоритм использовать для формирования запроса на транспортный сертификат. Например, для использования ГОСТ Р 34.10-2012 с длиной ключа 256 бит введите `2`.

3 Задайте назначения, для которых будет использоваться сертификат (подключение к ViPNet TLS Gateway администраторов, пользователей по TLS-каналу с односторонней аутентификацией, пользователей по TLS-каналу с двусторонней аутентификацией). Вы можете выбрать как одно, так и несколько назначений. При вводе нескольких значений разделяйте их запятой без пробела.

Примечание. Для подключения к ViPNet TLS Gateway администраторов могут использоваться только сертификаты, сформированные по алгоритмам ГОСТ.

---

4 Если вы хотите использовать сертификат для подключения к защищаемым ресурсам непосредственно по их адресам, в строке **Enter alternative IP addresses or/and domain names for certificate request or press 'enter' to skip** введите эти адреса или пропустите этот шаг, нажав клавишу **Enter**. При вводе нескольких значений разделяйте их символом `;` без пробелов.

5 Подключите USB-носитель и в строке **Enter folder to save requests for transport certificates** введите полный путь к каталогу для сохранения файлов с запросами. Например, вы можете сохранить запросы на транспортные сертификаты в корень USB-носителя, для этого укажите каталог автоматического монтирования USB-носителя: `/media/usb0/`.

Примечание. При вводе путей к файлам соблюдайте регистр букв в названиях каталогов и файлов.

В результате на USB-носитель в указанную выше папку будет сохранен файл запроса со следующим именем:

```
cert_req_<алгоритм шифрования>_<длина ключа>_<назначение сертификата
1>...<назначение сертификата n>
```

6 Если вы хотите создать еще один запрос на транспортный сертификат, например с использованием другого алгоритма шифрования, в строке **Step "Create certificate request" was already completed. Skip (Yes/No)** введите `n` и повторите шаги 2-5.

7 Отключите USB-носитель и передайте файлы с запросами администратору удостоверяющего центра для издания транспортных сертификатов.

8 Получите у администратора изданные сертификаты, а также корневой сертификат УЦ или сертификаты всех УЦ из цепочки доверия к сертификатам (см. глоссарий, стр. 211) и соответствующие CRL. Запишите их на USB-носитель. На этот же USB-носитель запишите сертификат администратора безопасности. Ключ электронной подписи и соответствующий сертификат администратора безопасности должен быть сформирован по алгоритмам ГОСТ.

Примечание. Если процедура издания сертификата займет длительное время, вы можете выключить аппаратную платформу (или виртуальную машину). После получения транспортных сертификатов запустите ViPNet TLS Gateway, введите пароль, выберите режим инициализации и далее пропустите все ранее пройденные шаги.

Установка сертификатов и CRL ViPNet TLS Gateway

Чтобы установить сертификаты и CRL, необходимые для работы ViPNet TLS Gateway, выполните следующие действия:

1 Подключите USB-носитель с записанными сертификатами к аппаратной платформе (или компьютеру с виртуальной машиной).

Внимание! На следующих шагах загрузите переданные вам сертификаты УЦ и CRL, начиная с корневого сертификата УЦ и далее последовательно все сертификаты и CRL в соответствии с иерархией УЦ. При попытке загрузить сертификаты УЦ в другой последовательности, будет появляться сообщение об ошибке. В этом случае еще раз загрузите сертификаты в нужной последовательности.

Если сертификат УЦ, в котором были изданы транспортные сертификаты ViPNet TLS Gateway, является корневым, то загрузите только корневой сертификат и соответствующий CRL.

2 Загрузите корневой сертификат УЦ. Для этого в строке **Enter full path for CA root certificate** введите полный путь к файлу с корневым сертификатом УЦ. Например, если файл с корневым сертификатом УЦ находится в файле `CARootCert.pem` в корне USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/CARootCert.pem`.

3 Загрузите CRL из того же УЦ, что и загруженный на предыдущем шаге корневой сертификат. Для этого в строке **Enter full path for CRL** введите полный путь к файлу с CRL. Например, если файл с CRL находится в файле `CARootCRL.crl` в корне USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/CARootCRL.crl`.

Внимание! Размер файла CRL не должен превышать значений, указанных в разделе Требования к сертификатам для работы с ViPNet TLS Gateway (на стр. 51).

4 Для загрузки следующего сертификата УЦ из цепочки доверия к сертификатам и соответствующего CRL:

   4.1 В строке **Do you want to install other CA certificate or/and CRL** введите `y`.

   4.2 На шаге "Load root certificate" в строке **Skip** введите `n` и укажите путь к файлу с сертификатом УЦ.

   4.3 На шаге "Load CRL" в строке **Skip** введите `n` и укажите путь к файлу с CRL.

   Повторите шаги 4.1-4.3 столько раз, сколько сертификатов УЦ (CRL) вам необходимо загрузить.

   4.4 После загрузки последних сертификатов цепочки или если у вас нет цепочек доверия к сертификатам, в строке **Do you want to install other CA certificate or/and CRL** введите `n`.

5 Загрузите транспортные сертификаты. Для этого в строке **Enter full path to transport certificate** введите полный путь к файлу сертификата. Например, если файл сертификата находится в файле `CARootCert.pem` в корне USB-носителя, укажите: `/media/usb0/CARootCert.pem`.

6 При необходимости измените назначения загруженного транспортного сертификата, для этого в строке **Do you want to change certificate purposes** введите `y` и задайте нужные назначения (см. Получение транспортных сертификатов ViPNet TLS Gateway на стр. 61).

   После успешной установки транспортного сертификата появится соответствующее сообщение.

7 Если вы хотите загрузить еще один транспортный сертификат, например для обеспечения другого типа доступа, в строке **Step "Install transport certificates" was already completed. Skip (Yes/No)** введите n и повторите шаги 5-6.

8 Загрузите сертификат администратора безопасности. Для этого в строке **Enter full path for Security administrator certificate** введите полный путь к файлу с сертификатом администратора безопасности. Например, `/media/usb0/SecAdmin.pem`.

   После успешной загрузки сертификата администратора безопасности появится соответствующее сообщение.

Завершение инициализации

Для завершения инициализации выполните следующие действия:

1 В строке **Do you want to finish the TLS-Gateway initialization** введите `y`. Появится сообщение о завершении настроек.

2 Для продолжения нажмите клавишу **Enter**. ViPNet TLS Gateway будет перезагружен.

3 Отсоедините USB-носитель.

Процедура первоначальной инициализации завершена.

Внимание! После проведения первоначальной инициализации рекомендуется настроить автоматическое обновление CRL из точек распространения (см. Настройка адресов точек распространения CRL на стр. 97). При истечении срока действия CRL доступ администраторов к веб-интерфейсу ViPNet TLS Gateway и пользователей к защищаемым

ресурсам будет невозможен. Для обновления CRL потребуется провести повторную инициализацию ViPNet TLS Gateway (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).

4

Организация работы администраторов ViPNet TLS Gateway

Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway 66

Управление доступом администраторов к веб-интерфейсу 76

Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway

Чтобы администраторы, которым назначены роли управления ViPNet TLS Gateway с помощью веб-интерфейса (см. Разграничение полномочий на основе ролей на стр. 34), могли управлять ресурсами и правами доступа пользователей к ресурсам, необходимо обеспечить их подключение к веб-интерфейсу ViPNet TLS Gateway. Подключение администраторов к веб-интерфейсу ViPNet TLS Gateway осуществляется по каналу, защищенному протоколом TLS с прохождением двусторонней аутентификации. В результате канал подключения к веб-интерфейсу будет защищен от перехвата и подмены информации.

Примечание. Настройка защищенного подключения к веб-интерфейсу ViPNet TLS Gateway для первого администратора безопасности производится при вводе ViPNet TLS Gateway в эксплуатацию, поскольку при первоначальной инициализации ViPNet TLS Gateway необходим сертификат администратора безопасности (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). Остальные администраторы могут быть добавлены позднее по мере необходимости.

Для организации защищенного подключения администратора по протоколу TLS на рабочем месте администратора должны использоваться ключи электронной подписи и соответствующий им сертификат администратора (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51). Сертификат следует получить у администратора вашего удостоверяющего центра (если он развернут в вашей организации) либо в стороннем удостоверяющем центре и установить в системное хранилище (см. Последовательность действий на стр. 66).

Последовательность действий

Чтобы для нового администратора организовать защищенное подключение по протоколу TLS с двусторонней аутентификацией, выполните все действия из приведенного ниже списка:

Таблица 15. Порядок организации защищенного подключения к веб интерфейсу ViPNet TLS Gateway

	Действие	Ссылка
☐	На рабочем месте подключаемого администратора создайте запрос на сертификат администратора с помощью программы ViPNet CSP, ViPNet PKI Client или стандартных средств криптопровайдеров сторонних производителей. Передайте его администратору удостоверяющего центра для издания сертификата	См. документ «ViPNet CSP. Руководство пользователя» главу "Получение сертификата и закрытого ключа" См. документ «ViPNet PKI Client. Руководство администратора» См. документацию к соответствующим средствам Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway (на стр. 68) Требования к сертификатам для работы с ViPNet TLS Gateway (на стр. 51)
☐	На рабочем месте подключаемого администратора установите полученный сертификат администратора, а также корневой сертификат удостоверяющего центра в системное хранилище с помощью программы ViPNet CSP, ViPNet PKI Client или стандартных средств операционной системы. Если сертификат удостоверяющего центра не является корневым, то должны быть загружены сертификаты всех УЦ, образующие цепочку доверия к сертификатам (см. глоссарий, стр. 211)	См. документ «ViPNet CSP. Руководство пользователя» главу "Установка контейнеров ключей и сертификатов" См. документ «ViPNet PKI Client. Руководство администратора» См. документацию к соответствующим средствам
☐	Передайте сертификат администратору безопасности ViPNet TLS Gateway для его добавления на ViPNet TLS Gateway и назначения необходимых ролей	
☐	На рабочем месте подключаемого администратора настройте параметры веб-браузера для защищенного подключения по протоколу TLS	Настройка параметров веб-браузера для подключения по протоколу TLS (на стр. 69)
☐	С рабочего места администратора безопасности подключитесь к веб-интерфейсу ViPNet TLS Gateway с соответствующими правами, добавьте сертификат подключаемого администратора и назначьте ему необходимую роль администрирования	Добавление нового администратора (на стр. 76)
☐	С рабочего места подключаемого администратора подключитесь к веб-интерфейсу ViPNet TLS Gateway с помощью установленного сертификата администратора	Подключение к веб-интерфейсу и завершение работы с ним (на стр. 69)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway

Для подключения к веб-интерфейсу ViPNet TLS Gateway по защищенному каналу на компьютере администратора должно быть установлено следующее программное обеспечение:

- Операционная система — Windows 7 SP1 (32/64-разрядная), Windows Server 2008 R2 SP1 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

  Для операционной системы рекомендуется установить последний пакет обновлений.
- Криптопровайдер:
  - ViPNet CSP:
    - Для ОС Windows 10 — версии 4.2 (8.51670) и выше.
    - Для остальных ОС Windows — версии 4.2.2 и выше.
  - ViPNet PKI Client версии 1.1 и выше.
  - Криптопровайдер сторонних производителей.
- Веб-браузер:
  - При использовании совместно с ViPNet CSP — Internet Explorer 11.
  - При использовании совместно с ViPNet PKI Client — Internet Explorer 11, а также Edge, Google Chrome, Mozilla Firefox, «Спутник» последних версий.

Примечание. Для корректного отображения страниц веб-интерфейса установите разрешение экрана не менее 1280x800.

Настройка параметров веб-браузера для подключения по протоколу TLS

Чтобы произвести настройки веб-браузера для защищенного подключения по протоколу TLS к веб-интерфейсу ViPNet TLS Gateway, на компьютере администратора выполните следующие действия:

1. Откройте веб-браузер Microsoft Internet Explorer и в меню **Сервис** выберите пункт **Свойства браузера**.
2. В открывшемся окне перейдите на вкладку **Дополнительно** и проверьте, что установлен флажок **Использовать TLS 1.2**, разрешающий соединения по TLS-протоколу версии 1.2.
3. Перейдите на вкладку **Безопасность** и убедитесь, что снят флажок **Включить защищенный режим**.
4. Нажмите кнопку **OK**.

Также для корректной работы с веб-интерфейсом ViPNet TLS Gateway в свойствах браузера необходимо разрешить использование Cookies.

В результате будут настроены параметры для установления защищенного соединения с веб-интерфейсом ViPNet TLS Gateway. Подключитесь к веб-интерфейсу (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69).

Начало работы с веб-интерфейсом

С помощью веб-интерфейса ViPNet TLS Gateway вы можете выполнять основные действия по настройке ViPNet TLS Gateway и управлению доступом пользователей к корпоративным ресурсам в соответствии с вашей ролью (см. Разграничение полномочий на основе ролей на стр. 34).

Для начала работы с веб-интерфейсом ViPNet TLS Gateway для вас должно быть организовано защищенное подключение к ViPNet TLS Gateway по протоколу TLS (см. Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway на стр. 66).

Подключение к веб-интерфейсу и завершение работы с ним

Для подключения к веб-интерфейсу по протоколу TLS выполните следующие действия:

1. Откройте веб-браузер Internet Explorer и в адресной строке введите:

   `https://<адрес сетевого интерфейса администрирования ViPNet TLS Gateway:порт>.`

Внимание! Если при первоначальной инициализации ViPNet TLS Gateway значение порта не изменялось (оставлено значение по умолчанию `443`), в адресной строке можно не указывать значение порта и ввести только следующую строку: `https://<адрес сетевого интерфейса администрирования>`.

2 В появившемся окне со списком сертификатов выберите свой сертификат, который вы установили в системное хранилище ОС Windows (см. Настройка защищенного подключения администраторов к веб-интерфейсу ViPNet TLS Gateway на стр. 66).

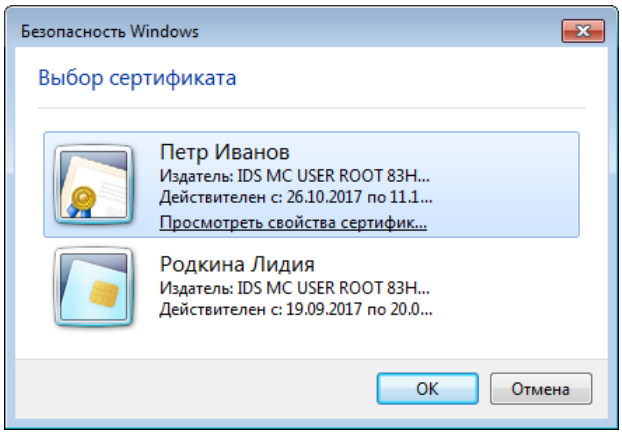

Рисунок 8. Выбор сертификата администратора в веб-браузере Internet Explorer

После успешной двусторонней аутентификации будет установлено защищенное соединение по протоколу TLS. Откроется страница веб-интерфейса ViPNet TLS Gateway (см. Веб-интерфейс ViPNet TLS Gateway на стр. 70), где будут доступны действия в соответствии с вашей ролью (см. Разграничение полномочий на основе ролей на стр. 34).

Чтобы завершить работу с веб-интерфейсом под текущей учетной записью администратора, в верхнем правом углу окна веб-интерфейса щелкните меню с вашим именем и выберите пункт **Отключиться от ViPNet TLS Gateway**. В результате сессия текущего администратора будет безопасно завершена. Чтобы повторно подключиться к веб-интерфейсу под администратором, нажмите на отображаемую на экране одноименную кнопку.

Внимание! Если администратору требуется подключиться к веб-интерфейсу в качестве пользователя (см. Управление доступом пользователей к ресурсам на стр. 100), необходимо сначала завершить работу с веб-интерфейсом под учетной записью администратора, а затем заново подключиться к веб-интерфейсу уже в качестве пользователя (в соответствии с документацией ViPNet TLS Gateway. Руководство пользователя).

Веб-интерфейс ViPNet TLS Gateway

Внешний вид веб-интерфейса ViPNet TLS Gateway рассмотрим на примере раздела **Сертификаты удостоверяющих центров**, представленного на рисунке ниже:

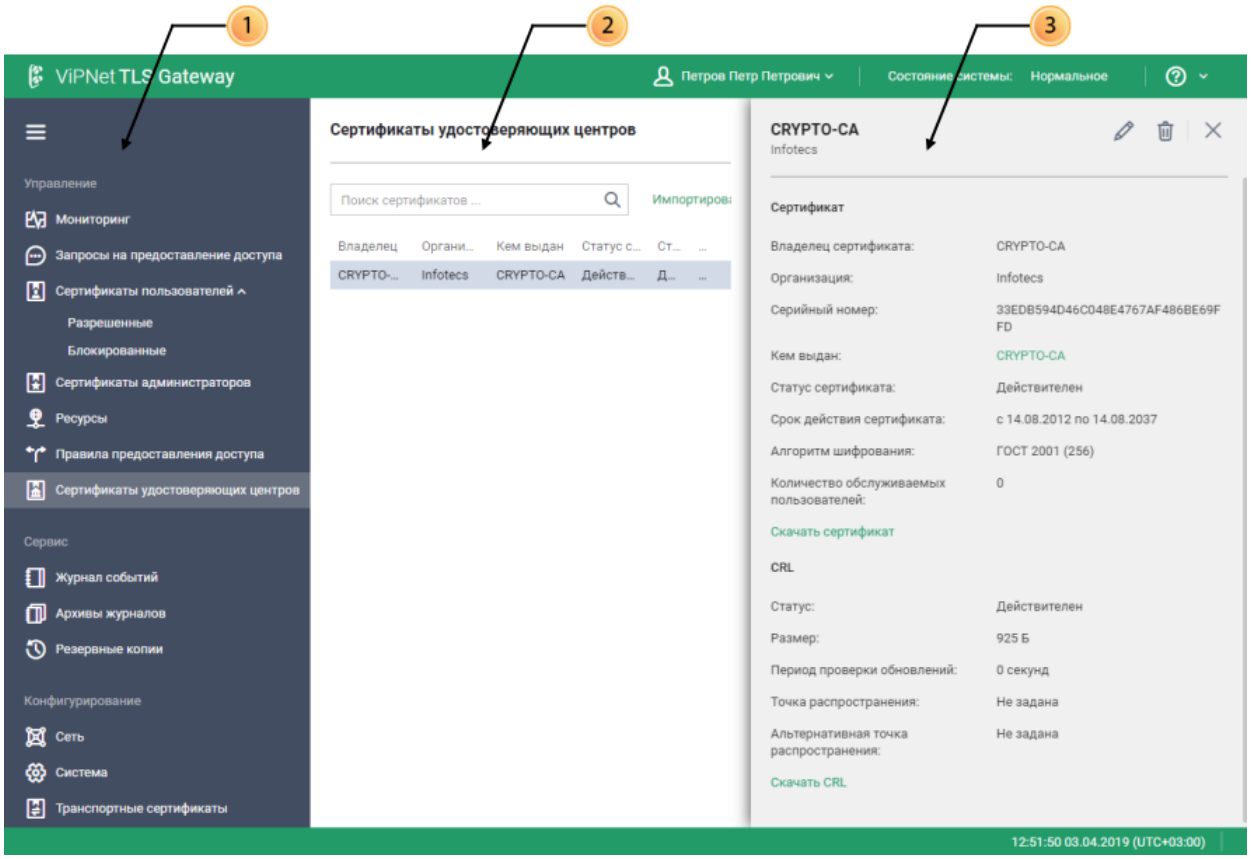

Рисунок 9. Веб-интерфейс ViPNet TLS Gateway

Цифрами на рисунке обозначены:

1 Панель навигации — содержит набор разделов для управления ViPNet TLS Gateway и просмотра результатов работы:

- **Мониторинг** — предназначен для просмотра отчетов мониторинга (см. Просмотр отчетов мониторинга на стр. 131). Раздел отображается в качестве стартовой страницы. Для исполнения TLS 1000 с модулем WAF отсюда же осуществляется переход в интерфейс WAF (подробнее о модуле WAF см. документ «ViPNet TLS Gateway Web Application Firewall. Руководство администратора»).
- **Запросы на предоставление доступа** — предназначен для обработки запросов от пользователей на получение доступа к защищаемым ресурсам (см. Назначение прав доступа к ресурсам по запросу пользователя на стр. 105).
- **Сертификаты пользователей** — содержит следующие подразделы:
  - **Разрешенные** — предназначен для добавления сертификатов пользователей на ViPNet TLS Gateway с целью разрешения доступа к необходимым защищаемым ресурсам, а также для просмотра и редактирования прав доступа пользователей к ресурсам (см. Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя на стр. 102).
  - **Блокированные** — предназначен для добавления сертификатов пользователей на ViPNet TLS Gateway с целью блокирования доступа ко всем защищаемым ресурсам и

к ViPNet TLS Gateway (см. Блокирование доступа нового пользователя к ViPNet TLS Gateway и ко всем ресурсам на стр. 104).

- **Сертификаты администраторов** — предназначен для управления доступом администраторов к веб-интерфейсу (см. Управление доступом администраторов к веб-интерфейсу на стр. 76).
- **Ресурсы** — предназначен для управления параметрами защищаемых ресурсов (см. Управление параметрами доступа к ресурсам на стр. 83).
- **Правила предоставления доступа** — предназначен для управления правилами автоматического назначения прав доступа к ресурсам (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109).
- **Сертификаты удостоверяющих центров** — предназначен для управления сертификатами доверенных удостоверяющих центров (см. Управление сертификатами доверенных удостоверяющих центров на стр. 92).
- **Журнал событий** — предназначен для просмотра журнала событий, где регистрируются все действия, производимые администраторами в ViPNet TLS Gateway (см. Просмотр журнала событий на стр. 127).
- **Архивы журналов** — предназначен для выгрузки архивов журналов событий в файл (см. Выгрузка архива журнала событий в файл на стр. 128).
- **Резервные копии** — предназначен для создания и сохранения резервных копий системы (см. Создание резервной копии данных на стр. 162).
- **Сеть** — предназначен для следующих настроек:
  - настройка сетевых интерфейсов ViPNet TLS Gateway (см. Сетевые настройки на стр. 136);
  - настройка статических маршрутов (на стр. 138);
  - диагностика сетевого окружения (на стр. 139).
- **Система** — предназначен для выполнения следующих действий:
  - обновление ПО ViPNet TLS Gateway (на стр. 149);
  - подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway (на стр. 133);
  - запуск процедуры самотестирования (см. Самотестирование на стр. 133);
  - настройка передачи данных в сторонние системы управления событиями информационной безопасности (SIEM) (см. глоссарий, стр. 210) в формате CEF (см. Настройка передачи данных в формате CEF на стр. 132);
  - настройка шаблона отображения пользователю страницы доступа к ресурсам (на стр. 89);
  - включение и выключение защиты веб-ресурсов от атак (на стр. 135);
  - настройка взаимодействия с Active Directory (на стр. 109);
  - изменение версии протокола TLS для подключения администраторов (на стр. 79);

- изменение версии протокола TLS для подключения пользователей (на стр. 124);
- настройка даты и времени (на стр. 147);
- тонкая настройка параметров подключения пользователей к защищаемым ресурсам (см. Дополнительные настройки параметров подключения к ViPNet TLS Gateway на стр. 151).

○ **Транспортные сертификаты** — предназначен для выполнения следующих действий:

- создание запроса на транспортный сертификат (на стр. 142);
- загрузка транспортного сертификата (на стр. 143);
- изменение назначений транспортного сертификата (на стр. 144);
- импорт ключа электронной подписи и сертификата из файла PFX (на стр. 145);
- просмотр данных о транспортных сертификатах (на стр. 146).

2 Панель просмотра — страница отображает содержимое раздела, выбранного на панели навигации или в настройках параметров работы ViPNet TLS Gateway (1).

3 Панель дополнительных сведений — страница отображает дополнительные сведения об элементе, выбранном на панели просмотра.

Установка, обновление и активация лицензии через веб-интерфейс

Чтобы установить или обновить и активировать лицензию ViPNet TLS Gateway с помощью веб-интерфейса, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с правами администратора доступа.

2 В верхнем правом углу окна веб-интерфейса в меню **Справка** выберите пункт **О программе**.

3 В появившемся окне информации о программе нажмите кнопку **Установить лицензию** или **Обновить лицензию** и выберите файл с лицензией (`*.itcslic`).

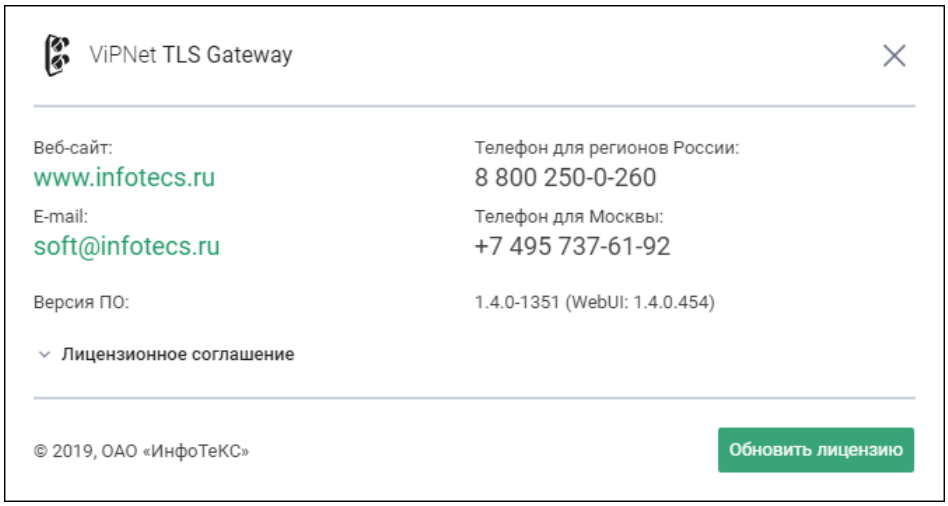

Рисунок 10. Установка лицензии через веб-интерфейс

4 В появившемся окне **Загружена лицензия ViPNet TLS Gateway** проверьте параметры устанавливаемой лицензии и нажмите кнопку **Установить**.

5 Если ViPNet TLS Gateway имеет доступ в Интернет, в списке **Активировать лицензию** выберите пункт **Через Интернет (онлайн)**. Лицензия будет активирована автоматически.

6 Если ViPNet TLS Gateway не имеет доступа в Интернет, в списке **Активировать лицензию** выберите пункт **По электронной почте** и в открывшемся окне выполните следующие действия:

- Если у вас установлен почтовый клиент, щелкните ссылку `reg@infotecs.biz`. Откроется окно вашего почтового клиента с уже сформированным письмом. Отправьте его в ОАО «ИнфоТеКС».
- Если у вас не установлен почтовый клиент, сохраните файл запроса и создайте письмо самостоятельно. Скопируйте в письмо содержимое файла запроса и отправьте на электронную почту `reg@infotecs.biz`. Тема письма может быть любой.

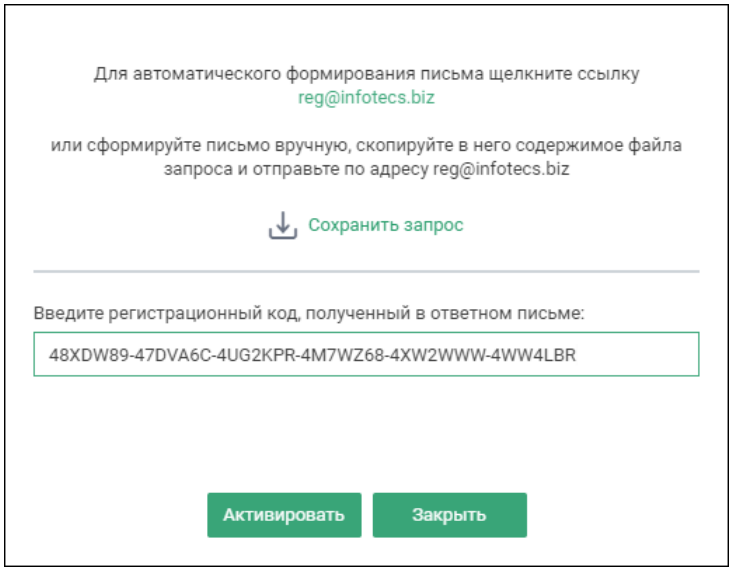

Рисунок 11. Активация лицензии по электронной почте

7 Дождитесь получения ответного письма, в котором будут указаны данные для активации.

8 Введите полученный регистрационный код и нажмите кнопку **Активировать**.

В результате будет установлена или обновлена и активирована лицензия ViPNet TLS Gateway. На экране появится соответствующее сообщение.

Информация о результатах активации лицензии фиксируется в журнале событий (см. Просмотр журнала событий на стр. 127).

Управление доступом администраторов к веб-интерфейсу

Чтобы администратор мог начать управление ресурсами и правами доступа пользователей к ресурсам, необходимо при подключении к веб-интерфейсу ViPNet TLS Gateway пройти двустороннюю аутентификацию с помощью сертификата. Для этого сертификат администратора должен быть добавлен на ViPNet TLS Gateway и этому сертификату добавлена необходимая роль управления.

Сертификат первого администратора безопасности добавляется на ViPNet TLS Gateway при его вводе в эксплуатацию (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). Сертификаты остальных администраторов необходимо добавить с помощью веб-интерфейса ViPNet TLS Gateway (см. Добавление нового администратора на стр. 76).

Добавление нового администратора

Перед добавлением администратора вам должен быть передан файл с сертификатом этого администратора (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51). Добавление нового администратора на ViPNet TLS Gateway заключается в загрузке его сертификата с помощью веб-интерфейса ViPNet TLS Gateway и назначении администратору роли управления.

Для добавления нового администратора на ViPNet TLS Gateway выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Сертификаты администраторов**.
3. На панели инструментов страницы **Сертификаты администраторов** нажмите кнопку **Добавить сертификат**.
4. В мастере добавления сертификата администратора на первой странице выберите файл с сертификатом и нажмите кнопку **Далее**.
5. На второй странице мастера выполните следующие действия:
   - **5.1** Проверьте данные об администраторе и его сертификате (данные подставляются из сертификата). Сертификат должен быть действительным.
   - **5.2** Укажите одну или несколько ролей для управления ViPNet TLS Gateway (см. Разграничение полномочий на основе ролей на стр. 34). Для этого в разделе **Полномочия администратора** установите флажки напротив необходимых ролей администратора.

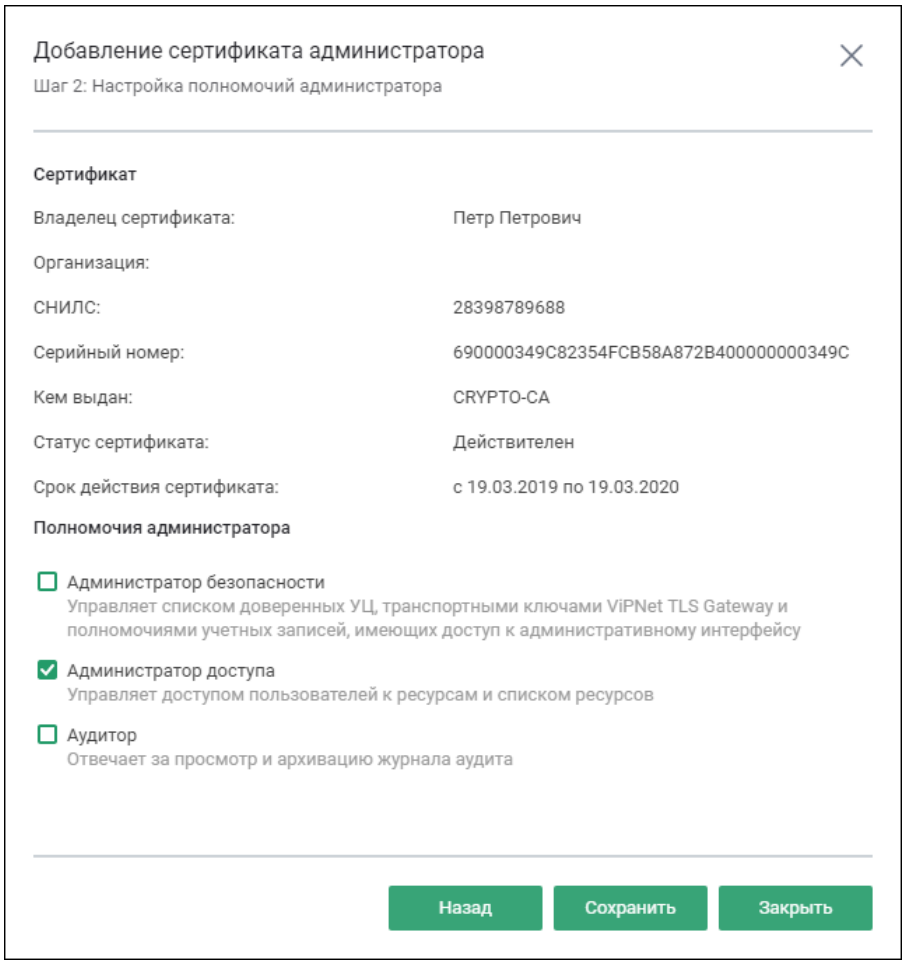

Рисунок 12. Назначение ролей администратору

6 Нажмите кнопку **Сохранить**.

В результате сертификат администратора будет добавлен на ViPNet TLS Gateway и для администратора будут заданы роли. Сертификат отобразится в списке на странице **Сертификаты администраторов**.

Новый администратор после выполнения необходимых настроек на своем рабочем месте (см. Последовательность действий на стр. 66) может подключиться к веб-интерфейсу ViPNet TLS Gateway для управления.

Просмотр данных об администраторах и их сертификатах

Вы можете просматривать данные о сертификатах администраторов, добавленных на ViPNet TLS Gateway, например, чтобы проверить сроки действия сертификатов. Для просмотра данных об администраторах, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора.

2 Перейдите в раздел **Сертификаты администраторов**.

3 На странице **Сертификаты администраторов** выберите нужный сертификат, на панели дополнительных сведений об администраторе отобразится краткая информация о сертификате администратора и заданных ролях.

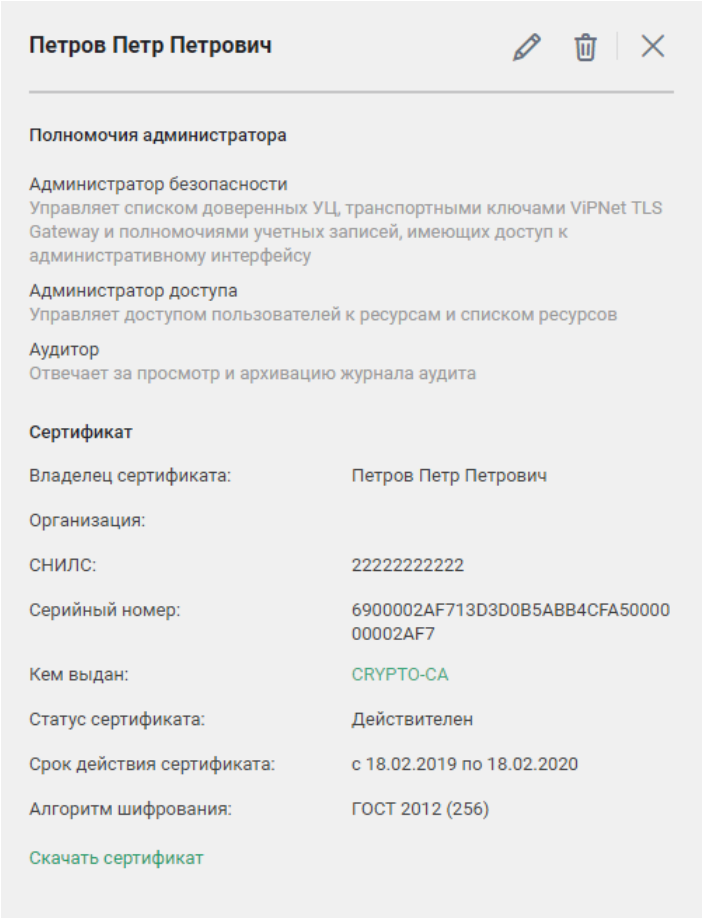

Рисунок 13. Просмотр данных об администраторах

4 При необходимости подробнее посмотреть параметры сертификата, на панели дополнительных сведений об администраторе щелкните ссылку **Скачать сертификат** и укажите место сохранения сертификата. После подтверждения сертификат будет сохранен в файл формата CER на вашем компьютере. Вы можете открыть файл и просмотреть сертификат администратора.

5 Для просмотра сертификата УЦ, издавшего сертификат администратора, на панели дополнительных сведений об администраторе в строке **Кем выдан** щелкните ссылку с названием издателя сертификата. Откроется раздел **Сертификаты удостоверяющих центров** с информацией о сертификате УЦ.

Управление ролями администратора

Вы можете изменять ранее назначенные роли администратора, например, если сотрудника, уже имеющего одну из ролей администратора, требуется наделить другими ролями администратора. Чтобы изменить роль администратора, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Сертификаты администраторов**.
3. На странице **Сертификаты администраторов** выберите сертификат нужного администратора и на панели дополнительных сведений об администраторе нажмите кнопку **Редактировать**.
4. В окне **Редактирование полномочий администратора** измените роли таким же образом, как и при добавлении нового администратора (см. Добавление нового администратора на стр. 76).
5. Нажмите кнопку **Сохранить**.

В результате роли администратора будут изменены. При следующем подключении к веб-интерфейсу ViPNet TLS Gateway администратор будет иметь полномочия в соответствии с новыми ролями.

Изменение версии протокола TLS для подключения администраторов

Версии протокола TLS для подключения администраторов задаются в процессе первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). При необходимости вы можете их изменить.

Изменение версии протокола TLS для подключения администраторов производится администратором безопасности (см. Администратор безопасности на стр. 35).

Внимание! Изменение версии протокола TLS может привести к потере удаленного доступа и всех соединений администраторов. Если вы используете криптопровайдер стороннего производителя, перед сохранением убедитесь, что он поддерживает выбранные версии протокола TLS (см. Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway на стр. 68).

Для восстановления доступа к веб-интерфейсу потребуется провести повторную инициализацию ViPNet TLS Gateway (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).

Чтобы изменить версию протокола TLS для подключения администраторов, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **TLS-подключение**.

4 В группе **Версия протокола TLS** в списке **Доступ администраторов** выберите нужные версии протокола TLS.

5 Нажмите кнопку **Сохранить**.

В результате для подключения администраторов будут использоваться выбранные версии протокола TLS.

Прекращение полномочий администратора

Полномочия администратора можно прекратить, например, в случае увольнения сотрудника, наделенного полномочиями администратора. Для прекращения полномочий администратора удалите сертификат администратора с ViPNet TLS Gateway. Чтобы удалить сертификат, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Сертификаты администраторов**.

3 На странице **Сертификаты администраторов** выберите нужный сертификат и на панели дополнительных сведений об администраторе нажмите кнопку **Удалить сертификат**.

Примечание. Вы можете удалить сертификаты сразу нескольких администраторов, для этого установите флажки напротив нужных сертификатов и на панели инструментов страницы **Сертификаты администраторов** нажмите кнопку **Удалить сертификаты**.

---

4 В появившемся окне подтвердите удаление сертификатов.

В результате сертификат администратора будет удален с ViPNet TLS Gateway. Данному администратору доступ к интерфейсу управления ViPNet TLS Gateway будет запрещен.

5

Организация доступа пользователей к защищаемым ресурсам

Последовательность действий 82

Управление параметрами доступа к ресурсам 83

Управление сертификатами доверенных удостоверяющих центров 92

Управление доступом пользователей к ресурсам 100

Последовательность действий

Чтобы организовать доступ пользователей к ресурсам вашей сети, необходимо настроить защищаемые ресурсы, добавить сертификаты пользователей и настроить правила доступа к ресурсам. Для этого выполните все действия из приведенного ниже списка.

Таблица 16. Порядок организации защищенного доступа пользователей к защищаемым ресурсам

	Действие	Ссылка
☐	Настройте параметры доступа к ресурсам, к которым планируете предоставлять защищенный доступ пользователям	Управление параметрами доступа к ресурсам (на стр. 83)
☐	Получите корневые сертификаты УЦ (или цепочки доверия к сертификатам (см. глоссарий, стр. 211)) и CRL у администраторов удостоверяющих центров, где изданы сертификаты пользователей	Установление доверия к одному или нескольким удостоверяющим центрам (на стр. 92)
☐	С рабочего места администратора безопасности подключитесь к веб-интерфейсу ViPNet TLS Gateway и добавьте полученные сертификаты на ViPNet TLS Gateway	Импорт сертификата и CRL доверенного УЦ (на стр. 93) Импорт списка сертификатов аккредитованных УЦ (на стр. 95)
☐	С рабочего места администратора доступа подключитесь к веб-интерфейсу ViPNet TLS Gateway и предоставьте пользователям защищенный доступ к необходимым ресурсам	Управление доступом пользователей к ресурсам (на стр. 100)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Управление параметрами доступа к ресурсам

Чтобы пользователи смогли удаленно получать доступ к веб-ресурсам вашей сети по защищенному каналу TLS, а также доступ к туннелируемым ресурсам, необходимо добавить ресурсы на ViPNet TLS Gateway и произвести настройки доступа к ним (см. Добавление веб-ресурса (на стр. 83) и Добавление TLS-туннеля (на стр. 85)). Управление параметрами доступа к ресурсам производится администратором доступа.

Добавление веб-ресурса

Для добавления защищаемого ресурса на ViPNet TLS Gateway выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На панели инструментов страницы **Ресурсы** нажмите кнопку **Добавить ресурс**.

4 В мастере добавления защищаемого ресурса на первой странице укажите следующую информацию о ресурсе:

- Наименование добавляемого ресурса. Это поле обязательно для заполнения, поскольку по наименованию ресурса администраторы смогут различать добавленные ресурсы для их настройки, а пользователи при подключении к ViPNet TLS Gateway смогут выбрать необходимые им ресурсы и запросить доступ к ним.
- Логотип ресурса. При необходимости вы можете загрузить логотип ресурса. Для пользователей выбранный логотип будет отображаться рядом с названием ресурса. Для загрузки нажмите кнопку **Загрузить** и выберите файл в формате PNG, JPEG, BMP или GIF. Размер загружаемых файлов не должен превышать 16 МБ. Рекомендуемый размер изображения 42x42 пикселя.
- Описание ресурса. При необходимости вы можете ввести описание ресурса, например, если из его наименования непонятно, для чего используется этот ресурс. Описание поможет пользователю разобраться, что это за ресурс.

5 На следующей странице мастера настройте режим работы с ресурсом:

5.1 В списке **Режим работы** выберите пункт **Веб-ресурс**.

5.2 Укажите адрес ресурса, по которому ViPNet TS Gateway будет обращаться к защищаемому ресурсу для перенаправления запросов от пользователей. Адрес защищаемого ресурса должен быть обязательно задан. Для этого в строке **Адрес ресурса** укажите в соответствующих полях протокол передачи данных, необходимый для подключения к

ресурсу (HTTP или HTTPS), IP-адрес или DNS-имя ресурса и порт (если используется). Например, `http://resource1.ru:123`.

6 На следующей странице мастера настройте параметры подключения к защищаемому ресурсу:

6.1 Укажите суффикс подключения ресурса (в виде сочетания букв или цифр). Это поле обязательно для заполнения. Суффикс будет добавлен к внешним адресам ViPNet TLS Gateway для доступа пользователей с указанным типом аутентификации, заданным в сетевых настройках (см. Сетевые настройки на стр. 136). По получившимся адресам подключения (отображаются ниже данной настройки) пользователи будут получать защищенный доступ к ресурсу, если доступ разрешен на ViPNet TLS Gateway. Например, адрес подключения пользователя к ресурсу может иметь вид:
`https://192.168.84.82:4431/wiki`, где

`https://192.168.84.82:4431` — адрес и порт сетевого интерфейса ViPNet TLS Gateway для доступа пользователей по каналу TLS с двусторонней аутентификацией, `wiki` — суффикс подключения веб-ресурса.

6.2 Укажите тип аутентификации пользователей для получения защищенного доступа к ресурсу по TLS-протоколу:

- Двусторонняя — позволяет ограничить доступ пользователей к ресурсу. Доступ пользователя к ресурсу возможен только после его явного разрешения администратором доступа и при наличии у пользователя действительного сертификата пользователя, а также корневых сертификатов или цепочки доверия к сертификатам (своего УЦ и УЦ ViPNet TLS Gateway). Это значение выбрано по умолчанию.
- Односторонняя — позволяет предоставить доступ к ресурсу любым пользователям, имеющим только корневой сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway (или цепочку доверия к сертификатам). При односторонней аутентификации доступ пользователей к ресурсу не может быть ограничен. Обеспечивается только защита канала доступа к ресурсу.

6.3 Укажите, нужно ли использовать выделенный порт для перенаправления запросов от пользователей к ресурсу с помощью флажка **Использовать выделенный порт**. По умолчанию флажок **Использовать выделенный порт** установлен и для перенаправления запросов от пользователей к настраиваемому ресурсу будет автоматически выделен порт. Рекомендуем использовать этот способ.

Внимание! При использовании выделенного порта для перенаправления запросов от пользователей к ресурсу файлы cookie этого ресурса будут попадать на другие защищаемые ресурсы. Чтобы избежать этого, снимите флажок **Использовать выделенный порт**. Подключение пользователей к ресурсу будет осуществляться с использованием суффиксов. В этом случае возможно неправильное отображение ресурса у пользователя и потребуется настройка правил преобразования URI ресурса (см. Создание правил преобразования URI ресурса на стр. 88).

6.4 Если вы используете исполнение TLS 1000 с модулем WAF, укажите, нужно ли использовать защиту ресурса от атак, сняв или установив флажок **Использовать Web Application Firewall**. По умолчанию защита ресурсов от атак отключена.

7 Нажмите кнопку **Сохранить**.

В результате данные о ресурсе и параметрах доступа к нему будут добавлены на ViPNet TLS Gateway. Список ресурсов отобразится на странице **Ресурсы**. Для каждого ресурса на панели дополнительных сведений вы можете посмотреть параметры подключения к ресурсу. После добавления параметров защищаемых ресурсов вы можете перейти к настройкам прав доступа к этим ресурсам для пользователей (см. Управление доступом пользователей к ресурсам на стр. 100).

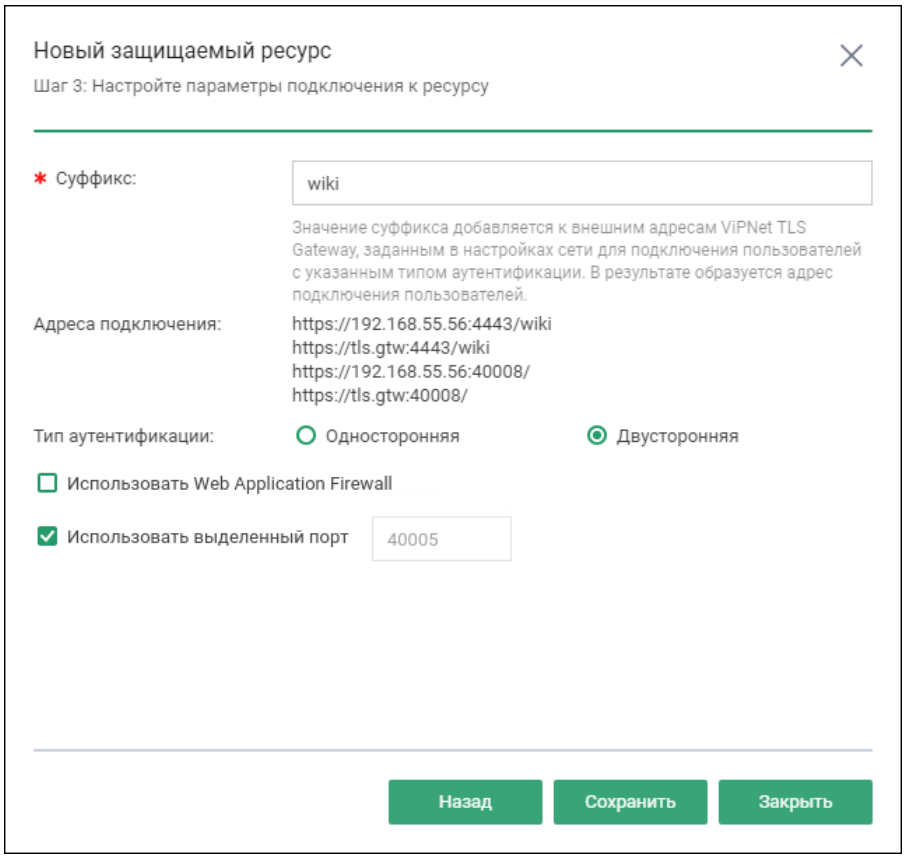

Рисунок 14. Добавление веб-ресурса

Добавление TLS-туннеля

Для добавления туннелируемого ресурса на ViPNet TLS Gateway выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На панели инструментов страницы **Ресурсы** нажмите кнопку **Добавить ресурс**.

4 В мастере добавления защищаемого ресурса на первой странице укажите следующую информацию о ресурсе:

- Наименование добавляемого ресурса. Это поле обязательно для заполнения, поскольку по наименованию ресурса администраторы смогут различать добавленные ресурсы для их настройки, а пользователи при подключении к ViPNet TLS Gateway смогут выбрать необходимые им ресурсы и запросить доступ к ним.
- Логотип ресурса. При необходимости вы можете загрузить логотип ресурса. Для пользователей выбранный логотип будет отображаться рядом с названием ресурса. Для загрузки нажмите кнопку **Загрузить** и выберите файл в формате PNG, JPEG, BMP или GIF. Размер загружаемых файлов не должен превышать 16 МБ. Рекомендуемый размер изображения 42x42 пикселя.
- Описание ресурса. При необходимости вы можете ввести описание ресурса, например, если из его наименования непонятно, для чего используется этот ресурс. Описание поможет пользователю разобраться, что это за ресурс.

5 На следующей странице мастера настройте режим работы с ресурсом:

5.1 В списке **Режим работы** выберите пункт **TLS-туннель**.

5.2 Укажите адрес ресурса, по которому ViPNet TS Gateway будет обращаться к защищаемому ресурсу для перенаправления запросов от пользователей. Адрес защищаемого ресурса должен быть обязательно задан. Для этого в строке **Адрес ресурса** укажите в соответствующих полях IP-адрес или DNS-имя ресурса и порт (если используется).

5.3 Укажите тип аутентификации пользователей для получения защищенного доступа к ресурсу по TLS-протоколу:

- Двусторонняя — позволяет ограничить доступ пользователей к ресурсу. Доступ пользователя к ресурсу возможен только после его явного разрешения администратором доступа и при наличии у пользователя действительного сертификата пользователя, а также корневых сертификатов или цепочки доверия к сертификатам (своего УЦ и УЦ ViPNet TLS Gateway). Это значение выбрано по умолчанию.
- Односторонняя — позволяет предоставить доступ к ресурсу любым пользователям, имеющим только корневой сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway (или цепочку доверия к сертификатам). При односторонней аутентификации доступ пользователей к ресурсу не может быть ограничен. Обеспечивается только защита канала доступа к ресурсу.

6 Нажмите кнопку **Сохранить**.

В результате данные о ресурсе и параметрах доступа к нему будут добавлены на ViPNet TLS Gateway. Список ресурсов отобразится на странице **Ресурсы**. Для каждого ресурса на панели дополнительных сведений вы можете посмотреть параметры подключения к ресурсу.

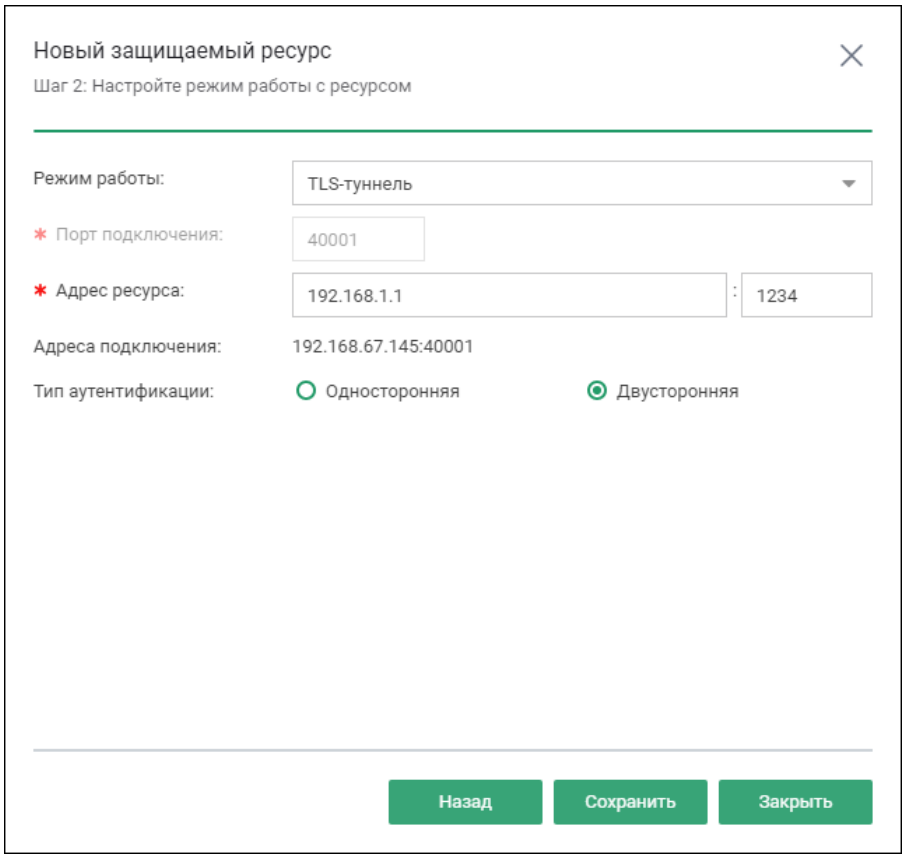

Рисунок 15. Добавление TLS-туннеля

Изменение параметров доступа к ресурсу

Вы можете изменить параметры доступа к защищаемому ресурсу, например, если изменился адрес доступа к ресурсу.

Чтобы изменить параметры доступа, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На странице **Ресурсы** выберите ресурс, параметры доступа к которому вы хотите изменить, и на панели дополнительных сведений о ресурсе нажмите кнопку **Редактировать**.

4 В окне **Редактирование параметров ресурса** на вкладке **Общие** и **Подключения** измените необходимую информацию о ресурсе таким же образом, как и при добавлении нового ресурса (см. Добавление веб-ресурса (на стр. 83) и Добавление TLS-туннеля (на стр. 85)).

5 Нажмите кнопку **Сохранить**.

В результате параметры доступа к защищаемому ресурсу будут изменены. Пользователям, при подключении к ресурсу будет предоставляться доступ в соответствии с новыми параметрами.

Для веб-ресурсов, при необходимости, вы можете создать правила преобразования URI ресурса в ходе выполнения функций прокси-сервера. Для этого перейдите на вкладку **Правила преобразования** (см. Создание правил преобразования URI ресурса на стр. 88).

Создание правил преобразования URI ресурса

Если у пользователей при подключении к защищаемому ресурсу нарушен формат его отображения, вы можете создать специальные правила преобразования URI для этого ресурса.

Внимание! Мы не рекомендуем добавлять эти правила без необходимости.

Чтобы настроить правила преобразования URI для ресурса, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На странице **Ресурсы** выберите ресурс, для которого необходимо настроить правила преобразования, и на панели дополнительных сведений о ресурсе нажмите кнопку **Редактировать**.

4 В окне **Редактирование параметров ресурса** перейдите на вкладку **Правила преобразования** и создайте правила преобразования URI выбранного ресурса в ходе выполнения функций прокси-сервера. Эти правила требуются для замены ссылок на различные объекты защищаемого ресурса, находящихся внутри html-страниц защищаемого ресурса, на ссылки, содержащие адрес сетевого интерфейса ViPNet TLS Gateway для доступа пользователей, а также для обратной замены.

   Для задания правил преобразования вы можете использовать следующий синтаксис:

   - `subs_filter_types [mime-types]` — перечень MIME-типов страниц, для которых применяются данные правила преобразования.
   - `subs_filter <регулярное выражение для поиска строки в источнике> <преобразованная строка> [<флаги преобразования>]`, где флаги преобразования могут иметь следующие значения:
     - `g` — (значение по умолчанию) замена всех совпадений в строке;
     - `i` — регистрозависимый поиск;
     - `o` — замена только для первого совпадения;
     - `r` — в качестве выражения для поиска используется регулярное выражение, а не фиксированная строка.

   Например, правила преобразования для сайта mosenergo.ru, видимого пользователям под адресом `tlsgateway.int/mosenergo`, могут выглядеть следующим образом:

```
subs_filter_types text/css text/xml;
```

```
subs_filter '(href=["\']*)(\/.+?)(["\' >]+)' '$1/mosenergo$2$3' gr;
subs_filter '(src=["\']*)(\/.+?)(["\' >]+)' '$1/mosenergo$2$3' gr;
subs_filter '(action=["\']*)(\/.+?)(["\' >]+)' '$1/mosenergo$2$3' gr;
subs_filter '(content=["\']*)(\/.+?)(["\' >]+)' '$1/mosenergo$2$3' gr;
subs_filter '(value=["\']*)(\/.+?)(["\' >]+)' '$1/mosenergo$2$3' gr;
subs_filter '(url[\(=]["\']*)(\/.+?)(["\' >\)]+)' '$1/mosenergo$2$3' gr;
subs_filter '(icon\':\'["\']*)(\/.+?)(["\' >\)]+)' '$1/mosenergo$2$3' gr;
```

5 Нажмите кнопку **Сохранить**.

В результате параметры доступа к защищаемому ресурсу будут изменены. Пользователям, при подключении к ресурсу будет предоставляться доступ в соответствии с новыми параметрами.

Прекращение защищенного доступа к ресурсу

Если к ресурсу больше не требуется предоставлять защищенный доступ пользователей, вы можете удалить данные об этом ресурсе с ViPNet TLS Gateway. Чтобы удалить ресурс с ViPNet TLS Gateway, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На странице **Ресурсы** выберите ресурс, который вы хотите удалить, и на панели дополнительных сведений о ресурсе нажмите кнопку **Удалить**.

Примечание. Вы можете удалить сразу несколько записей о ресурсах, для этого установите флажки напротив нужных ресурсов и на панели инструментов страницы **Ресурсы** нажмите кнопку **Удалить ресурсы**.

---

4 В появившемся окне подтвердите удаление ресурса, нажав кнопку **Да**.

В результате данные о ресурсе будут полностью удалены с ViPNet TLS Gateway. Пользователи больше не смогут получить к нему защищенный доступ.

Настройка шаблона отображения пользователю страницы доступа к ресурсам

Вы можете настроить внешний вид главной страницы ViPNet TLS Gateway, которая отображается пользователям при подключении к ViPNet TLS Gateway для получения доступа к защищаемым ресурсам. Вы можете настроить фон страницы и фон панели заголовка страницы, загрузив

графические файлы с необходимым фоном в формате PNG, JPEG, BMP или GIF. Размер загружаемых файлов не должен превышать 16 Мбайт.

Для настройки шаблона страницы доступа к ресурсам выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **Пользовательская страница** и на появившемся шаблоне отображения главной страницы ViPNet TLS Gateway щелкните элемент, фон которого вы хотите изменить.

4 Справа в разделе с названием выбранного элемента нажмите кнопку **Заменить фон** и выберите файл с фоном. При изменении фона страницы ниже из списка выберите способ применения фона к странице. Вы можете замостить страницу множеством одинаковых изображений из файла или растянуть изображение на всю страницу. Выбранный фон отобразится на шаблоне главной страницы. Если фон вам не нравится, для установки фона по умолчанию нажмите кнопку **По умолчанию**.

5 Выполните предыдущие действия для всех элементов шаблона страницы, которые вы хотите изменить.

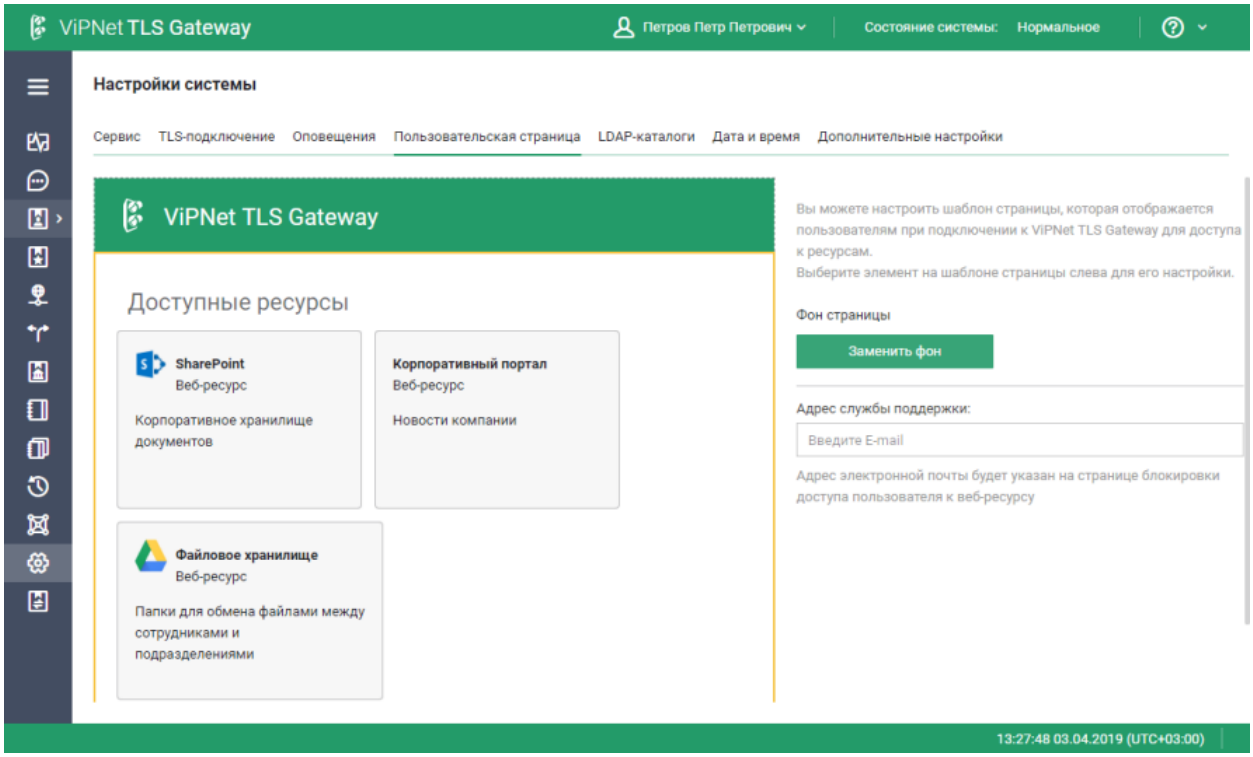

Рисунок 16. Настройка шаблона отображения страницы доступа к ресурсам

6 При необходимости настройте адрес электронной почты службы поддержки, который будет видеть пользователь в случае отказа в доступе к ресурсу (см. Изменение электронного адреса службы поддержки на стр. 91).

7 Нажмите кнопку **Сохранить**.

В результате фон страницы и/или фон панели заголовка страницы доступа к ресурсам будет изменен. Пользователи при подключении к ViPNet TLS Gateway для получения доступа к защищаемым ресурсам увидят главную страницу ViPNet TLS Gateway со списком доступных ресурсов в новом оформлении.

Изменение электронного адреса службы поддержки

Вы можете изменить адрес электронной почты службы поддержки, который будет видеть пользователь в случае отказа в доступе к защищаемому ресурсу.

Для изменения электронного адреса службы поддержки выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Перейдите в раздел **Система**.
3. На странице **Настройки системы** перейдите на вкладку **Пользовательская страница** и в разделе **Адрес службы поддержки** введите адрес электронной почты.
4. Нажмите кнопку **Сохранить**.

В результате адрес службы поддержки будет изменен. Пользователи, которым заблокирован доступ к ViPNet TLS Gateway, при попытке подключиться к ViPNet TLS Gateway или ресурсу увидят информацию об отказе в доступе и данный электронный адрес для связи со службой поддержки.

Управление сертификатами доверенных удостоверяющих центров

Установление доверия к одному или нескольким удостоверяющим центрам

Чтобы администраторы и пользователи смогли подключиться к ViPNet TLS Gateway по защищенному каналу TLS, на ViPNet TLS Gateway должно быть установлено доверие к УЦ, в которых изданы сертификаты администраторов и пользователей. Для этого на ViPNet TLS Gateway необходимо добавить действительные корневые сертификаты (см. глоссарий, стр. 210) и соответствующие действительные CRL (см. глоссарий, стр. 211) УЦ, в которых изданы сертификаты администраторов, пользователей и транспортные сертификаты ViPNet TLS Gateway (или сертификаты всех УЦ из цепочки доверия к сертификатам УЦ (см. глоссарий, стр. 211) и соответствующие CRL).

Доверие к УЦ, где изданы транспортные сертификаты ViPNet TLS Gateway и сертификаты администраторов, устанавливается в процессе первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). В дальнейшем сертификаты УЦ и CRL, например, при истечении срока их действия, добавляются на ViPNet TLS Gateway с помощью веб-интерфейса. Для автоматического добавления CRL вы можете настроить URL-адреса одной или нескольких точек распространения CRL. Если сертификаты пользователей были изданы в другом УЦ, то перед настройкой доступа пользователей к ресурсам необходимо установить доверие к УЦ пользователей.

Управление сертификатами УЦ и CRL производится администратором безопасности. Сертификаты УЦ и CRL вы можете получить у администратора УЦ, в котором издан соответствующий сертификат пользователя, после чего добавить каждый сертификат на ViPNet TLS Gateway (см. Импорт сертификата и CRL доверенного УЦ на стр. 93).

Если сертификаты пользователей выданы в аккредитованных УЦ (см. глоссарий, стр. 208), вы можете добавить сразу список сертификатов таких УЦ (см. Импорт списка сертификатов аккредитованных УЦ на стр. 95), импортировав их из файла со списком аккредитованных УЦ https://e-trust.gosuslugi.ru/CA в формате TSL (см. глоссарий, стр. 208).

Внимание! При загрузке CRL (автоматически из точек распространения или вручную) вам необходимо учитывать ограничения на суммарный размер файлов CRL, добавленных на ViPNet TLS Gateway (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51). Если суммарный размер добавленных файлов CRL превысит указанные значения,

будет ограничен доступ некоторых пользователей к защищаемым ресурсам по каналу TLS с двусторонней аутентификацией. В журнале событий (см. Работа с журналом событий на стр. 127) и на странице мониторинга (см. Просмотр отчетов мониторинга на стр. 131) появятся события с сообщением об ошибке при изменении конфигурационного файла веб-сервера. В журнале в столбце **Объект** для таких событий будет отображено наименование УЦ, в котором изданы сертификаты пользователей с заблокированным доступом. Для решения проблемы см. раздел Отображается ошибка при изменении конфигурационного файла веб-сервера (на стр. 190).

Импорт сертификата и CRL доверенного УЦ

Для установки доверия к УЦ на ViPNet TLS Gateway необходимо импортировать корневой сертификат и соответствующий CRL этого УЦ или в случае, если сертификат УЦ не является корневым, необходимо импортировать все сертификаты (и CRL) УЦ из цепочки доверия к сертификатам УЦ, начиная с корневого сертификата.

Перед импортом сертификатов получите их у администратора УЦ, к которому требуется установить доверие. Если получена цепочка сертификатов, убедитесь, что вы знаете, какому уровню иерархии издателей сертификатов из цепочки доверия принадлежат полученные сертификаты УЦ и соответствующие CRL. Загрузку этих сертификатов следует произвести строго в определенном порядке, начиная с корневого сертификата УЦ и соответствующего CRL и далее последовательно все сертификаты до последнего уровня иерархии цепочки доверия.

Чтобы импортировать сертификат удостоверяющего центра на ViPNet TLS Gateway, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Сертификаты удостоверяющих центров**.
3. На панели инструментов страницы **Сертификаты удостоверяющих центров** нажмите кнопку **Импортировать**.
4. В мастере импорта сертификатов на первой странице выберите файл с сертификатом УЦ в формате CER, CRT или PEM и нажмите кнопку **Далее**.
5. На второй странице мастера выполните следующие действия:
   - Проверьте данные об администраторе и его сертификате (данные подставляются из сертификата). Сертификат должен быть действительным.
   - В полях **Точка распространения CRL** и **Альтернативная точка распространения CRL** задайте URL-адреса сетевых ресурсов, на которых размещаются точки распространения CRL. Вы можете задать URL-адреса только основной точки распространения или обеих точек распространения.
   - Выберите интервал проверки наличия обновления CRL в заданных точках распространения. При установке значения `0` CRL обновляться не будут.

6 Нажмите кнопку **Импортировать**.

В результате сертификат УЦ будет добавлен на ViPNet TLS Gateway в список доверенных сертификатов и отобразится на странице **Сертификаты удостоверяющих центров**.

Если были заданы точки распространения CRL, соответствующий сертификату УЦ действительный CRL будет загружен на ViPNet TLS Gateway автоматически через несколько секунд в том случае, если в настройках был задан интервал времени проверки обновления CRL, отличный от нуля, а также есть доступ к этой точке распространения. CRL будет загружен из основной точки распространения, а в случае ее недоступности — из альтернативной точки распространения. Информация о статусе загрузки CRL отобразится на странице **Сертификаты удостоверяющих центров** в столбце **Статус CRL**. Если CRL автоматически загрузился, в столбце **Статус CRL** будет отображен статус **Действителен**.

Если CRL не загружается (в столбце **Статус CRL** отображен статус **Не загружен**) или в вашей организации недоступна возможность получения CRL из точек распространения CRL, то добавьте CRL следующим образом:

1 На панели инструментов страницы **Сертификаты удостоверяющих центров** нажмите кнопку **Загрузить CRL**.

2 Выберите файл с нужным CRL.

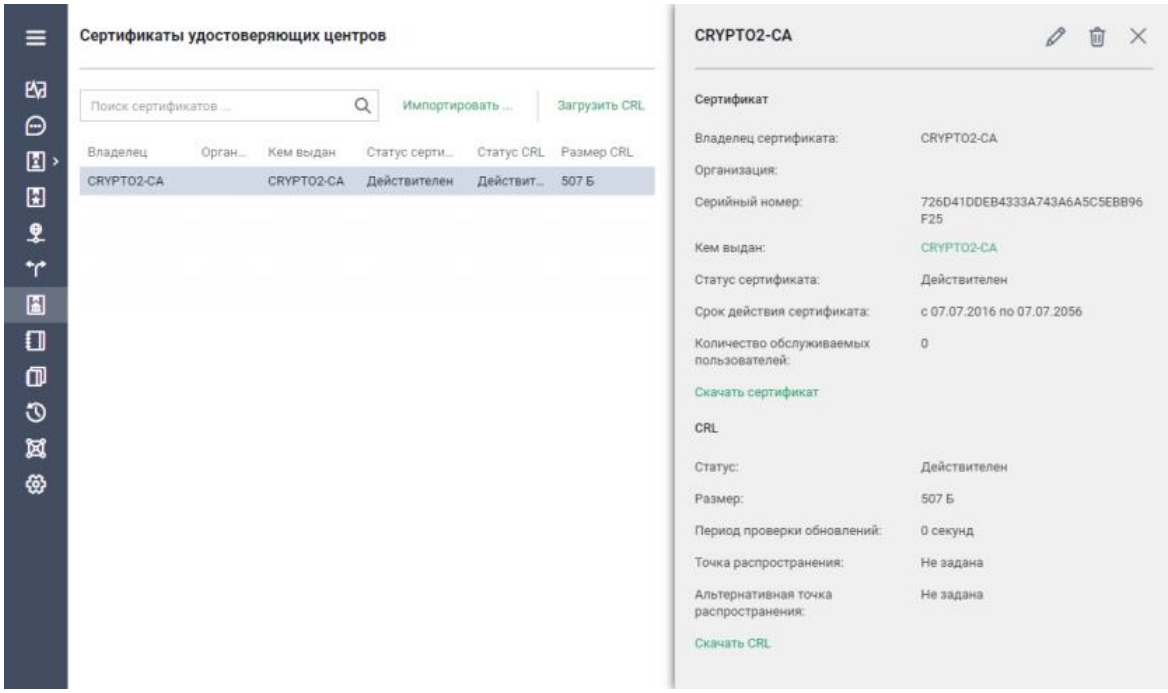

Рисунок 17. Сертификаты удостоверяющих центров

В результате CRL будет загружен на ViPNet TLS Gateway.

Повторите действия по импорту сертификата и CRL для сертификата и CRL каждого уровня иерархии из цепочки доверия к сертификатам. После загрузки последнего сертификата и CRL из цепочки доверия вы сможете управлять доступом к защищаемым ресурсам пользователей с

сертификатами, изданными в этих УЦ (см. Управление доступом пользователей к ресурсам на стр. 100).

Импорт списка сертификатов аккредитованных УЦ

Вы можете добавлять на ViPNet TLS Gateway по одному сертификату аккредитованного УЦ (см. Импорт сертификата и CRL доверенного УЦ на стр. 93) или добавить сразу список сертификатов УЦ, импортировав их из файла со списком сертификатов УЦ в формате TSL (далее — TSL-файл). Тем самым будет установлено доверие ко всем аккредитованным УЦ.

Внимание! Работа с TSL-файлом доступна в следующих исполнениях: TLS 1000, TLS 5000 и TLS VA. Виртуальная машина с TLS VA должна быть сконфигурирована специальным образом (см. Программная реализация TLS VA на стр. 16).

Для всех ранее настроенных защищаемых ресурсов и при добавлении новых ресурсов необходимо настраивать правила преобразования URI ресурса (см. Создание правил преобразования URI ресурса на стр. 88). Работа с использованием выделенных портов не поддерживается (см. Добавление веб-ресурса на стр. 83).

Перед импортом списка сертификатов аккредитованных УЦ на рабочем месте администратора безопасности загрузите следующие данные с портала уполномоченного федерального органа в области использования электронной подписи (Минкомсвязи России):

- корневой сертификат головного УЦ Минкомсвязи, сертификаты подчиненных УЦ первого уровня иерархии и CRL этих УЦ https://e-trust.gosuslugi.ru/MainCA;
- список сертификатов аккредитованных УЦ в формате TSL https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0.

Чтобы импортировать список сертификатов аккредитованных УЦ на ViPNet TLS Gateway, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Сертификаты удостоверяющих центров**.
3. Загрузите корневой сертификат головного УЦ Минкомсвязи и CRL (см. Импорт сертификата и CRL доверенного УЦ на стр. 93).
4. Загрузите поочередно все остальные сертификаты и CRL УЦ первого уровня иерархии, подчиненных головному УЦ Минкомсвязи (см. Импорт сертификата и CRL доверенного УЦ на стр. 93). Загрузка сертификатов подчиненных УЦ может быть произведена в любом порядке.
5. Убедитесь, что все сертификаты УЦ и CRL успешно загрузились на ViPNet TLS Gateway и отображаются на странице **Сертификаты удостоверяющих центров**. CRL считаются успешно загруженными, если для сертификата в столбце **Статус CRL** отображен статус **Действителен**.
6. На панели инструментов страницы **Сертификаты удостоверяющих центров** нажмите кнопку **Импортировать**.

7 В мастере импорта сертификатов на первой странице выберите TSL-файл с доверенным списком сертификатов аккредитованных УЦ в формате XML и нажмите кнопку **Далее**. Дождитесь загрузки данных о сертификатах аккредитованных УЦ из этого файла.

8 На второй странице мастера выполните следующие действия:

- Просмотрите появившийся список сертификатов УЦ и убедитесь, что он содержит необходимые вам сертификаты. Сертификаты будут импортированы и добавлены на ViPNet TLS Gateway в зависимости от присвоенного им статуса:
  - Новый — действующий сертификат, еще не добавленный на ViPNet TLS Gateway. Новые сертификаты будут импортированы из TSL-файла и добавлены на ViPNet TLS Gateway (помечены недоступным для редактирования флажком).
  - Загружен ранее — действующий сертификат, ранее добавленный на ViPNet TLS Gateway из TSL-файла. Ранее загруженные сертификаты повторно не добавляются на ViPNet TLS Gateway (сертификаты не помечены флажком и установка флажка недоступна).
  - Загружен вручную — аналогичный сертификат был ранее добавлен вручную из файла с сертификатом в формате CER, CRT или PEM. Вручную загруженные сертификаты не заменяются сертификатами из TSL-файла (сертификаты не помечены флажком и установка флажка недоступна).
  - Изменены адреса точек распространения — у действующего сертификата, ранее добавленного на ViPNet TLS Gateway из TSL-файла, изменились адреса точек распространения. Для таких сертификатов вам нужно принять решение о необходимости импорта и загрузки их на ViPNet TLS Gateway взамен ранее добавленных. По умолчанию адреса точек распространения изменены не будут.
  - Удален — действующий сертификат, ранее добавленный на ViPNet TLS Gateway из TSL-файла, отсутствует в TSL-файле. Для таких сертификатов вам нужно принять решение о необходимости их удаления с ViPNet TLS Gateway. По умолчанию сертификаты удалены не будут.
  - Отклонен — отклоненный сертификат по одной из причин: истек срок действия, имеет некорректную подпись, нет корневого сертификата для проверки электронной подписи, сертификат отозван и прочие причины. Отклоненные сертификаты не добавляются на ViPNet TLS Gateway (сертификаты не помечены флажком и установка флажка недоступна).

  Для поиска сертификатов вы можете воспользоваться строкой поиска сертификатов по имени владельца или организации, а также фильтрацией по присвоенным статусам.
- В случае наличия сертификатов с измененными адресами точек распространения установите флажки напротив тех сертификатов, которые необходимо импортировать, чтобы заменить ранее добавленные на ViPNet TLS Gateway сертификаты. По умолчанию флажки сняты.
- В случае наличия удаленных сертификатов установите флажки напротив тех сертификатов, которые необходимо удалить с ViPNet TLS Gateway. По умолчанию флажки сняты.

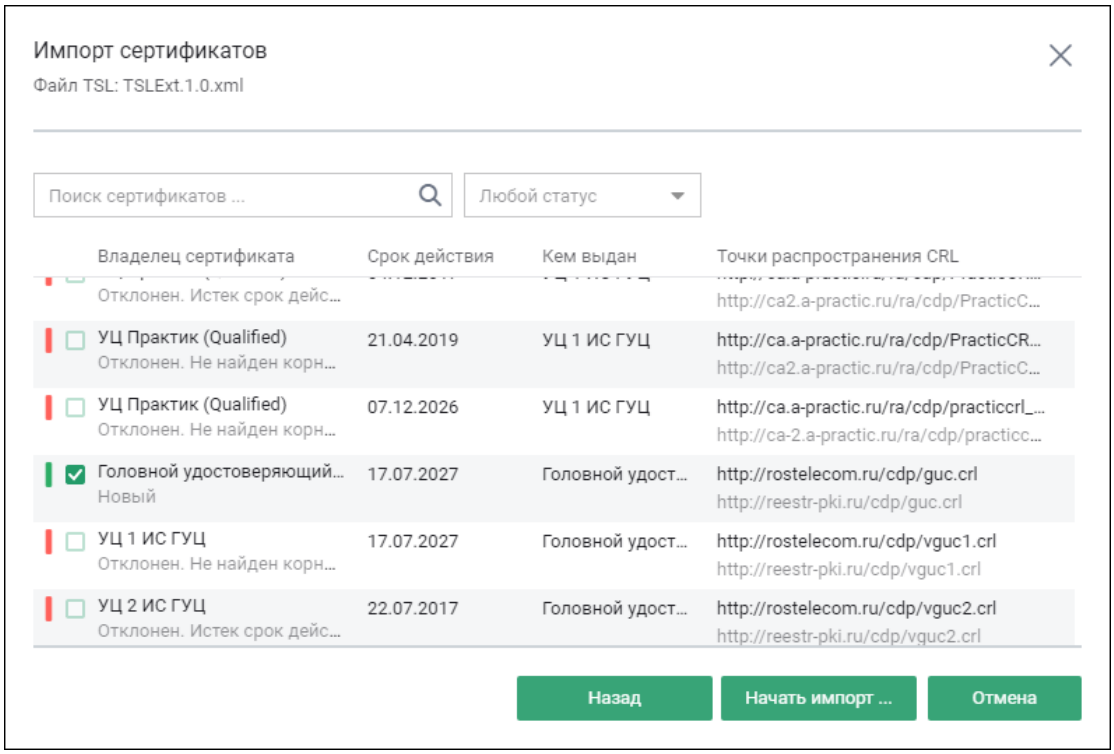

Рисунок 18. Просмотр списка импортируемых сертификатов

9 Нажмите кнопку **Начать импорт**. Дождитесь завершения импорта.

В результате список сертификатов УЦ в зависимости от статуса будет добавлен на ViPNet TLS Gateway в список доверенных сертификатов и отобразится на странице **Сертификаты удостоверяющих центров**. Если для сертификата была задана точка распространения CRL, соответствующий сертификату УЦ действительный CRL будет загружен на ViPNet TLS Gateway автоматически. Информация о статусе загрузки CRL также отобразится на странице **Сертификаты удостоверяющих центров** в столбце **Статус CRL**. При необходимости, вы можете настроить точки распространения CRL для каждого сертификата (см. Настройка адресов точек распространения CRL на стр. 97) или при наличии файлов с CRL загрузить их вручную (см. Импорт сертификата и CRL доверенного УЦ на стр. 93).

После загрузки всех необходимых действительных сертификатов и CRL УЦ, доверие ко всем аккредитованным УЦ будет установлено. Вы сможете управлять доступом к защищаемым ресурсам пользователей с сертификатами, выданными в этих УЦ (см. Управление доступом пользователей к ресурсам на стр. 100).

Настройка адресов точек распространения CRL

Если для сертификата УЦ не настроен адрес точки распространения CRL или необходимо изменить текущий адрес точки распространения, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Сертификаты удостоверяющих центров**.

3 На странице **Сертификаты удостоверяющих центров** выберите нужный сертификат и на панели дополнительных сведений нажмите кнопку **Редактировать**.

4 В окне **Редактирование параметров сертификата УЦ** произведите настройку точек распространения CRL и периода обновления CRL таким же образом, как и при добавлении сертификата УЦ (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92).

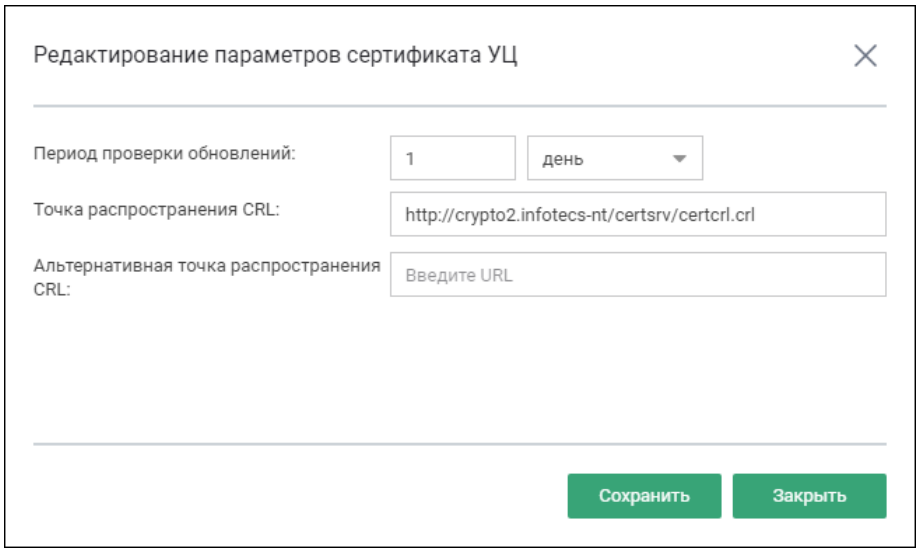

Рисунок 19. Настройка точки распространения CRL

В результате одна или несколько точек распространения CRL будут настроены. Наличие обновлений CRL будет проверяться с заданным периодом и при появлении на одной из точек распространения нового CRL, он будет автоматически загружен на ViPNet TLS Gateway (при наличии доступа к точке распространения). CRL будет загружен из основной точки распространения CRL, а в случае ее недоступности — из альтернативной точки распространения. Если в интервале времени проверки обновления CRL задано значение `0`, CRL автоматически загружаться не будет.

Исключение сертификата удостоверяющего центра из списка доверенных

Вы можете исключить сертификат какого-либо удостоверяющего центра, где изданы сертификаты пользователей, из списка доверенных, например, если удостоверяющий центр утратил доверие и необходимо прекратить доступ соответствующих пользователей к ViPNet TLS Gateway и защищаемым ресурсам. Для этого сертификат УЦ нужно удалить с ViPNet TLS Gateway.

Внимание! Удаление корневого сертификата УЦ доступно только после удаления всех сертификатов подчиненных ему УЦ.

Чтобы удалить сертификат УЦ, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Сертификаты удостоверяющих центров**.

3 На странице **Сертификаты удостоверяющих центров** выберите сертификат удостоверяющего центра, который вы хотите удалить, и на панели дополнительных сведений нажмите кнопку **Удалить сертификат**.

Внимание! При удалении сертификата УЦ будут удалены также все сертификаты пользователей, выданные данным УЦ.

4 В появившемся окне подтвердите удаление.

В результате сертификат УЦ будет исключен из списка доверенных сертификатов ViPNet TLS Gateway и пользователи с сертификатами, изданными в соответствующем УЦ, потеряют доступ к ViPNet TLS Gateway и защищаемым ресурсам. Для восстановления защищенного доступа указанных пользователей к ViPNet TLS Gateway и ресурсам необходимо заново установить доверие к их удостоверяющему центру (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92), а также заново добавить сертификаты пользователей (см. Управление доступом пользователей к ресурсам на стр. 100).

Управление доступом пользователей к ресурсам

Настройка доступа определенных пользователей к защищаемым ресурсам возможна только для тех ресурсов, в параметрах доступа которых задана двусторонняя аутентификация по протоколу TLS (см. Добавление веб-ресурса на стр. 83).

Управление доступом пользователей к защищаемым ресурсам, настроенным на ViPNet TLS Gateway, производится администратором доступа.

Чтобы предоставить или запретить новому пользователю защищенный доступ к необходимым ресурсам по каналу TLS с двусторонней аутентификацией, нужно добавить сертификат этого пользователя (см. Требования к сертификатам для работы с ViPNet TLS Gateway на стр. 51) на ViPNet TLS Gateway и произвести настройки доступа к ресурсам.

Внимание! Проверьте, что на ViPNet TLS Gateway добавлены действительные сертификаты и действительные CRL из цепочки доверия к УЦ, в которых изданы сертификаты пользователей (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92). Иначе этим пользователям невозможно будет предоставить защищенный доступ к ресурсам.

Вы можете настроить следующие права доступа пользователей к защищаемым ресурсам:

- Разрешить доступ к ресурсу.
- Запретить доступ к ресурсу.
- Запретить доступ к ViPNet TLS Gateway и ко всем ресурсам, настроенным на ViPNet TLS Gateway.

Для новых пользователей вы можете настроить права доступа к ресурсам следующими способами:

- Вручную с помощью добавления сертификатов пользователей (см. Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя на стр. 102).
- С помощью обработки запросов пользователей на доступ к ресурсам (см. Назначение прав доступа к ресурсам по запросу пользователя на стр. 105).
- Настроив правила автоматического назначения пользователям прав доступа к ресурсам (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109).

После первоначальной настройки прав доступа пользователей к ресурсам вы можете их изменять (см. Изменение прав доступа к ресурсам существующего пользователя на стр. 119).

Режимы доступа сертификатов пользователей

Все добавленные на ViPNet TLS Gateway сертификаты пользователей имеют режим доступа. Режим доступа определяет, кто на данный момент управляет правами доступа пользователя к защищаемым ресурсам.

На ViPNet TLS Gateway предусмотрены следующие режимы доступа сертификатов пользователей:

- **Доступ к ресурсам определяется администратором**, **Заблокирован администратором**.

  В этом режиме права доступа к ресурсам определяются администратором. На такие сертификаты не действуют правила автоматического предоставления доступа.

  В этот режим переводятся сертификаты пользователей при:

  - добавлении сертификатов пользователей вручную (см. Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя на стр. 102);
  - после обработки запросов пользователей на доступ к ресурсам (см. Назначение прав доступа к ресурсам по запросу пользователя на стр. 105);
  - изменении прав доступа к ресурсам вручную (см. Изменение прав доступа к ресурсам вручную на стр. 120).

- **Доступ к ресурсам определяется правилом <название правила>**, **Заблокирован правилом <название правила>**.

  В этом режиме права доступа к ресурсам определяются правилами, настроенными на ViPNet TLS Gateway (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109).

  В этот режим переводятся сертификаты пользователей при:

  - срабатывании правила автоматического предоставления доступа;
  - применении правил доступа к сертификату пользователя (см. Применение правил автоматического предоставления доступа на стр. 121).

- **К данному сертификату неприменимо ни одно из настроенных правил, доступ к ресурсам не определен.**

  В этот режим переводятся:

  - сертификаты новых пользователей, для которых неприменимо ни одно из настроенных правил доступа;
  - сертификаты существующих пользователей в режиме **Доступ к ресурсам определяется правилом <название правила>**, **Заблокирован правилом <название правила>**, для которых перестали применяться правила доступа, например, если внесли изменения в Active Directory и произошла синхронизация с LDAP-сервером, или администратор изменил существующие правила доступа.

  В этом режиме права доступа к ресурсам не определены.

Для предоставления доступа к ресурсам администратору необходимо изменить права доступа к ресурсам вручную (см. Изменение прав доступа к ресурсам вручную на стр. 120) или создать новое правило предоставления доступа к ресурсам (см. Создание правила предоставления доступа пользователю к заданным ресурсам на стр. 112).

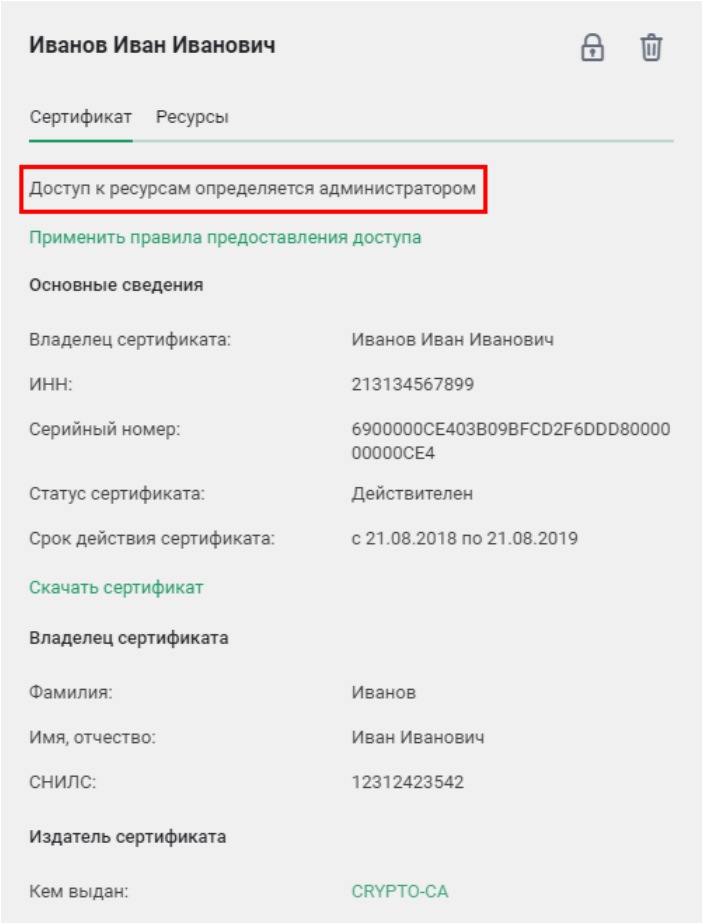

Рисунок 20. Режим доступа сертификата пользователя

Добавление нового пользователя и назначение прав доступа к ресурсам с помощью сертификата пользователя

Для добавления нового пользователя и назначения прав доступа получите его сертификат в удостоверяющем центре и загрузите на ViPNet TLS Gateway. Это позволит предоставить доступ пользователям без запросов от них. Вы можете добавить одного или сразу несколько пользователей. В результате пользователю могут быть назначены следующие права доступа на ресурсы:

- разрешить доступ к определенным ресурсам;
- запретить доступ к определенным ресурсам;

- заблокировать доступ пользователя к ViPNet TLS Gateway и ко всем веб-ресурсам (см. Изменение прав доступа к ресурсам существующего пользователя на стр. 119).

Для разрешения или запрета доступа пользователю к определенным ресурсам выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Сертификаты пользователей** > **Разрешенные**.

3 На панели инструментов страницы **Сертификаты пользователей, которым разрешено подключение по TLS-протоколу** нажмите кнопку **Добавить сертификат**.

4 В мастере добавления сертификатов пользователей на первой странице выберите один или несколько файлов с сертификатами.

5 На следующей странице **Проверка списка загруженных сертификатов** проверьте, что загружены действительные сертификаты со статусом **Новый**.

Примечание. Если сертификат пользователя уже добавлен на ViPNet TLS Gateway, в статусе сертификата отобразится значение **Существует**. Повторное добавление сертификата невозможно. Следующие шаги мастера будут недоступны. Об изменении прав доступа к ресурсам для пользователя этого сертификата см. в разделе Изменение прав доступа к ресурсам существующего пользователя (на стр. 119). Если выбрано несколько сертификатов, то следующие шаги мастера будут доступны только для сертификатов со статусом **Новый**.

---

6 На странице **Назначение прав доступа к ресурсам** назначьте права доступа к ресурсам. Предварительно вы можете воспользоваться поиском ресурсов. Для каждого ресурса выполните одно из следующих действий:

- Для разрешения доступа пользователя к ресурсу справа от названия ресурса нажмите кнопку **Разрешить**. Ресурс будет помечен как доступный.
- Для запрещения доступа пользователя к ресурсу справа от названия ресурса нажмите кнопку **Блокировать**. Ресурс будет помечен как блокированный.

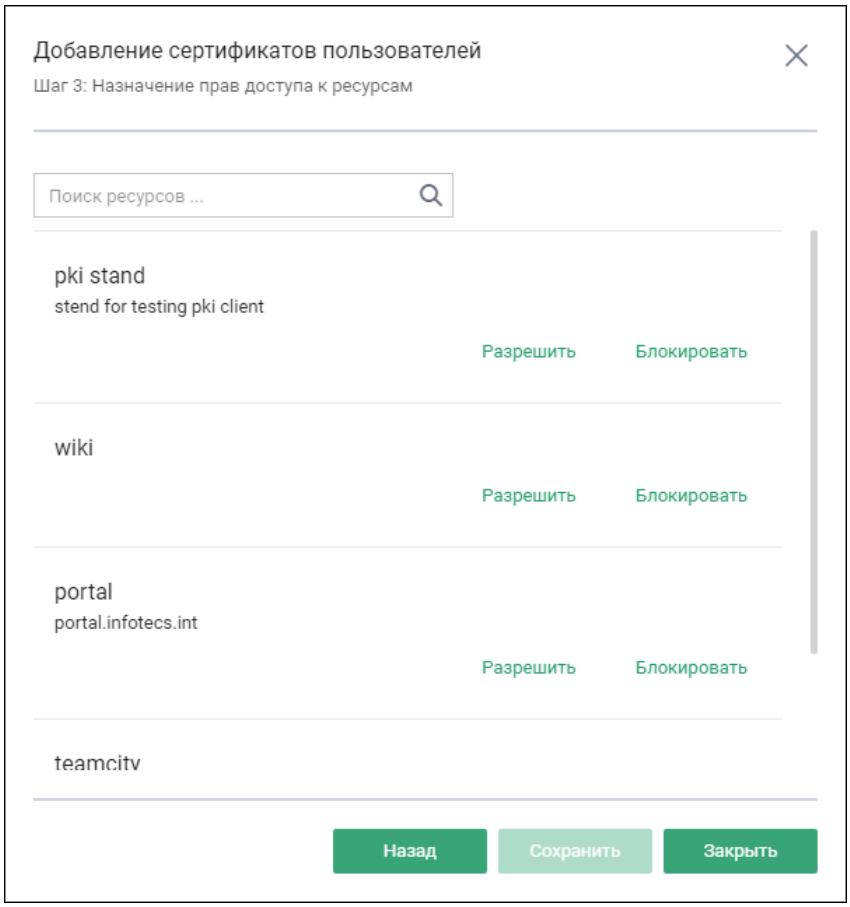

Рисунок 21. Назначение прав доступа к ресурсам

7 Нажмите кнопку **Сохранить**.

В результате сертификаты новых пользователей будут добавлены на ViPNet TLS Gateway в раздел **Сертификаты пользователей** > **Разрешенные** и переведены в режим **Доступ к ресурсам определяется администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). После установки пользователем на своем компьютере корневого сертификата УЦ и своего сертификата в системное хранилище пользователь сможет получить защищенный доступ по каналу TLS с двусторонней аутентификацией к разрешенным вами ресурсам.

Блокирование доступа нового пользователя к ViPNet TLS Gateway и ко всем ресурсам

Вы можете добавить одного или сразу несколько сертификатов новых пользователей и заблокировать им доступ к ViPNet TLS Gateway и ко всем заданным на нем ресурсам, например, чтобы временно не обслуживать пользователя. Для этого выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Сертификаты пользователей** > **Блокированные**.

3 На панели инструментов страницы **Сертификаты пользователей, которым запрещено подключение по TLS-протоколу** нажмите кнопку **Добавить сертификат**.

4 В мастере **Блокировка сертификатов** на первой странице выберите один или несколько файлов с сертификатами пользователей и нажмите кнопку **Далее**.

5 На следующей странице **Проверка списка загруженных сертификатов** проверьте, что загружены действительные сертификаты со статусом **Новый**, и нажмите кнопку **Блокировать**.

Примечание. Если сертификат пользователя уже добавлен на ViPNet TLS Gateway, в статусе сертификата отобразится значение **Существует**. Повторное добавление сертификата невозможно. Для существующего пользователя вы можете заблокировать доступ ко всем ресурсам в разделе **Сертификаты пользователей** > **Разрешенные** (см. Изменение прав доступа к ресурсам существующего пользователя на стр. 119).

В результате сертификаты новых пользователей будут добавлены на ViPNet TLS Gateway в список заблокированных (в раздел **Сертификаты пользователей** > **Блокированные**) и переведены в режим **Заблокирован администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). Этим пользователям будет запрещен защищенный доступ к ViPNet TLS Gateway и ко всем ресурсам, параметры доступа к которым настроены на ViPNet TLS Gateway (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109). При попытке пользователя подключиться к ViPNet TLS Gateway или какому-либо ресурсу по каналу TLS с двусторонней аутентификацией на экране пользователя появится страница с информацией о запрете доступа и адресом электронной почты администратора для связи (см. Изменение электронного адреса службы поддержки на стр. 91).

Назначение прав доступа к ресурсам по запросу пользователя

Пользователи при подключении к ViPNet TLS Gateway по каналу TLS с двусторонней аутентификацией для получения доступа к защищаемым ресурсам присылают запрос. Запрос на предоставление доступа содержит информацию о ресурсах, к которым требуется доступ, а также сертификат пользователя. После получения запрос появляется в списке запросов на предоставление доступа к ресурсам, где его можно обработать. В результате обработки запроса вы можете назначить пользователю следующие права доступа на запрашиваемые защищаемые ресурсы:

- разрешить доступ пользователю ко всем запрашиваемым ресурсам;
- настроить права доступа к запрашиваемым ресурсам;
- запретить доступ пользователю ко всем запрашиваемым ресурсам;
- запретить пользователю доступ к ViPNet TLS Gateway и ко всем заданным на нем ресурсам.

После обработки запроса сертификат пользователя добавляется на ViPNet TLS Gateway в список разрешенных или запрещенных сертификатов и переводится в режим **Доступ определяется администратором** или **Заблокирован администратором** в зависимости от настроенных пользователю прав доступа к ресурсам.

Внимание! Если на ViPNet TLS Gateway настроены правила предоставления доступа (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109), при поступлении запроса от пользователя, на сертификате которого сработало одно из правил, запрос будет обработан автоматически и пользователю будут выданы настроенные в правиле права доступа к ресурсам. Сертификат будет переведен в режим **Доступ к ресурсам определяется правилом <название правила>** (см. Режимы доступа сертификатов пользователей на стр. 101). В этом случае запрос не появится в списке запросов на обработку.

Чтобы обработать поступивший запрос на предоставление доступа, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Запросы на предоставление доступа**. Если в разделе есть необработанные запросы, справа от названия раздела будет отображена информация об их количестве.

3 На странице **Запросы на предоставление доступа** выберите один или несколько запросов. При необходимости предварительно воспользуйтесь поиском на панели инструментов страницы. В зависимости от количества выбранных запросов выполните одно из следующих действий:

- Для обработки одного запроса на панели дополнительных сведений о запросе выберите вкладку **Запрос на доступ** и назначьте права доступа пользователя к запрашиваемым ресурсам, выполнив одно из следующих действий:
  - Чтобы разрешить или запретить доступ сразу ко всем запрашиваемым ресурсам, на панели дополнительных сведений нажмите кнопку **Еще** и в меню выберите пункт **Разрешить все** или **Блокировать все**.
  - Чтобы разрешить или запретить доступ к определенным ресурсам из запроса пользователя, нажмите кнопку **Разрешить** или **Блокировать** справа от названия ресурса.
  - Для полного запрета пользователю доступа к ViPNet TLS Gateway и ко всем ресурсам на панели дополнительных сведений нажмите кнопку **Еще** и из меню выберите **Блокировать сертификат**.

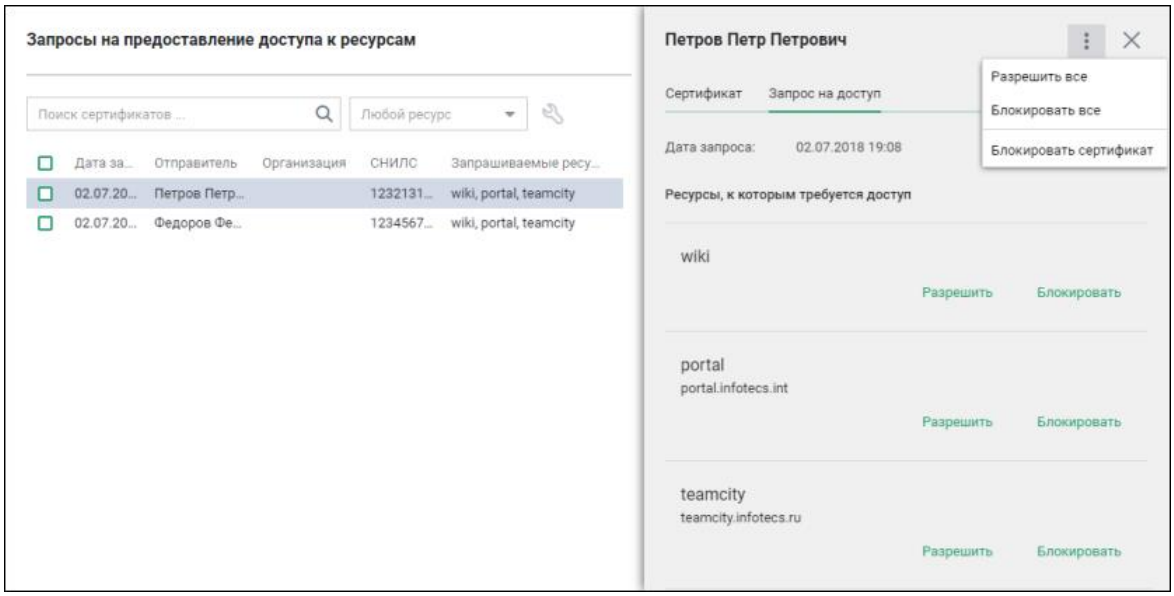

Рисунок 22. Обработка одного запроса пользователя на доступ к ресурсам

- Для обработки нескольких выбранных запросов от пользователей на панели инструментов страницы **Запросы на предоставление доступа** щелкните меню **Настроить доступ к ресурсу** и для каждого запрашиваемого ресурса выполните одно из следующих действий:
  - Для разрешения доступа пользователей к ресурсу выберите пункт меню **Разрешить доступ** и далее название ресурса.
  - Для запрещения доступа пользователей к ресурсу выберите пункт меню **Блокировать доступ** и далее название ресурса.

Внимание! Назначение прав доступа будет доступно только для тех ресурсов, доступ к которым запрашивается во всех выбранных запросах.

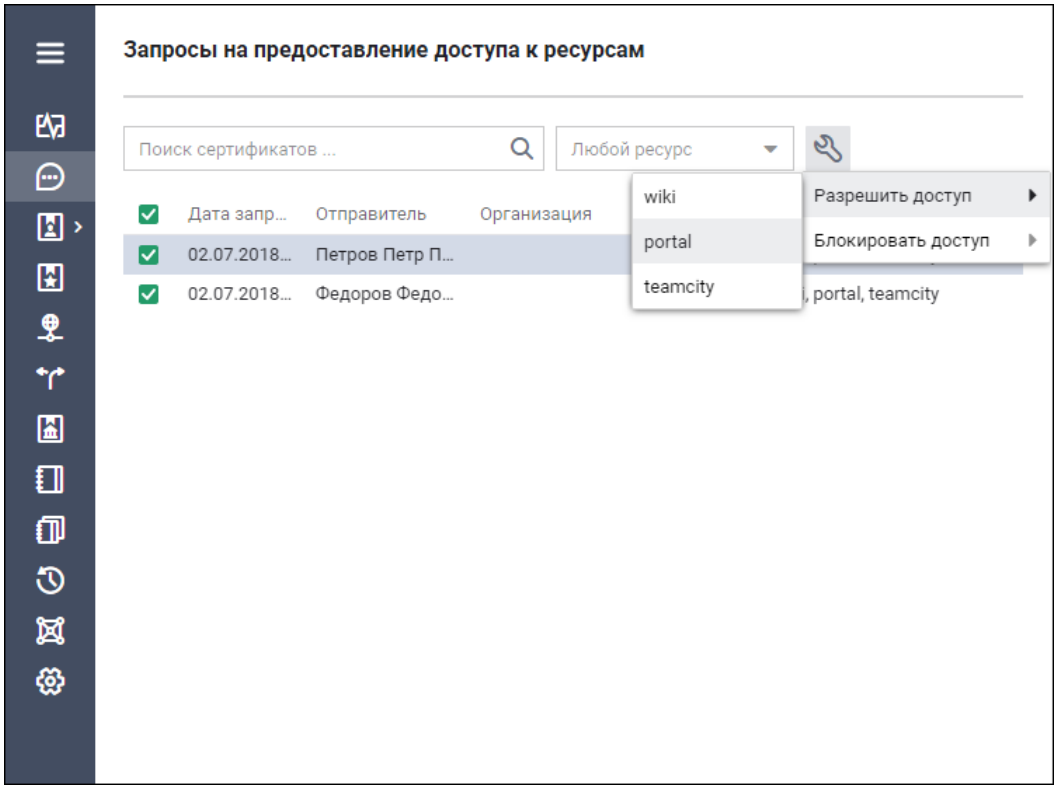

Рисунок 23. Обработка нескольких запросов пользователей на доступ к ресурсам

После назначения прав доступа для всех перечисленных в запросах ресурсов запросы будут обработаны и исчезнут из списка запросов.

Сертификаты новых пользователей, которым настроен доступ к определенным ресурсам добавятся на ViPNet TLS Gateway в раздел **Сертификаты пользователей** > **Разрешенные** и будут добавлены права доступа к ресурсам. Для пользователей, чьи сертификаты уже присутствуют в разделе **Сертификаты пользователей** > **Разрешенные**, будут добавлены настроенные вами права доступа на защищаемые ресурсы. Указанные выше сертификаты будут переведены в режим **Доступ к ресурсам определяется администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). В результате пользователи получат защищенный доступ по каналу TLS с двусторонней аутентификацией к запрашиваемым ресурсам в соответствии с вашими настройками.

Сертификаты пользователей, которым запрещен доступ к ViPNet TLS Gateway и ко всем ресурсам, будут добавлены на ViPNet TLS Gateway в раздел **Сертификаты пользователей** > **Блокированные** и переведены в режим **Заблокирован администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). При попытке пользователя подключиться к ViPNet TLS Gateway или какому-либо ресурсу по каналу TLS с двусторонней аутентификацией на экране пользователя появится страница с информацией о запрете доступа и адресом электронной почты администратора для связи (см. Изменение электронного адреса службы поддержки на стр. 91).

Правила автоматического назначения пользователям прав доступа к ресурсам

Вы можете настроить правила предоставления защищенного доступа к ресурсам пользователям по определенному признаку в их сертификате или атрибутам, импортированным из службы каталогов Active Directory (см. Настройка взаимодействия с Active Directory на стр. 109). Согласно этим правилам доступ к защищаемым ресурсам будет приниматься на ViPNet TLS Gateway автоматически (без участия администратора). Правила предоставления доступа применяются к сертификатам пользователей при:

- получении от пользователя запроса на доступ к ресурсу;
- редактировании и изменении порядка применения правил;
- синхронизации данных из службы каталогов Active Directory, если в ней произошли изменения.

В правиле предоставления доступа настраиваются:

- Условия выполнения правила: значения полей сертификата или атрибуты, импортированные из службы каталогов Active Directory и операторы условий.
- Действие при выполнении условий:
  - Предоставить или запретить доступ к ресурсам, настроенным в правиле (см. Создание правила предоставления доступа пользователю к заданным ресурсам на стр. 112). В этом случае в правиле задаются права доступа к необходимым ресурсам.
  - Отказать в предоставлении доступа к ViPNet TLS Gateway и ко всем заданным на нем ресурсам (см. Создание правила блокировки доступа пользователю к ViPNet TLS Gateway и ко всем ресурсам на стр. 117).

После создания правил вы можете настроить порядок их применения к сертификатам пользователей (см. Просмотр, редактирование и настройка порядка применения правил доступа на стр. 118). Все правила применяются последовательно друг за другом и при выполнении условий одного из правил, последующие правила не применяются.

Настройка взаимодействия с Active Directory

Если в вашей сети используется служба каталогов Active Directory, вы можете импортировать из нее данные сотрудников в ViPNet TLS Gateway для предоставления прав доступа к ресурсам (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109).

Для этого:

1. Добавьте LDAP-каталог в настройки ViPNet TLS Gateway (см. Добавление LDAP-каталога на стр. 110).
2. Синхронизируйте данные о пользователях, хранящиеся на ViPNet TLS Gateway с LDAP-каталогом (см. Синхронизация LDAP-каталога на стр. 111).

Добавление LDAP-каталога

Чтобы добавить LDAP-каталог, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **LDAP-каталоги** и нажмите кнопку **Добавить каталог.**

4 В разделе **Настройки подключения** в соответствующих полях укажите следующие данные:

- Наименование добавляемого LDAP-каталога.
- Адрес и порт LDAP-сервера. По умолчанию указан порт 389.
- Учетные данные пользователя LDAP-сервера, который обладает правами на чтение записей LDAP-сервера.
- Выделенное имя (DN, Distinguished Name) базы поиска, с которой начинаются операции поиска в LDAP-каталоге.
- В поле **Фильтр** задайте одно или несколько условий поиска записей в LDAP-каталоге в формате `<Атрибут AD><Оператор сравнения><Значение>`, где `<Оператор сравнения>` может принимать следующие значения:
  - = (равно);
  - >= (больше или равно);
  - <= (меньше или равно).

  По умолчанию задано значение «(objectClass=*)», при котором будут найдены все записи с атрибутом objectClass, имеющие любое значение.
- Глубину поиска записей относительно базы поиска.
- Чтобы импортировать в ViPNet TLS Gateway только определенные атрибуты, установите флажок **Выгружать заданные атрибуты** и в поле **Атрибут LDAP** введите имя атрибута, который хотите импортировать. При необходимости вы можете добавить другие атрибуты. Для этого нажмите кнопку и в соответствующем поле введите имя атрибута.

  По умолчанию будут импортированы все атрибуты, которые содержатся в записях, заданных в поле **Фильтр**.

5 Чтобы проверить соединение с LDAP-сервером, нажмите соответствующую кнопку.

6 В разделе **Расписание синхронизации** задайте время и периодичность синхронизации данных LDAP-каталога с данными, импортированными на ViPNet TLS Gateway.

7 Нажмите кнопку **Сохранить настройки**.

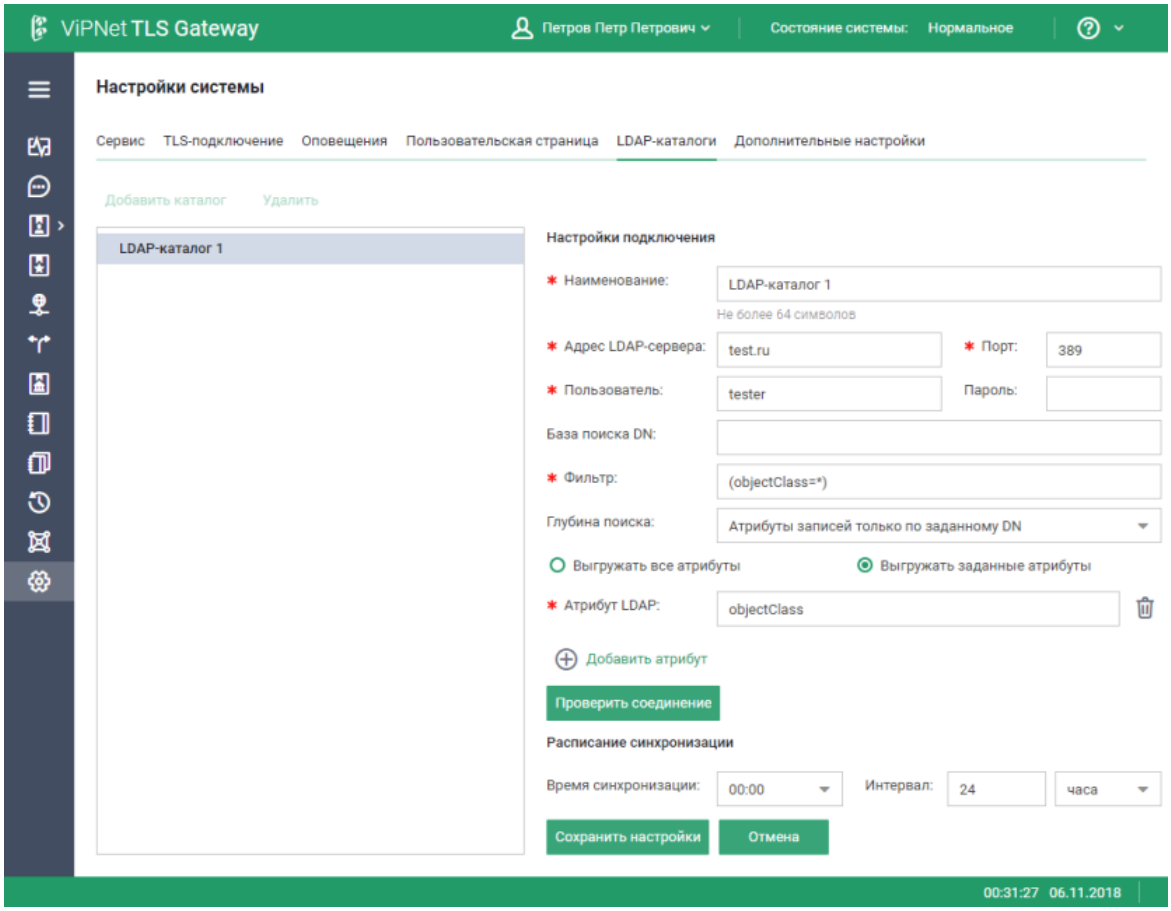

Рисунок 24. Добавление LDAP-каталога

В результате LDAP-каталог будет добавлен в настройки ViPNet TLS Gateway.

Синхронизация LDAP-каталога

Чтобы после добавления LDAP-каталога его данные можно было использовать при создании правил предоставления доступа к ресурсам, синхронизируйте данные о пользователях, хранящиеся на ViPNet TLS Gateway, с LDAP-каталогом. Для этого:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **LDAP-каталоги** и в списке выберите каталог, который хотите синхронизировать.

4 В разделе **Расписание синхронизации** нажмите кнопку **Синхронизировать**.

В результате данные о пользователях будут синхронизированы с LDAP-каталогом и вы сможете их использовать при создании правил предоставления доступа к ресурсам (см. Создание правила предоставления доступа пользователю к заданным ресурсам на стр. 112).

Удаление LDAP-каталога

Вы можете удалить LDAP-каталог, добавленный в ViPNet TLS Gateway, например, если он не используется.

Вы можете удалить только те LDAP-каталоги, которые не связаны ни с одним правилом предоставления доступа.

Чтобы удалить LDAP-каталог, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **LDAP-каталоги**.

4 В списке выберите LDAP-каталог, нажмите кнопку **Удалить** и подтвердите свое действие.

В результате LDAP-каталог будет удален из настроек ViPNet TLS Gateway.

Создание правила предоставления доступа пользователю к заданным ресурсам

Вы можете создать правило предоставления защищенного доступа, при выполнении которого пользователю будет разрешен или запрещен доступ к ресурсам, настроенным в этом правиле. Для создания правила предоставления доступа выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Правила предоставления доступа**.

3 На панели инструментов страницы **Правила предоставления доступа** нажмите кнопку **Добавить правило**.

4 В мастере **Создание правила предоставления доступа** на первой странице в соответствующих полях настройте следующие параметры:

- Укажите наименование правила, под которым правило будет отображаться в списке правил.
- В списке **Действие с сертификатом** выберите значение **Зарегистрировать сертификат пользователя**.
- Если вы хотите связать правило с данными из службы каталогов Active Directory, установите соответствующий флажок и в списке **LDAP-каталог для связи с правилом** выберите нужный LDAP-каталог.
- Нажмите кнопку **Далее**.

5 На второй странице мастера задайте условия выполнения правила (см. Задание условий выполнения правила на стр. 113) и нажмите кнопку **Далее**.

6 На следующей странице мастера назначьте права доступа к необходимым ресурсам. Для каждого ресурса выполните одно из следующих действий:

- Для разрешения доступа пользователя к ресурсу справа от названия ресурса щелкните кнопку **Разрешить**. Ресурс будет помечен как доступный.
- Для запрещения доступа пользователя к ресурсу справа от названия ресурса щелкните кнопку **Блокировать**. Ресурс будет помечен как блокированный.

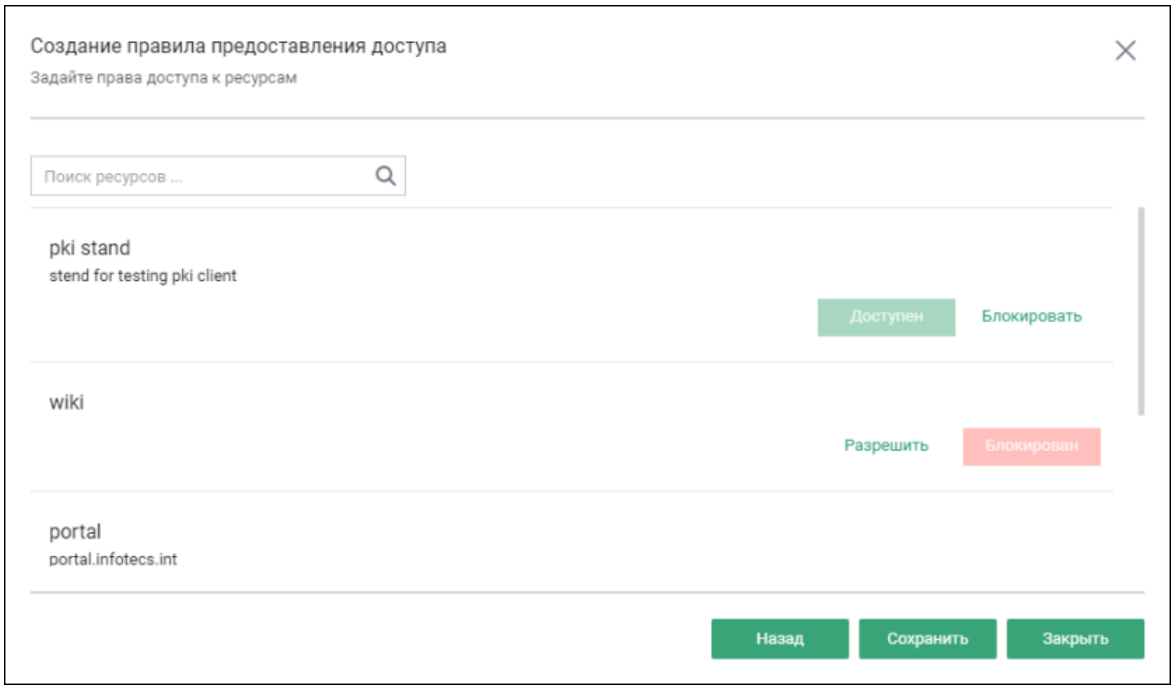

Рисунок 25. Назначение прав доступа к ресурсам

7 Нажмите кнопку **Сохранить**.

В результате созданное правило будет добавлено на страницу **Правила предоставления доступа** в конец списка правил и будет применяться последним. Вы можете изменить порядок применения правил (см. Просмотр, редактирование и настройка порядка применения правил доступа на стр. 118).

При срабатывании правила сертификат пользователя будет добавлен на ViPNet TLS Gateway в список разрешенных сертификатов (отобразится в разделе **Сертификаты пользователей** > **Разрешенные**). Сертификат будет переведен в режим **Доступ к ресурсам определяется правилом <название правила>** (см. Режимы доступа сертификатов пользователей на стр. 101). Пользователю будет разрешен защищенный доступ по каналу TLS с двусторонней аутентификацией к тем ресурсам, которые настроены в правиле.

Задание условий выполнения правила

Примечание. Описание приведено на примере задания условий выполнения правила, не связанного с LDAP-каталогом. Задание условий выполнения правила, связанного с LDAP-каталогом, осуществляется аналогично.

Вы можете задать условия выполнения правила предоставления доступа с помощью конструктора. Для этого на странице задания условий выполнения правила произведите следующие действия:

1. В списке **Поле сертификата** выберите поле сертификата, для которого вы хотите задать условие.
2. В следующем списке выберите оператор условия для анализа полей сертификата. Вы можете использовать следующие операторы:
   - == (равно);
   - <> (не равно);
   - `Regexp` (использовать регулярное выражение PostgreSQL https://www.postgresql.org/docs/current/static/functions-matching.html#FUNCTIONS-POSIX-REGEXP).

   Примечание. Оператор `Regexp` недоступен, если правило предоставления доступа связано с LDAP-каталогом.

3. В следующем поле введите значение поля сертификата, выбранного в первом списке, при котором будет срабатывать условие.
4. Чтобы добавить новое условие, нажмите кнопку **Добавить условие**. Чтобы удалить условие, нажмите кнопку **Удалить условие** напротив нужного условия.

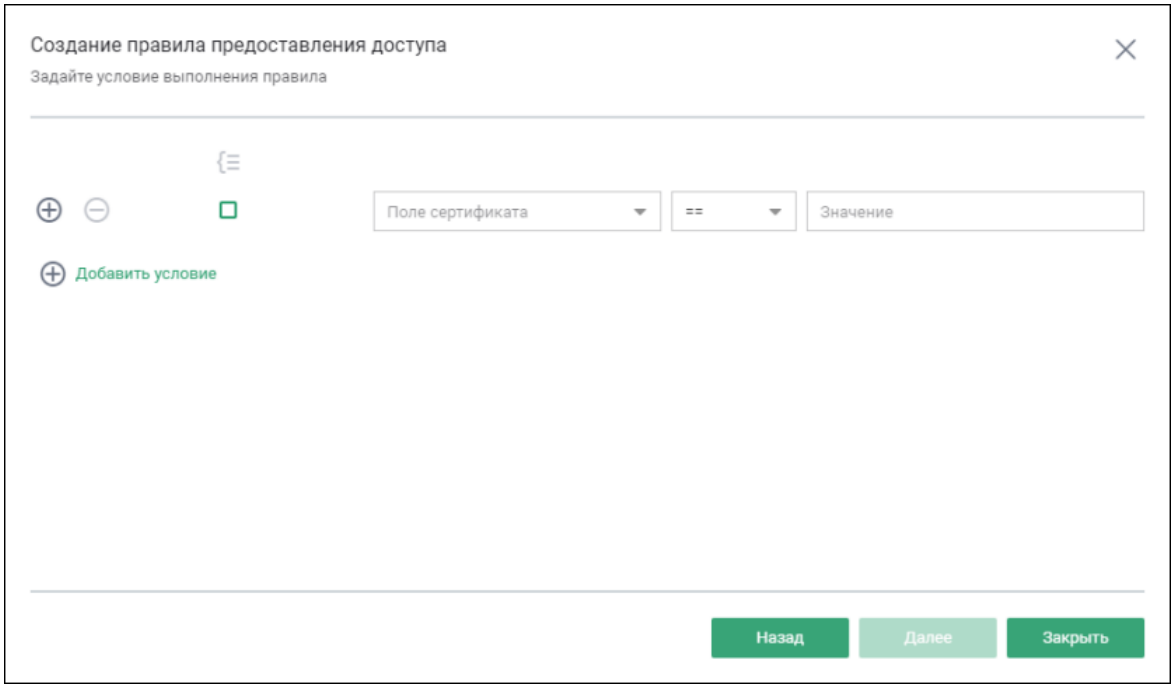

Рисунок 26. Задание условий выполнения правила предоставления доступа пользователям

5 В списке между двумя условиями выберите логический оператор, которым они будут объединены (**И**, **ИЛИ**).

6 Чтобы сгруппировать несколько условий, установите флажки напротив нужных условий и нажмите кнопку . При необходимости в списке между условиями измените логический оператор, которым они будут объединены. Чтобы разгруппировать условия, нажмите кнопку рядом с ними.

Группирование позволяет установить порядок проверки заданных условий. Вы можете группировать условия, группы или группы и условия.

Внимание! Группа может содержать не более двух вложенных групп. Группы не могут пересекаться между собой.

В пределах одной группы оператор **И** имеет больший приоритет, чем оператор **ИЛИ**. Операторы, имеющие одинаковый приоритет в рамках одной группы, применяются последовательно в порядке следования на странице задания условий. Таким образом если в пределах одной группы будет объединено несколько условий с разными логическими операторами, то сначала последовательно будут применены все условия, объединенные оператором **И**, а затем последовательно применятся все операторы, объединенные оператором **ИЛИ**.

Несгруппированные условия проверяются в порядке следования на странице задания условий.

Рассмотрим пример настройки условий выполнения правила для автоматической регистрации сертификатов квалифицированной электронной подписи (с заполненным полем `СНИЛС`), выданных УЦ "Infotecs" для организации "Организация 1" и "УЦ Infotecs-Trust" для организации "Организация 2". Для настройки условий нужно выполнить следующие действия:

1. Добавить условие "поле Issuer.CN равно Infotecs": `Издатель.Наименование == Infotecs`.

2. Добавить условие "поле Subject.O равно Организация 1": `Владелец.Организация == Организация 1`.

3. Сгруппировать условия 1 и 2, используя оператор **И**.

4. Добавить условие "поле Issuer.CN равно Infotecs-Trust": `Издатель.Наименование == Infotecs-Trust`.

5. Добавить условие "поле Subject.O равно Организация 2": `Владелец.Организация == Организация 2`.

6. Сгруппировать условия 4 и 5, используя оператор **И**.

7. Добавить условие "поле СНИЛС соответствует регулярному выражению **.+** (поле содержит хотя бы один символ): `Владелец.СНИЛС владельца Regexp .+`.

8. Объединить группы 3 и 6, используя оператор **ИЛИ**.

9. Объединить группу 8 и условие 7, используя оператор **И**.

В результате в окне задания условий отобразятся следующие условия выполнения правила (см. рисунок ниже), при выполнении которых сертификат пользователя будет зарегистрирован в ViPNet TLS Gateway (заблокирован или разрешен в зависимости от указанного в правиле действия с сертификатом).

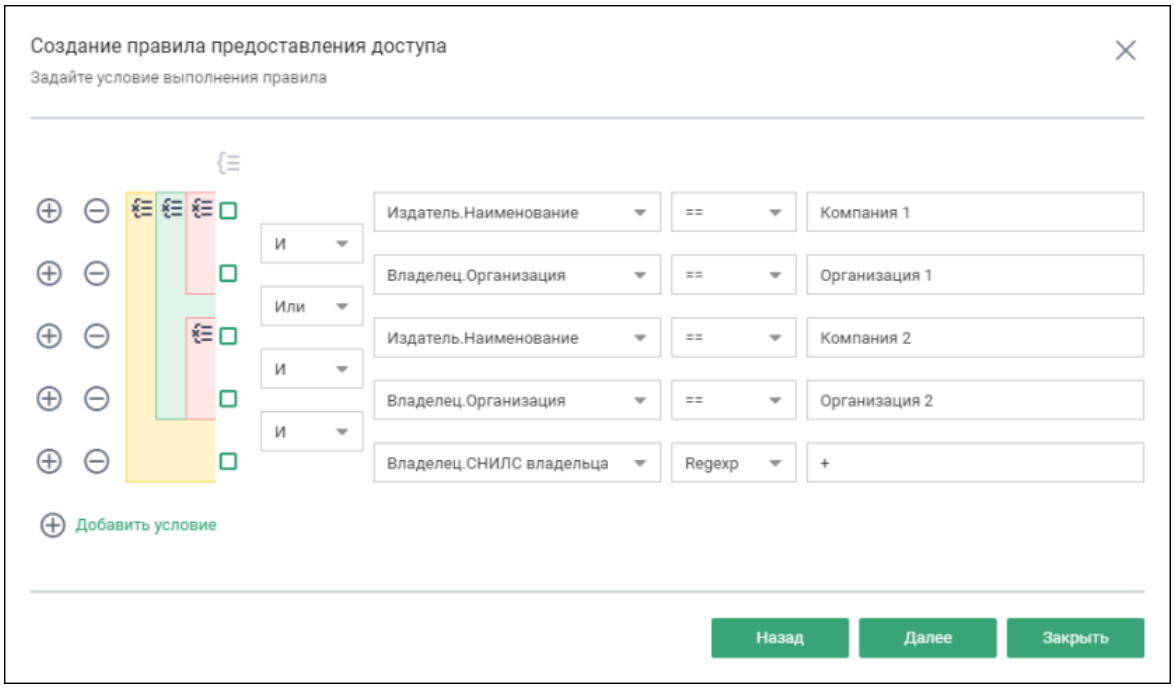

Рисунок 27. Пример задания условий выполнения правила для автоматической регистрации сертификатов

Создание правила блокировки доступа пользователю к ViPNet TLS Gateway и ко всем ресурсам

Вы можете создать правило блокировки доступа, при выполнении которого пользователю будет запрещен доступ к ViPNet TLS Gateway и ко всем ресурсам, заданным на ViPNet TLS Gateway. Для создания правила блокировки доступа выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Перейдите в раздел **Правила предоставления доступа**.
3. На панели инструментов страницы **Правила предоставления доступа** нажмите кнопку **Добавить правило**.
4. В мастере **Создание правила предоставления доступа** на первой странице в соответствующих полях настройте следующие параметры:
   - Укажите наименование правила, под которым правило будет отображаться в списке правил.
   - В списке **Действие с сертификатом** выберите значение **Заблокировать сертификат пользователя**.
   - Если вы хотите связать правило с данными из службы каталогов Active Directory, установите соответствующий флажок и в списке **LDAP-каталог для связи с правилом** выберите нужный LDAP-каталог.
5. Нажмите кнопку **Далее**.
6. На следующей странице мастера задайте условия выполнения правила (см. Задание условий выполнения правила на стр. 113).
7. Нажмите кнопку **Сохранить**.

В результате созданное правило будет добавлено на страницу **Правила предоставления доступа** в конец списка правил и будет применяться последним. Вы можете изменить порядок применения правил (см. Просмотр, редактирование и настройка порядка применения правил доступа на стр. 118).

При срабатывании правила сертификат пользователя будет добавлен на ViPNet TLS Gateway в список заблокированных (отобразится в разделе **Сертификаты пользователей** > **Блокированные**). Сертификат будет переведен в режим **Заблокирован правилом <название правила>** (см. Режимы доступа сертификатов пользователей на стр. 101). Пользователю будет запрещен защищенный доступ к ViPNet TLS Gateway и ко всем ресурсам, параметры доступа к которым настроены на ViPNet TLS Gateway (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109). При попытке пользователя подключиться к ViPNet TLS Gateway или какому-либо ресурсу по каналу TLS с двусторонней аутентификацией на экране пользователя появится страница с информацией о запрете доступа и адресом электронной почты администратора для связи.

Просмотр, редактирование и настройка порядка применения правил доступа

Вы можете просмотреть созданные правила доступа, при необходимости отредактировать параметры правил и настроить порядок применения правил к сертификатам пользователей, приславшим запросы на доступ к ресурсам. Для этого выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Правила предоставления доступа**.

3 На странице **Правила предоставления доступа** выполните следующие действия:

3.1 Просмотрите созданные правила. Выберите правило и на панели дополнительных сведений о правиле отобразится детальная информация об условиях выполнения правила и настроенных правах доступа к ресурсам.

3.2 При необходимости отредактируйте выбранное правило. Для этого на панели дополнительных сведений о правиле нажмите кнопку **Редактировать** и в окне **Редактирование правила** измените параметры правила таким же образом, как и при создании правил предоставления доступа (см. Создание правила предоставления доступа пользователю к заданным ресурсам на стр. 112) или блокировки доступа (см. Создание правила блокировки доступа пользователю к ViPNet TLS Gateway и ко всем ресурсам на стр. 117).

3.3 Настройте порядок применения правил. Все правила применяются сверху вниз согласно порядковому номеру, отображаемому в столбце **Порядок**. Для изменения порядка применения правил выберите правило и переместите его на требуемое место, нажимая на панели дополнительных сведений кнопки со стрелками **Поднять приоритет**, **Понизить приоритет**.

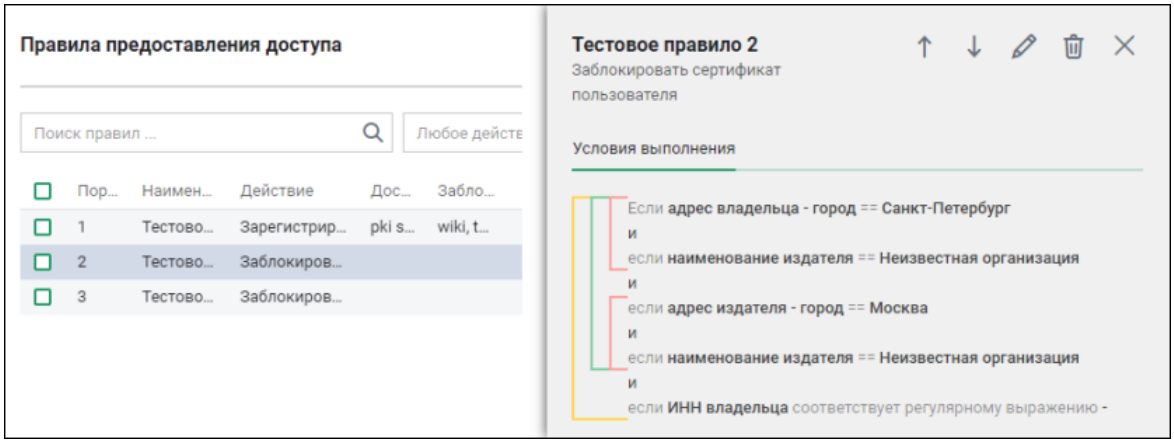

Рисунок 28. Настройка порядка применения правил доступа

В результате правила будут применяться к сертификатам согласно новому порядку.

Удаление правила доступа

Если правило предоставления доступа утратило свою актуальность, вы можете его удалить. Для этого выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Правила предоставления доступа**.

3 На странице **Правила предоставления доступа** выберите нужное правило и на панели дополнительных сведений нажмите кнопку **Удалить правило**.

Примечание. Вы можете удалить сразу несколько правил, для этого установите флажки напротив нужных правил и на панели инструментов страницы **Правила предоставления доступа** нажмите кнопку **Удалить правила**.

---

4 В появившемся окне подтвердите удаление правила.

В результате правило предоставления доступа более не будет использоваться и удалится с ViPNet TLS Gateway.

Изменение прав доступа к ресурсам существующего пользователя

Вы можете заблокировать защищенный доступ пользователя к ранее разрешенному для него ресурсу, а также наоборот, разрешить защищенный доступ пользователя к ранее заблокированному ресурсу. Также при необходимости вы можете заблокировать доступ пользователя к ViPNet TLS Gateway и ко всем защищаемым ресурсам, например, для временного прекращения обслуживания пользователя или применить к сертификату пользователю правила автоматического предоставления доступа.

После первоначальной настройки прав доступа пользователей к ресурсам вы можете:

- Изменить права доступа пользователей к ресурсам вручную (см. Изменение прав доступа к ресурсам вручную на стр. 120).
- Применить к сертификатам пользователей правила автоматического предоставления доступа (см. Применение правил автоматического предоставления доступа на стр. 121).
- Возобновить доступ пользователей к ViPNet TLS Gateway (см. Возобновление доступа пользователя к ViPNet TLS Gateway и к ранее запрещенным ресурсам на стр. 123).

Изменение прав доступа к ресурсам вручную

Чтобы изменить права доступа пользователя к защищаемым ресурсам, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Сертификаты пользователей** > **Разрешенные**.

3 На странице **Сертификаты пользователей, которым разрешено подключение по TLS-протоколу** выберите один или несколько сертификатов пользователей. В зависимости от количества выбранных сертификатов выполните одно из следующих действий:

- Для изменения прав доступа к ресурсам одного пользователя на панели дополнительных сведений о запросе выберите вкладку **Ресурсы** и назначьте права доступа пользователя к ресурсам, выполнив одно из следующих действий:
  - Чтобы разрешить или запретить доступ пользователя к необходимым ресурсам, справа от названия ресурса нажмите кнопку **Разрешить** или **Блокировать**.
  - Для полного запрета пользователю доступа к ViPNet TLS Gateway и ко всем защищаемым ресурсам на панели дополнительных сведений нажмите кнопку **Блокировать доступ** и подтвердите блокировку сертификата в окне подтверждения.

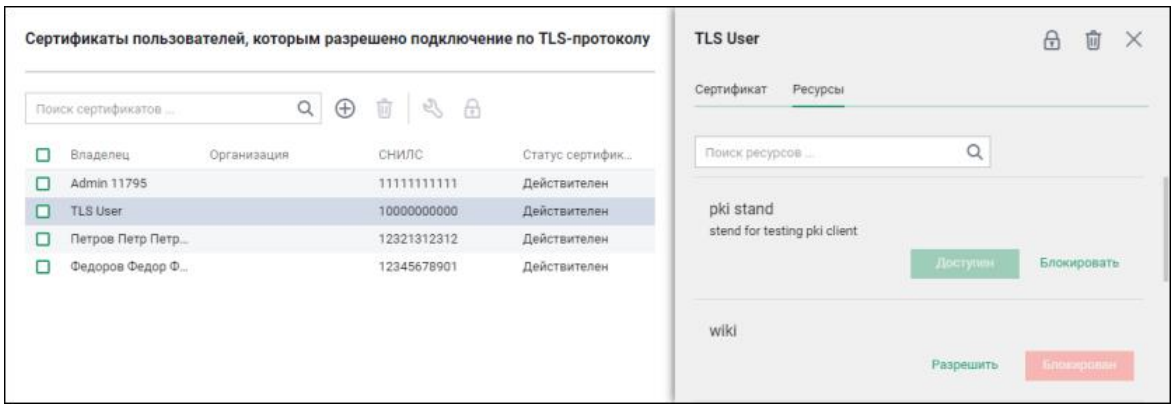

Рисунок 29. Изменение прав доступа к ресурсам для одного сертификата пользователя

- Для изменения прав доступа нескольких выбранных сертификатов пользователей на панели инструментов страницы **Сертификаты пользователей, которым разрешено подключение по TLS-протоколу** выполните одно из следующих действий:
  - Чтобы разрешить или запретить доступ пользователей к необходимым ресурсам, нажмите кнопку **Настроить доступ к ресурсу**, выберите пункт **Разрешить доступ** или **Блокировать доступ** и далее название ресурса.
  - Для полного запрета выбранным пользователям доступа к ViPNet TLS Gateway и ко всем ресурсам на панели дополнительных сведений нажмите кнопку **Блокировать доступ** и подтвердите блокировку сертификатов в окне подтверждения.

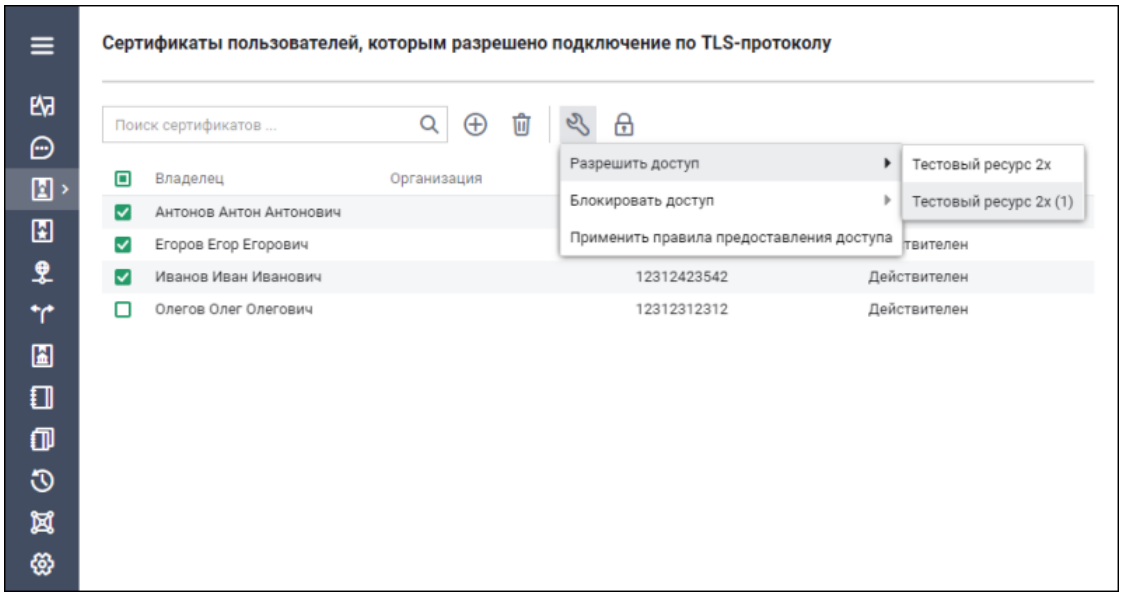

Рисунок 30. Изменение прав доступа к ресурсам для нескольких сертификатов пользователей

В результате права доступа пользователей к ресурсам будут изменены в соответствии с новыми настройками. Сертификаты пользователей будут переведены в режим **Доступ к ресурсам определяется администратором** (см. Режимы доступа сертификатов пользователей на стр. 101).

При блокировке доступа к ViPNet TLS Gateway и ко всем защищаемым ресурсам сертификаты пользователей будут перемещены в раздел **Сертификаты пользователей** > **Блокированные**, доступ пользователей будет заблокирован, при этом сохранятся все настройки для конкретных ресурсов, ранее заданные для пользователей. Сертификаты будут переведены в режим **Заблокирован администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). При возобновлении доступа к ViPNet TLS Gateway вам не нужно будет перенастраивать права доступа к этим ресурсам.

Применение правил автоматического предоставления доступа

Чтобы применить к сертификату пользователя правила автоматического предоставления доступа к ресурсам, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Сертификаты пользователей** > **Разрешенные**.

3 На странице **Сертификаты пользователей, которым разрешено подключение по TLS-протоколу** выберите один или несколько сертификатов пользователей. В зависимости от количества выбранных сертификатов выполните одно из следующих действий:

- Чтобы применить правила автоматического предоставления доступа к одному сертификату пользователя, на панели дополнительных сведений нажмите кнопку **Применить правила предоставления доступа**.

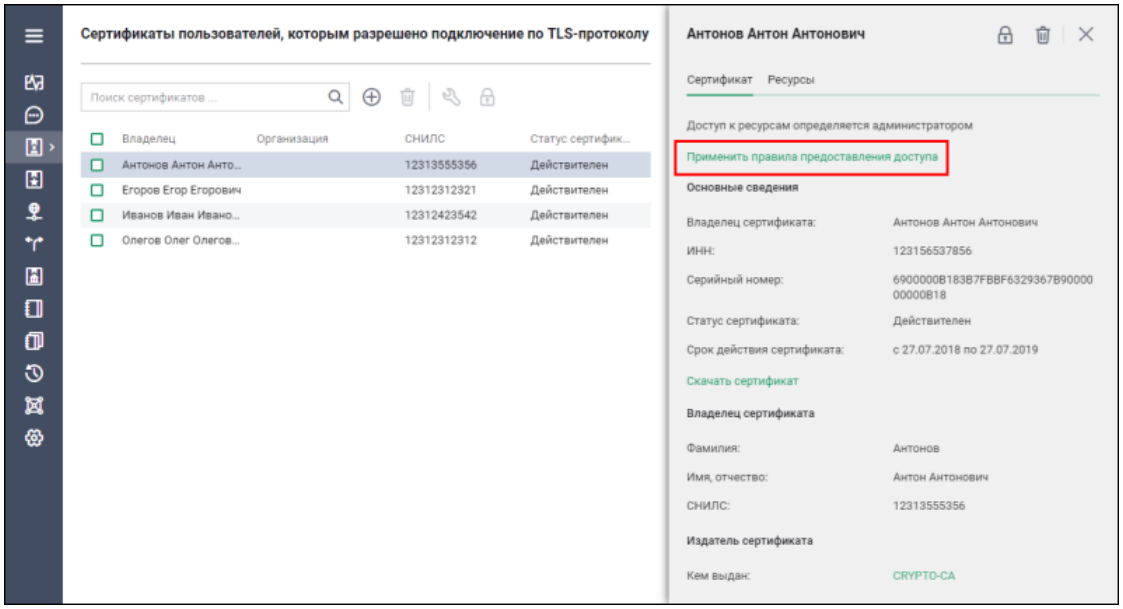

Рисунок 31. Применение правил автоматического предоставления доступа к одному сертификату пользователя

- Чтобы применить правила автоматического предоставления доступа к нескольким выбранным сертификатам пользователей на панели инструментов страницы **Сертификаты пользователей, которым разрешено подключение по TLS-протоколу** нажмите кнопку **Настроить доступ к ресурсу** и выберите пункт **Применить правила предоставления доступа**.

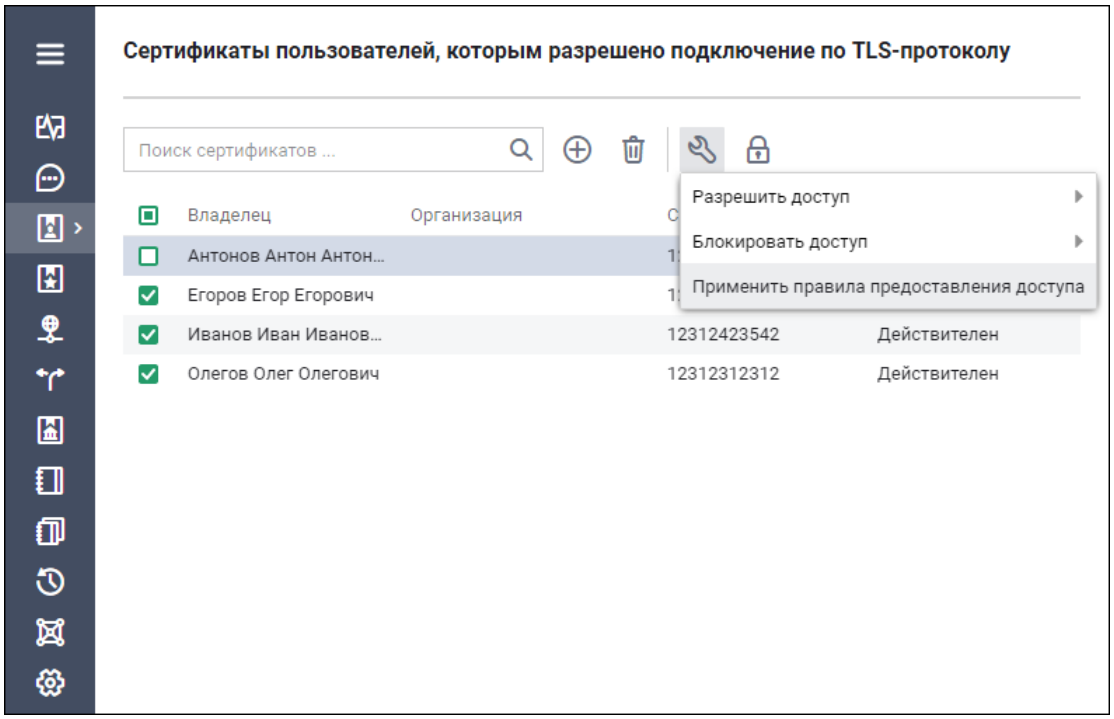

Рисунок 32. Применение правил автоматического предоставления доступа к нескольким сертификатам пользователей

В результате права доступа пользователей к ресурсам будут изменены в соответствии с настроенными правилами. Сертификаты пользователей, к которым применились правила доступа, будут переведены в режим **Доступ к ресурсам определяется правилом <название правила>**.

Если к сертификату пользователю неприменимо ни одно из настроенных правил доступа, он будет переведен в режим **К данному сертификату неприменимо ни одно из настроенных правил, доступ к ресурсам не определен** (см. Режимы доступа сертификатов пользователей на стр. 101).

При блокировке доступа к ViPNet TLS Gateway и ко всем защищаемым ресурсам сертификаты пользователей будут перемещены в раздел **Сертификаты пользователей** > **Блокированные**, доступ пользователей будет заблокирован. Сертификаты будут переведены в режим **Заблокирован правилом <название правила>** (см. Режимы доступа сертификатов пользователей на стр. 101).

Возобновление доступа пользователя к ViPNet TLS Gateway и к ранее запрещенным ресурсам

Вы можете возобновить защищенный доступ к ViPNet TLS Gateway и к защищаемым ресурсам пользователям, которым вы или правила автоматического предоставления доступа временно запрещали этот доступ. Для возобновления защищенного доступа пользователя выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Перейдите в раздел **Сертификаты пользователей** > **Блокированные**.
3. На странице **Сертификаты пользователей, которым запрещено подключение по TLS-протоколу** выберите один или несколько сертификатов пользователей, для которых вы хотите возобновить доступ к ресурсам, щелкнув строку с нужным сертификатом или установив флажки напротив нужных сертификатов соответственно. В зависимости от количества выбранных сертификатов выполните одно из следующих действий:
   - Чтобы возобновить доступ к ViPNet TLS Gateway и к ресурсам одному пользователю, на панели дополнительных сведений нажмите кнопку **Разрешить доступ**.
   - Чтобы возобновить доступ к ViPNet TLS Gateway и к ресурсам сразу нескольким пользователям, на панели инструментов страницы **Сертификаты пользователей, которым запрещено подключение по TLS-протоколу** нажмите кнопку **Разрешить доступ**.

В результате защищенный доступ пользователей к защищаемым ресурсам будет восстановлен в соответствии с ранее заданными настройками прав доступа к ресурсам. Сертификаты пользователей будут переведены в режим **Доступ к ресурсам определяется администратором** (см. Режимы доступа сертификатов пользователей на стр. 101). Пользователи при подключении по каналу TLS с двусторонней аутентификацией смогут получить доступ к разрешенным ресурсам и запросить доступ к тем ресурсам, на которые права доступа еще не назначались.

Изменение версии протокола TLS для подключения пользователей

Версии протокола TLS для подключения пользователей задаются в процессе первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). При необходимости вы можете их изменить.

Изменение версии протокола TLS для подключения пользователей производится администратором безопасности (см. Администратор безопасности на стр. 35).

Внимание! Изменение версии протокола TLS может привести к потере удаленного доступа. Также будут разорваны все соединения, для которых вы изменили версию протокола TLS.

Перед сохранением убедитесь, что криптопровайдер, установленный на компьютерах пользователей, поддерживает выбранные версии протокола TLS.

Чтобы изменить версию протокола TLS для подключения пользователей, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Система**.
3. На странице **Настройки системы** перейдите на вкладку **TLS-подключение**.
4. В группе **Версия протокола TLS** в соответствующем списке выберите нужные версии протокола TLS.
5. Нажмите кнопку **Сохранить**.

В результате для подключения пользователей будут использоваться выбранные версии протокола TLS.

Просмотр данных о пользователях и их сертификатах

Вы можете просматривать данные пользователей, сертификаты которых добавлены на ViPNet TLS Gateway, например, чтобы проверить сроки действия сертификатов или посмотреть, на какие ресурсы разрешен доступ пользователю. Вы можете просматривать данные о пользователях, которым разрешен защищенный доступ к каким-либо ресурсам и о пользователях, которым доступ ко всем ресурсам запрещен. Чтобы просмотреть данные о пользователях, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора.

2 Перейдите в раздел **Сертификаты пользователей** > **Разрешенные** (для просмотра данных о пользователях, которым разрешен доступ к каким-либо ресурсам) или **Сертификаты пользователей** > **Блокированные** (для просмотра данных о пользователях, которым доступ ко всем ресурсам заблокирован).

3 На странице **Сертификаты пользователей** выберите нужный сертификат.

4 Чтобы просмотреть информацию о правах доступа к ресурсам, на панели дополнительных сведений о пользователе перейдите на вкладку **Ресурсы**.

Примечание. При наличии прав администратора доступа вы сможете изменить права доступа к ресурсам (см. Изменение прав доступа к ресурсам существующего пользователя на стр. 119).

---

5 Чтобы просмотреть краткую информацию о сертификате, на панели дополнительных сведений о пользователе перейдите на вкладку **Сертификат**.

6 При необходимости подробнее посмотреть параметры сертификата, на панели дополнительных сведений о пользователе щелкните ссылку **Скачать сертификат** и укажите место сохранения сертификата. После подтверждения сертификат будет сохранен в файл формата CER на вашем компьютере. Вы можете открыть файл и просмотреть сертификат пользователя.

7 Для просмотра сертификата УЦ, издавшего сертификат пользователя, на панели дополнительных сведений в строке **Кем выдан** щелкните ссылку с именем издателя сертификата. Откроется раздел **Сертификаты удостоверяющих центров** с информацией о сертификате УЦ.

6

Управление и настройка ViPNet TLS Gateway

Управление и настройка с помощью веб-интерфейса 127

Управление с помощью консоли Linux 154

Управление и настройка с помощью веб-интерфейса

Работа с журналом событий

Все действия, производимые администраторами в ViPNet TLS Gateway, фиксируются в журнале событий. Журнал может просматривать (см. Просмотр журнала событий на стр. 127) администратор безопасности, администратор доступа или аудитор.

В журнале регистрируются следующие категории событий:

- Авторизация — события авторизации пользователей в интерфейсе управления.
- Редактирование доступа — события управления доступом администраторов и пользователей.
- Ресурсы — события управления защищаемыми ресурсами.
- Настройки — события настройки ViPNet TLS Gateway.
- Ключи — события управления транспортными ключами и сертификатами.
- Сертификаты УЦ — события управления доверенными сертификатами удостоверяющих центров и CRL.
- Резервное копирование — события работы с резервными копиями.
- Система — системные события.
- Лицензирование — события, связанные с лицензиями.
- Аудит — действия с журналом событий (аудита).
- Обновление ПО — события, связанные с обновлением ПО ViPNet TLS Gateway.
- WAF — включение и выключение модуля WAF (только для исполнения TLS 1000 с модулем WAF).
- LDAP-каталоги — добавление, удаление и синхронизация LDAP-каталогов.
- Общие события — другие события.

Один раз в месяц выполняется автоматическая архивация журналов. В процессе архивации старые записи журнала (старше 30 дней от текущей даты) переносятся из основного журнала в архив. Аудитор может просматривать и скачивать архивы журналов (см. Выгрузка архива журнала событий в файл на стр. 128).

Просмотр журнала событий

Чтобы просмотреть журнал событий, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора.

2 Перейдите в раздел **Журнал событий**.

3 На странице **Журнал событий** просмотрите информацию о событиях.

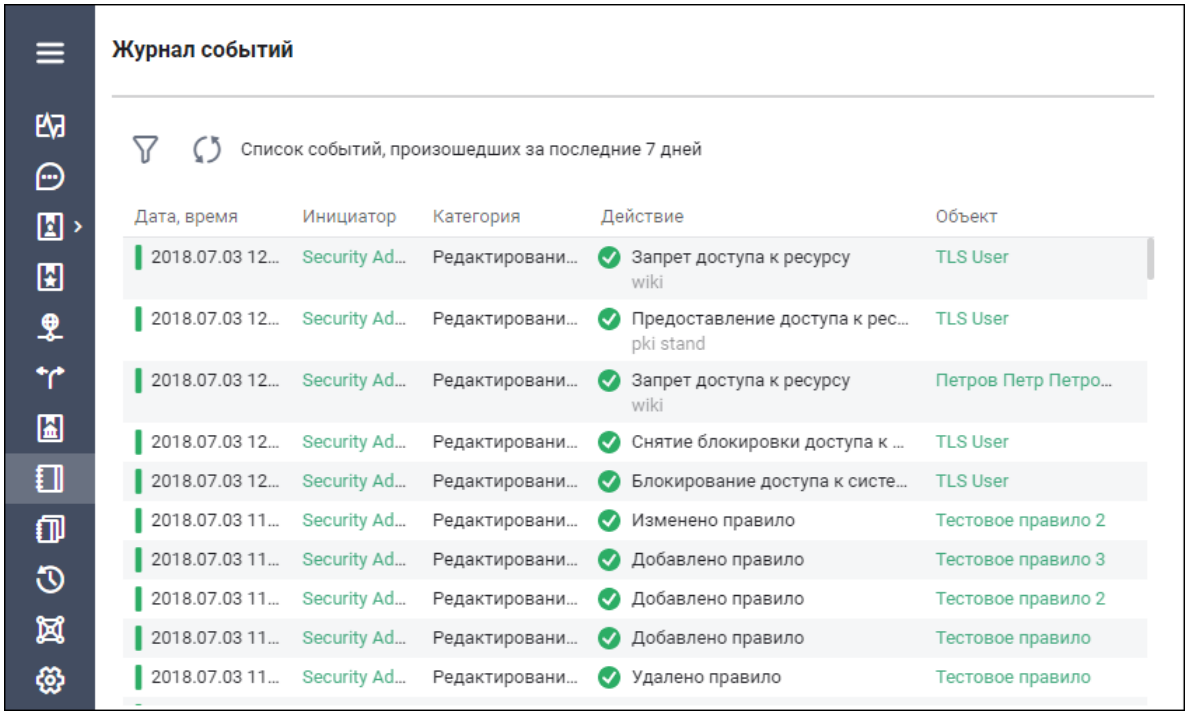

Рисунок 33. Просмотр журнала событий

По умолчанию отображаются записи журнала о всех зарегистрированных событиях за последнюю неделю. Для поиска событий за другой период времени, вы можете воспользоваться фильтром поиска , расположенным на панели задач.

События обозначены зеленым, желтым или красным цветом в зависимости от их важности (см. Уровни важности событий на стр. 130). Также все события, в зависимости от успешности или неуспешности действий, в результате которых они зафиксированы, отмечены следующим значками в столбце **Действие**:

- — действие выполнено успешно;
- — при выполнении действия произошла ошибка.

Выгрузка архива журнала событий в файл

Аудитор может искать и скачивать архивы журналов, например, если требуется просмотреть информацию из журналов ViPNet TLS Gateway старше 30 дней.

Чтобы просмотреть и выгрузить архив журнала в файл, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями аудитора.

2 Перейдите в раздел **Архивы журналов**.

3 На странице **Архивы журналов** выберите архив, щелкнув строку с нужным архивом, и на панели дополнительных сведений об архиве нажмите кнопку **Скачать**.

4 Задайте пароль для защиты архива и нажмите кнопку **Скачать архив**.

Примечание. Пароль должен содержать не менее восьми символов.

---

5 Укажите место сохранения архива.

В результате выбранный архив журналов будет сохранен в файле указанном месте. Информацию из архива с журналом можно просмотреть с помощью стороннего программного обеспечения.

Мониторинг работоспособности

Для обеспечения бесперебойной работы, а также для быстрого выявления нештатных ситуаций, в ViPNet TLS Gateway реализованы механизмы контроля различных параметров работы. Вы можете осуществлять мониторинг работы ViPNet TLS Gateway, а именно:

- Отслеживать оповещения о состоянии ViPNet TLS Gateway (см. Оповещение о состоянии ViPNet TLS Gateway на стр. 130).
- Просматривать отчеты о состоянии работы ViPNet TLS Gateway и количестве запросов на подключение для каждого ресурса (см. Просмотр отчетов мониторинга на стр. 131).
- Настроить передачу данных о работоспособности ViPNet TLS Gateway в систему управления событиями информационной безопасности (см. Настройка передачи данных в формате CEF на стр. 132).
- Запускать процедуру самотестирования (см. Самотестирование на стр. 133).
- Создавать архив служебных журналов для диагностики работы ViPNet TLS Gateway (см. Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway на стр. 133).

Мониторинг доступен любому администратору, но данные мониторинга (в том числе журнала событий), которые сможет увидеть администратор, зависят от его роли.

Данные мониторинга помогут вам оперативно разобраться с причиной возникновения тех или иных событий, а при возникновении неполадок — предпринять действия по их устранению.

Уровни важности событий

В ViPNet TLS Gateway регистрируются события, которые происходят в процессе работы (см. Просмотр журнала событий на стр. 127). События разделены на несколько уровней важности. По уровню важности событий можно оценить, в каком состоянии находится ViPNet TLS Gateway, и насколько серьезна выявленная проблема. Информация о важности событий отображается в веб-интерфейсе (в журнале событий, разделе мониторинга и оповещениях) различными цветами. Выделяются следующие уровни событий:

- Высокий уровень (красный цвет) — наиболее важные и критичные события. Выявлены серьезные проблемы, требующие немедленного вмешательства. ViPNet TLS Gateway находится в критическом состоянии, работоспособность его нарушена.
- Средний уровень (желтый цвет) — ViPNet TLS Gateway находится в опасном состоянии. Выявлены проблемы, не требующие немедленного вмешательства. Однако если данные проблемы не решить в ближайшем будущем, они могут нарушить работоспособность ViPNet TLS Gateway.
- Информационное событие (зеленый цвет) — события, носящие уведомительный характер. ViPNet TLS Gateway находится в нормальном состоянии и работает в штатном режиме.

Оповещение о состоянии ViPNet TLS Gateway

О наличии проблем в работе ViPNet TLS Gateway вы всегда можете узнать по индикатору работоспособности, расположенному на панели заголовка веб-интерфейса ViPNet TLS Gateway (см. Веб-интерфейс ViPNet TLS Gateway на стр. 70) и видимом на любой странице веб-интерфейса. Щелкнув индикатор, вы увидите сводную информацию о состоянии ViPNet TLS Gateway (см. Просмотр отчетов мониторинга на стр. 131), которая позволит вам быстро оценить существующие проблемы работоспособности.

Чтобы посмотреть информацию о состоянии ViPNet TLS Gateway, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора.
2. Посмотрите на индикатор работоспособности **Состояние системы**, расположенный на панели заголовка. Индикатор работоспособности в зависимости от важности проблемы (см. Уровни важности событий на стр. 130) может отображать следующие состояния:
   - Критическое.
   - Опасное.
   - Нормальное.

Для просмотра детальной информации щелкните индикатор работоспособности или перейдите в раздел **Мониторинг** (см. Просмотр отчетов мониторинга на стр. 131).

Просмотр отчетов мониторинга

В процессе работы ViPNet TLS Gateway осуществляется мониторинг своего состояния и состояния модуля Web Application Firewall (для исполнения TLS 1000 с модулем WAF), а также отслеживается количество необработанных запросов от пользователей на предоставление доступа к каждому защищаемому ресурсу. По результатам мониторинга формируются отчеты с детальной информацией.

Чтобы посмотреть отчеты мониторинга, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора для просмотра отчетов мониторинга ViPNet TLS Gateway или с полномочиями администратора доступа для просмотра отчетов мониторинга модуля WAF.

2 Щелкните индикатор работоспособности (см. Оповещение о состоянии ViPNet TLS Gateway на стр. 130) или перейдите в раздел **Мониторинг**.

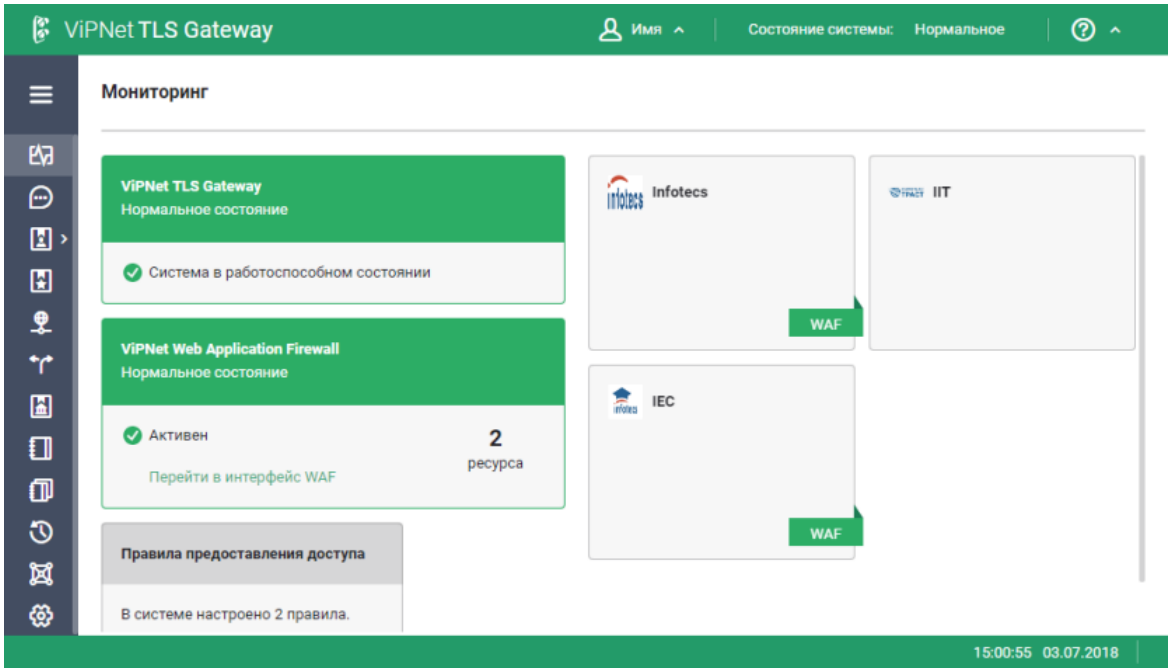

Рисунок 34. Просмотр отчета мониторинга

3 Просмотрите представленную информацию о ViPNet TLS Gateway и информацию о модуле WAF (для исполнения TLS 1000 с модулем WAF). Состояния отображаются блоками **ViPNet TLS Gateway** и **ViPNet Web Application Firewall** определенного цвета в зависимости от уровня важности событий (см. Уровни важности событий на стр. 130), вызвавших это состояние.

Примечание. Блок **ViPNet Web Application Firewall** отображается только если вы используете исполнение TLS 1000 с модулем WAF и подключились к ViPNet TLS Gateway с полномочиями администратора доступа.

При наличии проблем в работоспособности будут отображены события, в результате которых возникли эти проблемы, а также для некоторых событий будут указаны причины их

возникновения. Если причин возникновения события более пяти, будет отображено только количество таких причин. Для просмотра детального списка причин возникновения события вы можете в блоке с названием события нажать кнопку **Подробнее** и перейти в журнал событий (см. Просмотр журнала событий на стр. 127). Для решения некоторых проблем вы можете в блоке с названием события нажать кнопку **Исправить** и выполнить предлагаемое действие. Например, если для какого-либо УЦ отображается критическая проблема **CRL устарел**, для решения проблемы нажмите ссылку **Исправить** и загрузите новый действительный CRL для указанного УЦ. В результате для данного УЦ проблема с CRL будет устранена.

4 Просмотрите представленную информацию о списке защищаемых ресурсов и количестве имеющихся запросов на доступ к ним.

   При наличии необработанных запросов от пользователей на предоставление доступа к ресурсам вы увидите на плитке ресурса информацию о количестве запросов. Для обработки запросов вы можете щелкнуть ссылку с количеством запросов и обработать запросы (см. Назначение прав доступа к ресурсам по запросу пользователя на стр. 105).

Настройка передачи данных в формате CEF

Вы можете настроить автоматическую отправку данных о работоспособности и лицензионных ограничениях ViPNet TLS Gateway в формате CEF в какую-либо систему управления событиями информационной безопасности (SIEM) (см. глоссарий, стр. 210). Для этого вам нужно включить передачу данных и выполнить настройку принимающего сервера. По умолчанию передача данных в формате CEF выключена.

Чтобы включить и настроить передачу данных в формате CEF, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **Оповещения** и в разделе **Оповещения по CEF** включите переключатель **Использовать автоматическое оповещение по CEF**.

4 В полях **Адрес сервера** укажите IP-адрес и порт принимающего сервера системы SIEM.

5 В поле **Период отправки** укажите период отправки данных на принимающий сервер (в секундах, минутах или часах).

6 Нажмите кнопку **Сохранить**.

В результате будет включена и настроена передача данных о работоспособности и лицензионных ограничениях ViPNet TLS Gateway в формате CEF с заданным периодом на указанный адрес принимающего сервера SIEM. Выполненные настройки не гарантируют получение отправленных данных принимающей стороной.

Описание структуры сообщений и перечня поддерживаемых параметров см. в приложении Описание структуры сообщения в формате CEF (на стр. 191).

Внимание! Если вы отключите передачу данных в формате CEF, настройки принимающего сервера не сохранятся.

Самотестирование

В ViPNet TLS Gateway реализована процедура самотестирования, которая заключается в проверке целостности ПО ViPNet TLS Gateway и контроле корректности его работы. Процедура самотестирования запускается автоматически при запуске ViPNet TLS Gateway и по расписанию один раз в 24 часа. Администратор безопасности и администратор доступа могут запустить процедуру самотестирования вручную посредством веб-интерфейса ViPNet TLS Gateway, например, для регламентной проверки контроля целостности ПО.

Если в процессе самотестирования обнаружен факт нарушения целостности ПО, процедура самотестирования прервется и ViPNet TLS Gateway будет перезагружен. Далее при запуске ViPNet TLS Gateway процедура самотестирования запустится автоматически. В случае повторного обнаружения нарушения целостности ПО работа ViPNet TLS Gateway будет заблокирована. Для восстановления работоспособности ViPNet TLS Gateway воспользуйтесь процедурой восстановления работоспособности и данных после программного сбоя (см. Восстановление ViPNet TLS Gateway после программного сбоя на стр. 167).

Чтобы запустить процедуру самотестирования вручную, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway с полномочиями администратора безопасности или администратора доступа.
2. Перейдите в раздел **Система**.
3. На странице **Настройки системы** откройте вкладку **Сервис** и в разделе **Самотестирование** нажмите кнопку **Выполнить тест**. Запустится процедура самотестирования.

По завершении самотестирования в разделе **Самотестирование** появится сообщение о его успешном выполнении и отобразится дата и время последнего самотестирования. Информация о самотестировании также зафиксируется в журнале событий (см. Просмотр журнала событий на стр. 127).

Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway

В процессе работы ViPNet TLS Gateway ведутся служебные журналы, где сохраняется информация о работе модулей и подсистем ViPNet TLS Gateway. Служебные журналы позволяют диагностировать правильность работы ПО ViPNet TLS Gateway и выявлять неполадки. Если в работе ViPNet TLS Gateway происходят сбои и у вас не получается разобраться с их причиной, вы можете подготовить архив со всеми служебными журналами ViPNet TLS Gateway и передать его специалистам службы технической поддержки ОАО «ИнфоТеКС» для исследования и составления рекомендаций по устранению неполадок функционирования ПО ViPNet TLS Gateway.

Примечание. Если к веб-интерфейсу нет доступа, вы можете сохранить служебные журналы в консоли Linux, подключившись к ViPNet TLS Gateway локально (см. Выгрузка служебных журналов для диагностики работы на стр. 155).

Для подготовки служебных журналов выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями любого администратора.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** откройте вкладку **Сервис** и в разделе **Архив служебных журналов** выполните одно из следующих действий:

- Если архив служебных журналов еще не создавался, нажмите кнопку **Сформировать** и дождитесь создания архива. В названии архива будет отображена его дата и время создания.
- Если архив служебных журналов уже создан, обновите его, нажав кнопку **Переформировать**.

Внимание! Единовременно формирование архивов служебных журналов должен производить один администратор, так как создание архивов одновременно несколькими администраторами может привести к конфликту доступа к файлам с журналами.

4 Сохраните архив служебных журналов в файле. Для этого нажмите кнопку **Скачать архив служебных журналов** и укажите место сохранения архива.

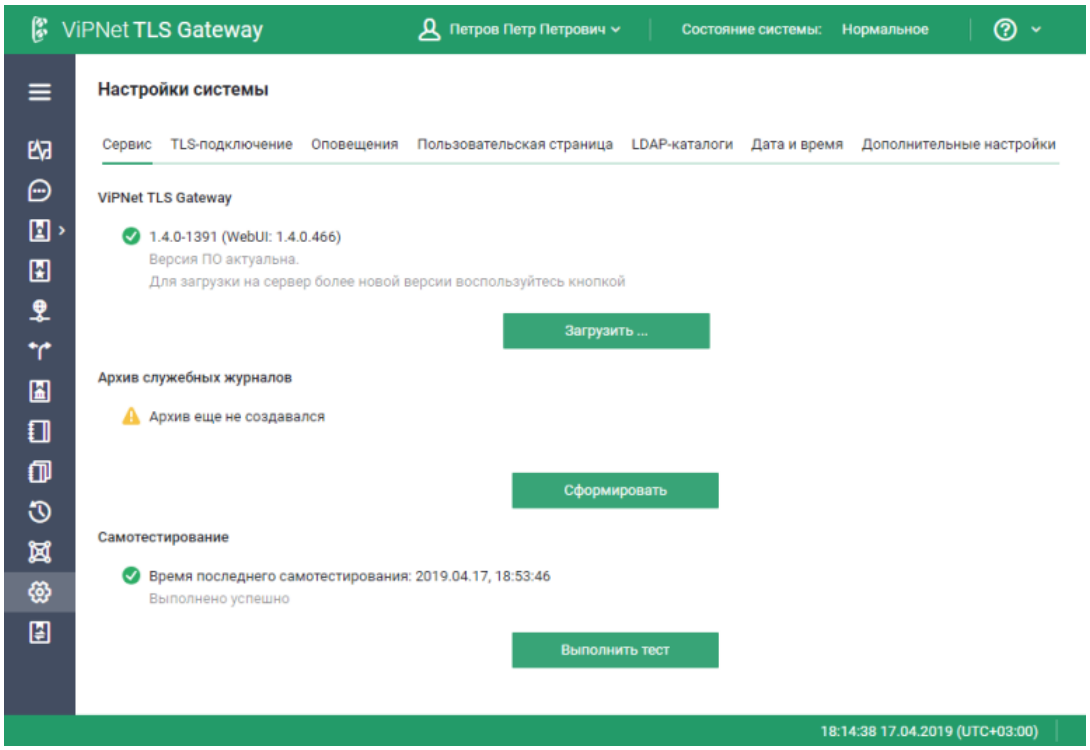

Рисунок 35. Подготовка архива служебных журналов

В результате архив служебных журналов будет сохранен в файл формата TAR.

Внимание! Обязательно проверьте, что в архиве не содержатся файлы с конфиденциальными данными.

Включение и выключение защиты веб-ресурсов от атак

Защита веб-ресурсов от атак может быть отключена (модуль WAF не будет использоваться для защиты веб-ресурсов) или включена (модуль WAF будет использоваться для защиты веб-ресурсов). Начальное состояние модуля WAF зависит от настроек, выполненных в процессе первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).

Включать и отключать защиту веб-ресурсов от атак может администратор с правами администратора доступа (см. Администратор доступа на стр. 36).

Чтобы отключить защиту веб-ресурсов от атак, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** откройте вкладку **Сервис** и в разделе **Web Application Firewall** нажмите кнопку **Отключить**.

В результате будет выключена защита веб-ресурсов от атак, при этом доступ к ресурсам, защищаемым модулем WAF, не будет прекращен.

Чтобы включить защиту веб-ресурсов от атак, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** откройте вкладку **Сервис** и в разделе **Web Application Firewall** нажмите кнопку **Активировать**.

В результате защита веб-ресурсов от атак будет включена.

Сетевые настройки

Первоначально сетевые настройки задаются при развертывании ViPNet TLS Gateway в консоли Linux (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). В дальнейшем при наличии роли администратора безопасности или администратора доступа вы можете изменить сетевые настройки с помощью веб-интерфейса ViPNet TLS Gateway.

Внимание! Некорректное изменение сетевых настроек может привести к неработоспособности системы и невозможности подключения пользователей к защищаемым ресурсам. При изменении IP-адресов сетевых интерфейсов для возможности подключения пользователей или администраторов может потребоваться издание нового транспортного сертификата для соответствующего типа подключения. При изменении IP-адреса сетевого интерфейса для подключения администраторов убедитесь, что в текущем сертификате для доступа администраторов присутствуют заданные значения IP-адресов и DNS-имен. В противном случае изменение может привести у потере удаленного доступа . Восстановление работоспособности будет возможно только с помощью локального доступа (см. Управление с помощью консоли Linux на стр. 154).

Чтобы изменить сетевые настройки ViPNet TLS Gateway, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности или администратора доступа.

2 Перейдите в раздел **Сеть**.

3 На странице **Настройки сети** откройте вкладку **Общие** и измените настройки основного (предпочитаемого) и, при необходимости, альтернативного DNS-сервера, а также IP-адрес основного шлюза (шлюза по умолчанию).

4 Убедитесь, что все настройки заданы верно и нажмите кнопку **Сохранить**.

5 Перейдите на вкладку **Сетевые подключения** и выполните настройки сетевых интерфейсов, которые будут использоваться для подключений:

- В левой панели выберите нужный сетевой интерфейс и, если он не включен, включите его. Для этого справа в разделе **Настройки интерфейса** включите переключатель **Использовать интерфейс <название интерфейса>**.
- Укажите IP-адрес сетевого интерфейса, маску подсети и, при необходимости, DNS-имена. При вводе нескольких значений DNS-имен разделяйте их запятыми без пробелов.

6 Выполните настройки типов подключений для доступа администраторов, подключения пользователей по TLS-каналу с односторонней аутентификацией, подключения пользователей по TLS-каналу с двусторонней аутентификацией к ViPNet TLS Gateway, а также подключения ViPNet TLS Gateway к ресурсам для перенаправления запросов от пользователей:

- В разделе **Типы подключений** справа от названия нужного типа подключения нажмите кнопку **Редактировать**.

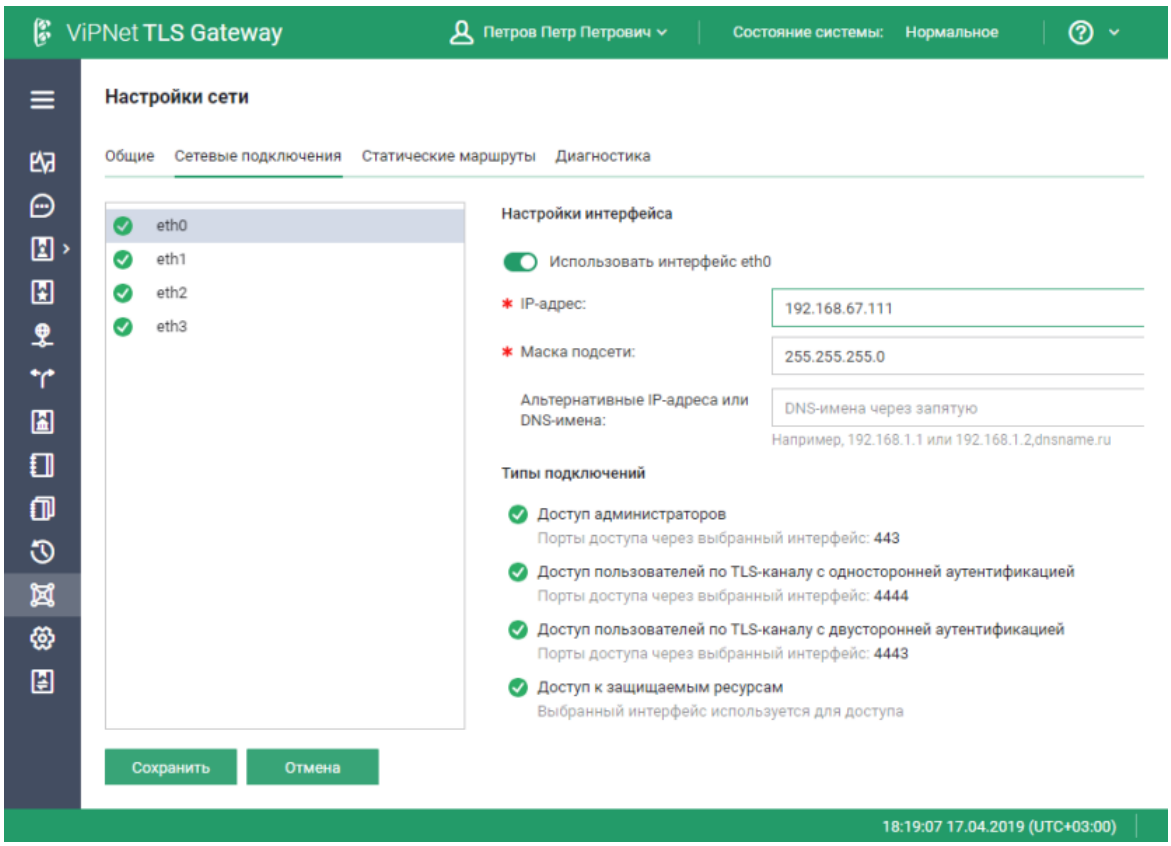

Рисунок 36. Сетевые настройки ViPNet TLS Gateway

- В появившемся окне установите флажки напротив сетевых интерфейсов и укажите порты доступа через выбранные интерфейсы, которые будут использоваться для настраиваемого типа подключения. Вы можете выбрать только включенные сетевые интерфейсы. При

вводе нескольких значений портов доступа разделяйте их запятыми без пробелов. Для типа подключения **Доступ к защищаемым ресурсам** выберите только сетевой интерфейс подключения.

Внимание! Для разных типов подключения вы можете настроить как разные сетевые интерфейсы, так и один. При настройке разных сетевых интерфейсов укажите уникальные IP-адреса для каждого интерфейса. В случае использования одного сетевого интерфейса для разных типов подключения необходимо указать уникальные номера портов. Вы можете использовать любые номера портов кроме значений из диапазона 40000-50000, поскольку они зарезервированы для работы ViPNet TLS Gateway в режиме перенаправления запросов от пользователей к ресурсу с использованием выделенного порта.

---

7 Убедитесь, что все настройки заданы верно и нажмите кнопку **Сохранить**.

8 В окне подтверждения изменений ознакомьтесь со всеми предупреждениями и, при согласии, подтвердите изменения сетевых настроек, нажав кнопку **Применить изменения**.

В результате сетевые настройки ViPNet TLS Gateway будут изменены. Для подключений к ViPNet TLS Gateway следует использовать новые адреса доступа.

Внимание! Если изменились адреса сетевых интерфейсов, не забудьте создать запросы (см. Создание запроса на транспортный сертификат на стр. 142) и получить новые транспортные сертификаты ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143).

Настройка статических маршрутов

Вы можете прописать статические маршруты, если требуется явно указать маршрут прохождения сетевых пакетов, адресованных определенным узлам. Например, настройка статических маршрутов может потребоваться для организации доступа к веб-ресурсам в других подсетях.

Чтобы задать статические маршруты, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Сеть**.

3 На странице **Настройки сети** откройте вкладку **Статические маршруты** и нажмите кнопку **Добавить маршрут**.

4 В поле **Адрес назначения** укажите IP-адрес подсети назначения. Например, 10.10.10.0.

5 В поле **Маска подсети** укажите маску подсети назначения. Например, 255.255.255.0.

6 В поле **Адрес шлюза** укажите IP-адрес шлюза для доступа к IP-адресу назначения.

7 Нажмите кнопку **Сохранить изменения**.

8 В окне **Внимание** подтвердите изменения статических маршрутов.

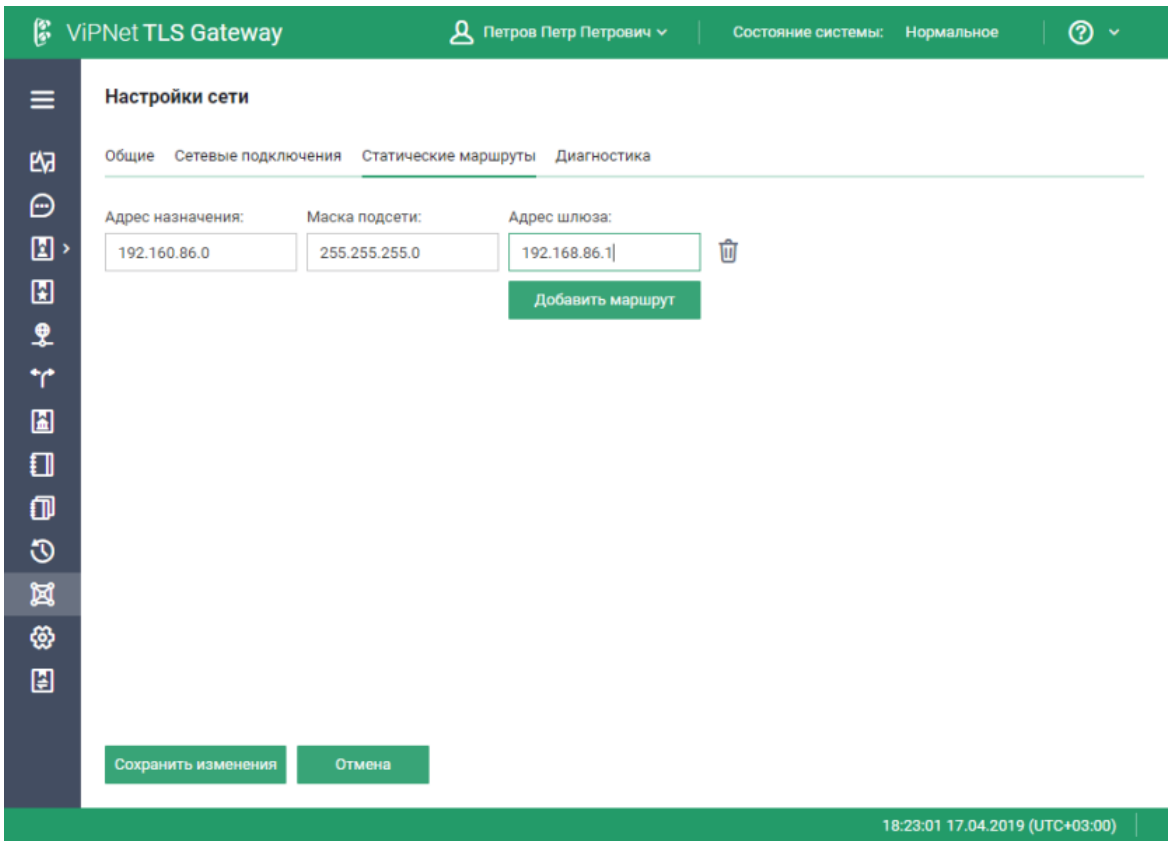

Рисунок 37. Настройка статических маршрутов

В результате будет задан статический маршрут для пакетов, адресованных узлам из подсети назначения.

При необходимости вы можете отредактировать параметры статических маршрутов и сохранить изменения, нажав одноименную кнопку.

Вы можете удалить добавленный статический маршрут, например, если он утратил актуальность. Для удаления справа от записи маршрута нажмите кнопку **Удалить**.

Диагностика сетевого окружения

В процессе работы ViPNet TLS Gateway вы можете произвести диагностику сетевого окружения, например, если какой-то сетевой ресурс недоступен или вам необходимо посмотреть информацию обо всех сетевых интерфейсах ViPNet TLS Gateway. В ViPNet TLS Gateway доступны следующие виды диагностики:

- Проверка соединения с узлом сети.
- Просмотр ARP-таблиц (таблиц преобразования IP-адресов и MAC-адреса) для включенных сетевых интерфейсов ViPNet TLS Gateway.
- Просмотр информации обо всех сетевых интерфейсах ViPNet TLS Gateway.

Чтобы произвести диагностику сетевого окружения ViPNet TLS Gateway, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Перейдите в раздел **Сеть**.
3. На странице **Настройки сети** откройте вкладку **Диагностика** и выполните следующие действия в зависимости от вида диагностики:
   - Для проверки соединения с узлом сети:
     - в списке **Команда** выберите значение **ping**;
     - в поле **Адрес назначение** укажите IP-адрес или DNS-имя узла для проверки соединения;
     - в поле **Количество пакетов** укажите число отправляемых сообщений с запросами.
   - Для просмотра ARP-таблицы:
     - в списке **Команда** выберите значение **arp**;
     - в поле **Адрес назначение** укажите IP-адрес, для которого вы хотите просмотреть ARP-таблицу. Для просмотра ARP-таблиц всех используемых сетевых интерфейсов оставьте это поле пустым.
   - Для просмотра информации о сетевых интерфейсах в списке **Команда** выберите значение **ifconfig**.
4. Нажмите кнопку **Выполнить**. Запустится выполнение выбранной команды.

Результаты диагностики отобразятся в одноименном поле. Вы можете просмотреть, а также выделить и скопировать информацию в буфер обмена.

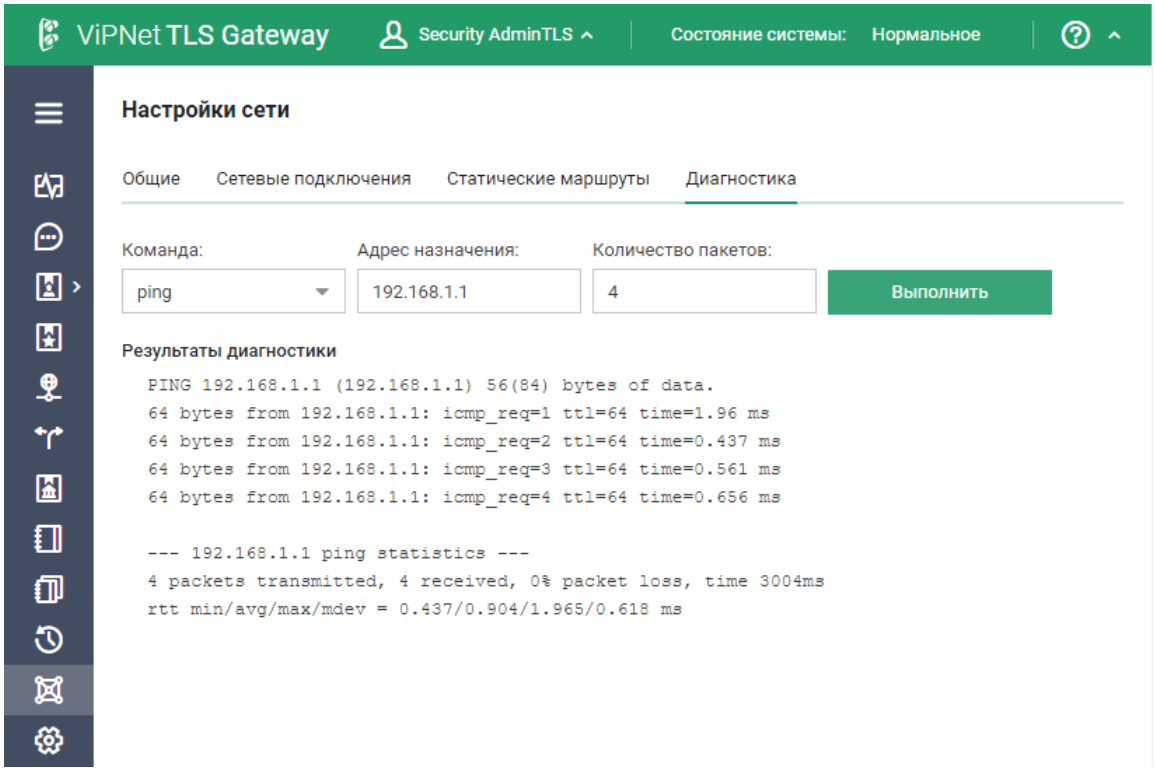

Рисунок 38. Диагностика сетевого окружения

Работа с транспортными сертификатами

Транспортные сертификаты обеспечивают подключение пользователей и администраторов к ViPNet TLS Gateway по протоколу TLS с использованием определенных алгоритмов.

Для обеспечения доступа пользователей с односторонней и двусторонней аутентификацией могут использоваться сертификаты, сформированные по алгоритмам ГОСТ, RSA, ECDSA. Для обеспечения доступа администраторов могут использоваться только сертификаты, сформированные по алгоритмам ГОСТ.

Вы можете загрузить на ViPNet TLS Gateway любое количество сертификатов, сформированных по алгоритмам ГОСТ, RSA и ECDSA, однако для обеспечения доступа по каналу TLS с использованием алгоритмов ГОСТ вы можете назначить только один сертификат, а с использованием алгоритмов RSA, ECDSA — неограниченное количество.

Первоначально транспортные сертификаты добавляются на ViPNet TLS Gateway при развертывании в консоли Linux (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). Если в процессе эксплуатации потребуется, например обеспечить доступ к защищаемым ресурсам по протоколу TLS с использованием другого алгоритма, выполните следующие действия:

- Создайте запрос на издание транспортного сертификата (см. Создание запроса на транспортный сертификат на стр. 142).
- Загрузите полученный сертификат на ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143).

Также в процессе эксплуатации администратор безопасности может изменять типы подключения, для которых будут использоваться транспортные сертификаты (см. Изменение назначений транспортного сертификата на стр. 144).

Создание запроса на транспортный сертификат

Чтобы создать запрос на издание транспортного сертификата, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Транспортные сертификаты** .
3. Если вы хотите создать запрос на основе имеющегося транспортного сертификата, выберите этот сертификат в списке и на панели дополнительных сведений нажмите кнопку .
4. Если вы хотите создать новый запрос, в группе **Запросы** нажмите кнопку **Создать запрос на сертификат**.
5. На первой странице мастера укажите следующие данные:
   - Алгоритм, с помощью которого будут сформированы ключ электронного подписи и ключ проверки электронной подписи.
   - Адреса подключений, для которых необходимо сформировать запрос. Для этого выберите уже имеющиеся на ViPNet TLS Gateway адреса ресурсов или введите их в поле **Адрес** и нажмите кнопку **Добавить в список**. Чтобы в дальнейшем с помощью сертификата можно было обеспечить подключение к защищаемым ресурсам непосредственно по их адресам, добавьте адреса этих ресурсов в запрос.

   Примечание. В поле **Адрес** вы можете задавать адреса с помощью маски вида `*.<адрес защищаемого ресурса>`. Например, для обеспечения доступа по адресам `test.example.com`, `login.example.com` достаточно добавить в запрос адрес вида `*.example.com`. Такие сертификаты называются wildcard-сертификатами.

6. Нажмите кнопку **Далее**.

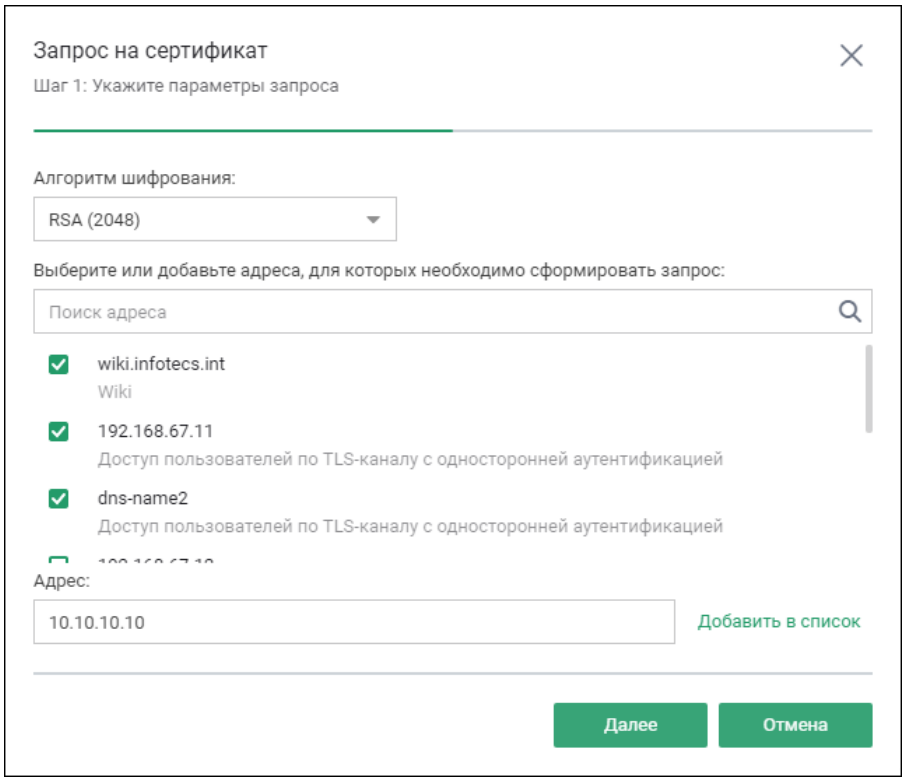

Рисунок 39. Создание запроса на транспортный сертификат

7 На следующей странице мастера проверьте правильность введенных данных и нажмите кнопку **Готово**.

Созданный запрос будет загружен на компьютер администратора и появится в списке в группе **Запросы**.

Примечание. Если при создании запроса вы указали не все нужные IP-адреса или DNS-имена, вы можете перевыпустить запрос на основе имеющегося закрытого ключа. Для этого в группе **Запросы** в списке выберете этот запрос и на панели дополнительных сведений нажмите кнопку . . В открывшемся окне заново выберете адреса подключений (см. шаг 5) и нажмите кнопку **Сохранить**.

---

8 Передайте запрос в удостоверяющий центр.

После получения сертификата загрузите его на ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143).

Загрузка транспортного сертификата

Чтобы загрузить транспортный сертификат на ViPNet TLS Gateway, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Транспортные сертификаты** и в группе **Сертификаты** нажмите кнопку **Загрузить сертификат**.

3 В открывшемся окне выберите файл сертификата и нажмите кнопку **Открыть**.

4 На первой странице мастера ознакомьтесь с параметрами сертификата и нажмите кнопку **Далее**.

5 На следующей странице мастера с помощью флажков укажите типы доступа, для которых вы хотите использовать сертификат и нажмите кнопку **Сохранить**.

   Если для выбранного типа доступа с алгоритмом шифрования ГОСТ уже используется другой сертификат, появится соответствующее предупреждение. При сохранении следует учитывать, что другой сертификат больше не будет использоваться для выбранного типа доступа.

В результате на ViPNet TLS Gateway будет загружен новый транспортный сертификат, который будет использоваться для выбранного типа доступа.

Изменение назначений транспортного сертификата

Например, на вашем ViPNet TLS Gateway для обеспечения доступа администраторов, пользователей с односторонней и двусторонней аутентификацией (алгоритм шифрования ГОСТ) используется один транспортный сертификат. Вы приняли решение, что для обеспечения доступа пользователей с двусторонней аутентификацией будете использовать отдельный транспортный сертификат. Для этого вам нужно создать запрос на издание нового транспортного сертификата (см. Создание запроса на транспортный сертификат на стр. 142) и установить его на ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143), а в текущем транспортном сертификате изменить соответствующие назначения. Для этого:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Транспортные сертификаты**.

3 В группе **Сертификаты** в списке выберите нужный сертификат и на панели дополнительных сведений нажмите кнопку .

4 В списке с помощью флажков укажите типы доступа, для которых вы хотите использовать сертификат и нажмите кнопку **Сохранить**.

   Если для выбранного типа доступа с алгоритмом шифрования ГОСТ уже используется другой сертификат, появится соответствующее предупреждение. При сохранении следует учитывать, что другой сертификат больше не будет использоваться для выбранного типа доступа.

В результате сертификат будет использоваться для выбранных типов доступа.

Настройка подключения к защищаемым ресурсам непосредственно по их адресам

Чтобы для подключения к защищаемым ресурсам пользователям не приходилось заходить на страницу со списком защищаемых ресурсов или использовать адреса в формате `https://<Адрес ViPNet TLS Gateway для подключения пользователей:порт>/<суффикс подключения>`, вы можете настроить подключение к защищаемым ресурсам непосредственно по их адресам. Сделать это можно следующими способами:

- Для всех алгоритмов электронной подписи — добавьте IP-адрес или DNS-имя защищаемого ресурса в запрос на издание транспортного сертификата (см. Создание запроса на транспортный сертификат на стр. 142). Загрузите полученный сертификат на ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143) и назначьте его для обеспечения того же типа доступа, что и тип защищаемого ресурса.
- Для алгоритмов RSA, ECDSA — экспортируйте ключ электронной подписи и соответствующий сертификат защищаемого ресурса в PFX-файл. Затем импортируйте PFX-файл на ViPNet TLS Gateway (см. Импорт ключа электронной подписи и сертификата из файла PFX на стр. 145) и назначьте добавленный сертификат для обеспечения того же типа доступа, что и тип защищаемого ресурса.

Импорт ключа электронной подписи и сертификата из файла PFX

Внимание! Импорт ключей электронной подписи и сертификатов, сформированных по алгоритмам ГОСТ не поддерживается.

Чтобы импортировать ключ электронной подписи и соответствующий сертификат из файла PFX, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.
2. Перейдите в раздел **Транспортные сертификаты** .
3. В группе **Сертификаты** нажмите кнопку **Импортировать PFX** и укажите путь к файлу PFX.
4. В окне **Требуется пароль** введите пароль от файла PFX и нажмите кнопку **Сохранить**.
5. На первой странице мастера импорта ознакомьтесь с информацией о сертификате и нажмите кнопку **Далее**.
6. На следующей странице мастера установите флажки напротив тех же типов доступа, что и типы защищаемых ресурсов и нажмите кнопку **Сохранить**. Под назначениями сертификата будут указаны добавленные на ViPNet TLS Gateway ресурсы, для предоставления доступа к которым может использоваться сертификат.

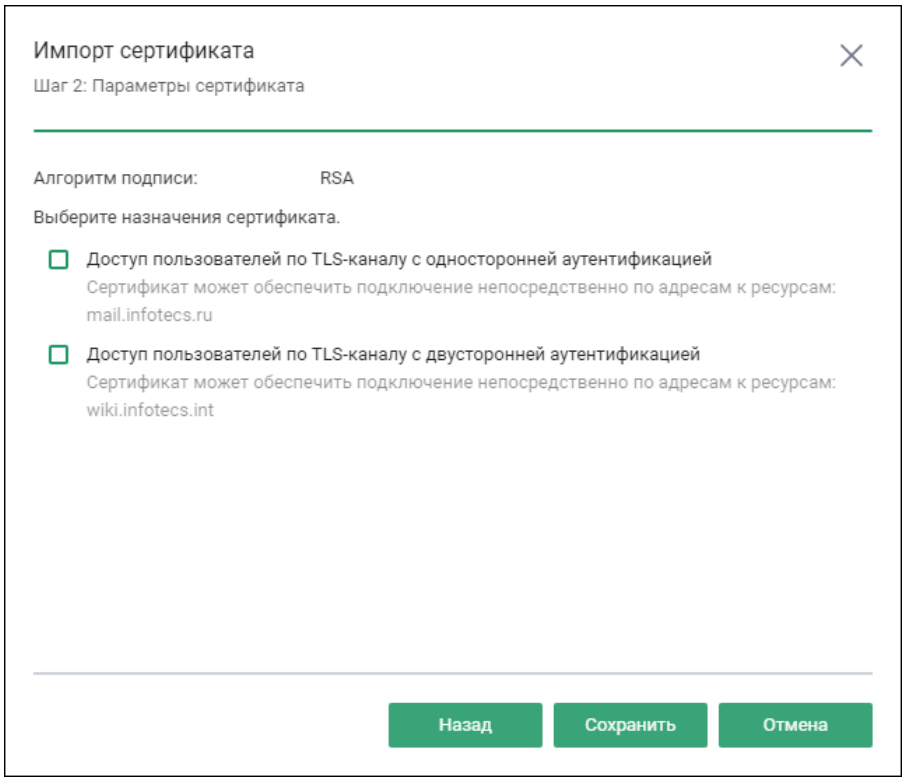

Рисунок 40. Импорт PFX-файла

В результате транспортный сертификат будет использоваться для подключения пользователей к защищаемому ресурсу непосредственно по его адресу.

Просмотр данных о транспортных сертификатах

Вы можете просматривать данные о транспортных сертификатах, добавленных на ViPNet TLS Gateway, например, чтобы проверить их сроки действия. Для просмотра данных о сертификатах, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности.

2 Перейдите в раздел **Транспортные сертификаты** .

3 В группе **Сертификаты** в списке выберите нужный сертификат, на панели дополнительных сведений отобразится краткая информация о транспортном сертификате.

4 При необходимости посмотреть подробные сведения о сертификате, на панели дополнительных сведений щелкните ссылку **Скачать сертификат** и укажите место сохранения сертификата. После подтверждения сертификат будет сохранен в файл формата CER на вашем компьютере. Вы можете открыть файл и просмотреть сертификат администратора.

5 Для просмотра сертификата УЦ, издавшего транспортный сертификат, на панели дополнительных сведений в строке **Кем выдан** щелкните ссылку с названием издателя сертификата. Откроется раздел **Сертификаты удостоверяющих центров** с информацией о сертификате УЦ.

Настройка даты и времени

Первоначально дата и время задаются при развертывании ViPNet TLS Gateway в консоли Linux (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). В дальнейшем при наличии роли администратора доступа или аудитора вы можете:

- Изменить дату и время вручную.
- Настроить синхронизацию даты и времени с NTP-сервером (см. глоссарий, стр. 207).

Для этого:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Перейдите в раздел **Система**.
3. На странице **Настройки системы** перейдите на вкладку **Дата и время**.
4. Чтобы изменить дату и время вручную, установите переключатель в положение **Установить вручную** и в соответствующих полях задайте часовой пояс, дату и время.

   В результате будут изменены дата и время ViPNet TLS Gateway, при этом также будут изменены дата и время, установленные в BIOS аппаратной платформы или виртуальной машины.
5. Чтобы настроить синхронизацию с NTP-сервером, установите переключатель в положение **По протоколу NTP** и в соответствующих полях задайте:
   - Часовой пояс.
   - Время синхронизации.
   - Интервал опроса NTP-сервера.
   - Адрес NTP-сервера. Для добавления еще одного адреса NTP-сервера используйте кнопку **Добавить адрес**. Опрос NTP-серверов осуществляется сверху вниз. При успешной синхронизации последующие сервера не опрашиваются.

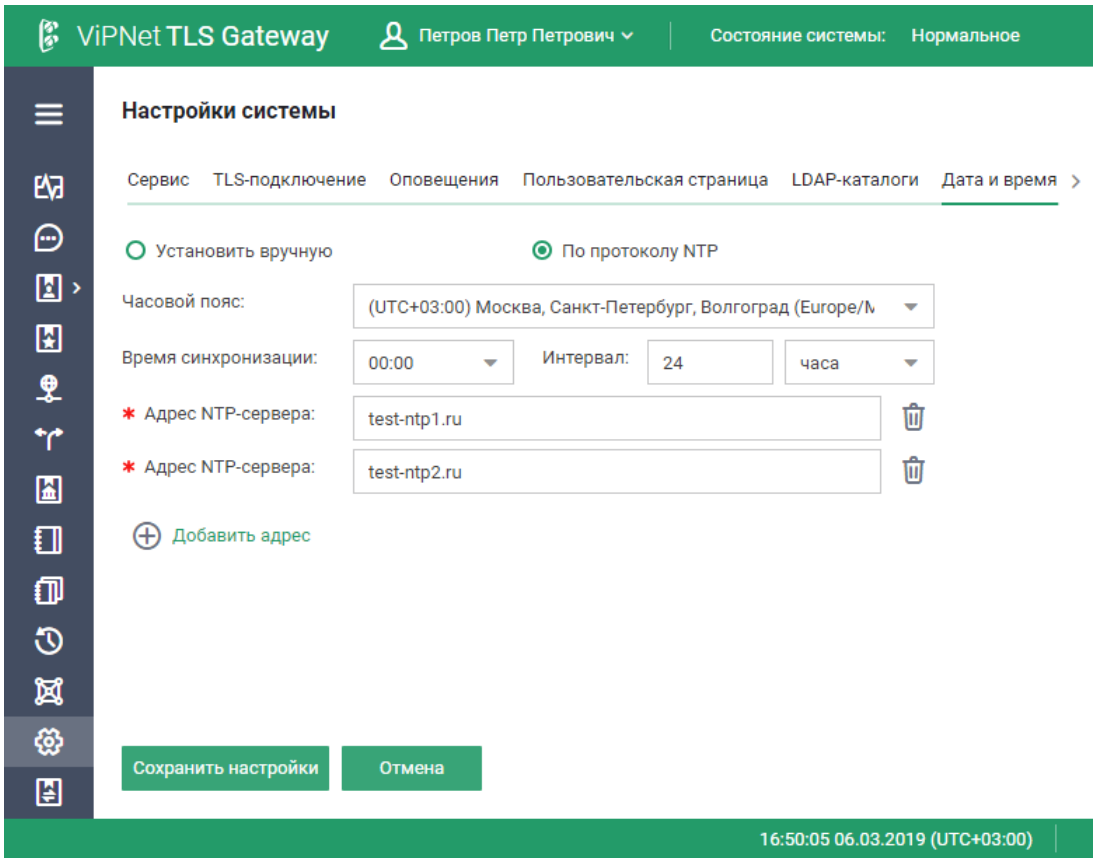

Рисунок 41. Настройка синхронизации даты и времени с NTP-сервером

В результате дата и время ViPNet TLS Gateway будут синхронизироваться с одним из добавленных NTP-серверов с заданной периодичностью.

Обновление ViPNet TLS Gateway

Обновление лицензии

Обновление лицензии может потребоваться для расширения используемых функций ViPNet TLS Gateway или при истечении срока действия текущей лицензии (см. Лицензирование на стр. 39). За 60 дней до окончания срока действия лицензии индикатор состояния ViPNet TLS Gateway выдаст предупреждение о необходимости обновить лицензию (см. Оповещение о состоянии ViPNet TLS Gateway на стр. 130). Для получения новой лицензии обратитесь в отдел продаж ОАО «ИнфоТеКС». Полученную лицензию необходимо установить на ViPNet TLS Gateway.

Если произошел сбой активации текущей лицензии, например, в случае изменений конфигурации аппаратной платформы ViPNet TLS Gateway (см. Лицензирование на стр. 39), или при изменении серийного номера лицензии, потребуется заново активировать и установить лицензию.

Обновление лицензии производится с помощью веб-интерфейса (см. Установка, обновление и активация лицензии через веб-интерфейс на стр. 73).

Обновление ПО ViPNet TLS Gateway

Внимание! При обновлении до версии 1.3.1 и выше требуется файл лицензии, который содержит информацию о максимальном количестве одновременных подключений по протоколу TLS с односторонней и двусторонней аутентификацией (см. Лицензирование на стр. 39). В противном случае пользователи не смогут подключаться к защищаемым веб-ресурсам и туннелируемым ресурсам.

Вы можете обновить ПО ViPNet TLS Gateway на более новую версию или восстановить старую. Для получения обновления ПО обратитесь в службу технической поддержки ОАО «ИнфоТеКС».

Совет. Рекомендуем перед обновлением ПО создать резервную копию данных и сохранить ее на внешний носитель (см. Создание резервной копии данных на стр. 162).

Внимание! Перед обновлением исполнения TLS VA убедитесь, что сконфигурированная виртуальная машина соответствует системным требованиям из раздела Программная реализация TLS VA (на стр. 16). В противном случае обновление ПО может привести к неработоспособности ViPNet TLS Gateway.

Примечание. Если к веб-интерфейсу нет доступа, вы можете обновить ПО в консоли Linux, подключившись к ViPNet TLS Gateway локально (см. Обновление и восстановление целостности ПО ViPNet TLS Gateway на стр. 157).

Чтобы обновить ПО ViPNet TLS Gateway, выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway с полномочиями администратора доступа.
2. Перейдите в раздел **Система**.
3. На странице **Настройки системы** перейдите на вкладку **Сервис**.
4. В разделе **ViPNet TLS Gateway** нажмите кнопку **Загрузить** и выберите файл с обновлением ПО `vipnet_tls_gateway_release-update<XXX>-<YYY>.tar.gz` (где `XXX` — номер версии и сборка, с которой производится обновление, а `YYY` — номер версии и сборка, на которую производится обновление), в зависимости от текущей версии и версии, до которой вы хотите обновить или восстановить ПО. После успешной загрузки обновления в разделе **ViPNet TLS Gateway** отобразится информация о загруженном обновлении и номере его версии. Также появится всплывающее окно оповещения о загруженном обновлении.

   Внимание! Не переименовывайте файл с обновлением. Он защищен контрольной суммой и после переименования вы не сможете его использовать для обновления.

Примечание. Если загруженное обновление не соответствует вашим ожиданиям, например, имеет неправильный номер версии обновления, вы можете загрузить другое обновление, повторно нажав кнопку **Загрузить**.

5 Для установки обновления ПО во всплывающем окне оповещения о загруженном обновлении нажмите кнопку **Обновить сейчас** или в разделе **ViPNet TLS Gateway** справа от информации с номером загруженного обновления нажмите кнопку **Установить**. В появившемся окне **Внимание** нажмите кнопку **Продолжить**. В результате запустится процесс обновления ПО ViPNet TLS Gateway.

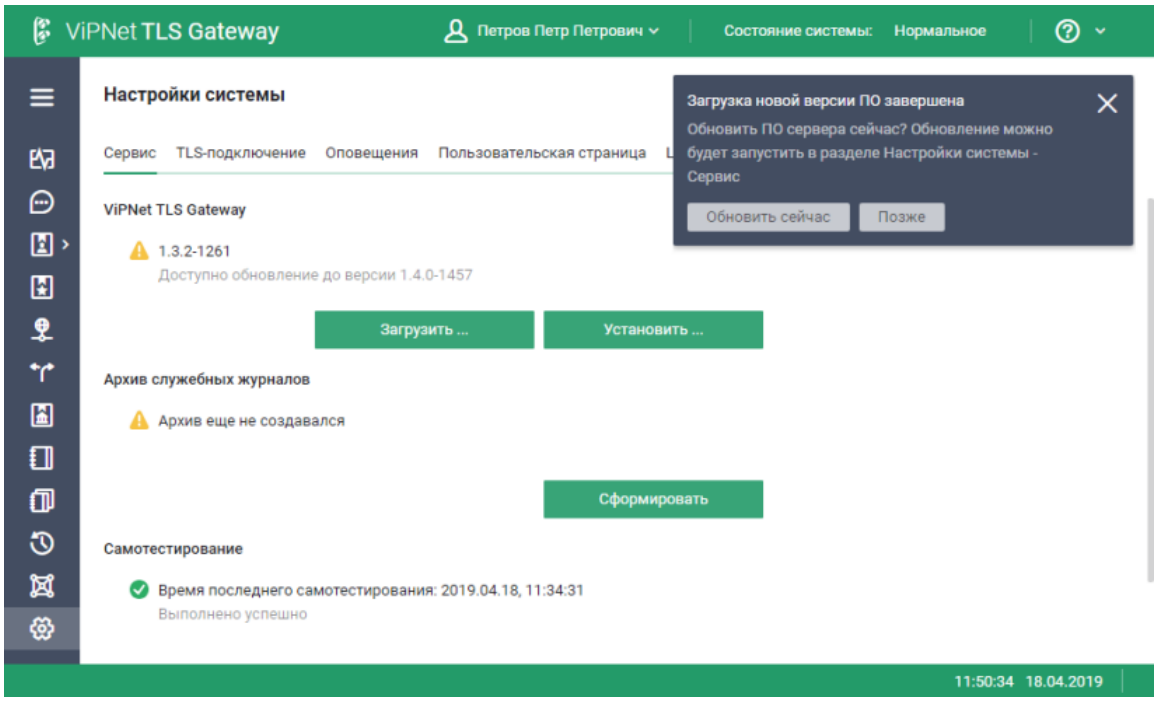

Рисунок 42. Загрузка и установка обновления ПО ViPNet TLS Gateway

Внимание! В ходе процедуры обновления ПО может быть произведена перезагрузка ViPNet TLS Gateway. Во время перезагрузки обслуживание пользователей будет приостановлено.

6 Заново подключитесь к веб-интерфейсу ViPNet TLS Gateway с полномочиями администратора доступа.

Информация о загрузке файла с обновлением и о результатах обновления будет отображена в журнале событий (см. Просмотр журнала событий на стр. 127).

По завершении обновления номер установленной версии ПО будет отображен на странице **О программе** в разделе **Сведения о программе**. Для просмотра информации в верхнем правом углу окна веб-интерфейса в меню **Справка** выберите пункт **О программе**.

Обновление транспортных сертификатов ViPNet TLS Gateway

Транспортные сертификаты ViPNet TLS Gateway для всех типов подключения (доступа пользователей и доступа администраторов) имеют срок действия, определенный администратором в УЦ. За 90 дней до завершения срока действия индикатор состояния ViPNet TLS Gateway выдаст соответствующее предупреждение (см. Оповещение о состоянии ViPNet TLS Gateway на стр. 130). В течение 90 дней после появления предупреждения рекомендуем обновить соответствующие транспортные сертификаты ViPNet TLS Gateway (см. глоссарий, стр. 211). Обновление транспортных сертификатов производится администратором безопасности.

Внимание! При истечении срока действия транспортного сертификата для какого-либо типа подключения доступ с соответствующим типом подключения будет заблокирован и все текущие соединения будут разорваны. Если истек срок действия транспортного сертификата для подключения администраторов, то обновить транспортные сертификаты возможно будет только с помощью локального доступа к ViPNet TLS Gateway (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).

Чтобы обновить транспортные сертификаты, выполните следующие действия:

1. Создайте запрос на издание транспортного сертификата (см. Создание запроса на транспортный сертификат на стр. 142).
2. Загрузите транспортный сертификат на ViPNet TLS Gateway (см. Загрузка транспортного сертификата на стр. 143).

Дополнительные настройки параметров подключения к ViPNet TLS Gateway

Внимание! Изменение дополнительных настроек ViPNet TLS Gateway может привести к потере удаленного доступа пользователей к защищаемым ресурсам.

По умолчанию установлены оптимальные значения параметров дополнительных настроек для разных типов подключения. Изменять их не рекомендуется.

Дополнительные настройки ViPNet TLS Gateway предназначены для тонкой настройки параметров подключения пользователей к защищаемым ресурсам. Например, при невысокой скорости передачи данных в сети вам может потребоваться увеличить **Таймаут установления соединения** или для загрузки на веб-ресурсы файлов объемом более 100 Мбайт потребуется увеличить **Максимальный размер запроса пользователя**.

Администратор доступа может изменять дополнительные настройки для разных типов подключения пользователей, а также для конкретного защищаемого ресурса. Веб-ресурсы и TLS-туннели имеют разный набор параметров для редактирования.

Чтобы изменить дополнительные настройки для типа подключения, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности или администратора доступа.

2 Перейдите в раздел **Система**.

3 На странице **Настройки системы** перейдите на вкладку **Дополнительные настройки**.

4 В группе в левой части страницы выберите тип подключения. В правой части страницы отобразится перечень параметров, которые вы можете изменить.

5 Измените необходимые параметры и нажмите кнопку **Сохранить**.

Внимание! При сохранении изменений все текущие соединения выбранного типа будут разорваны.

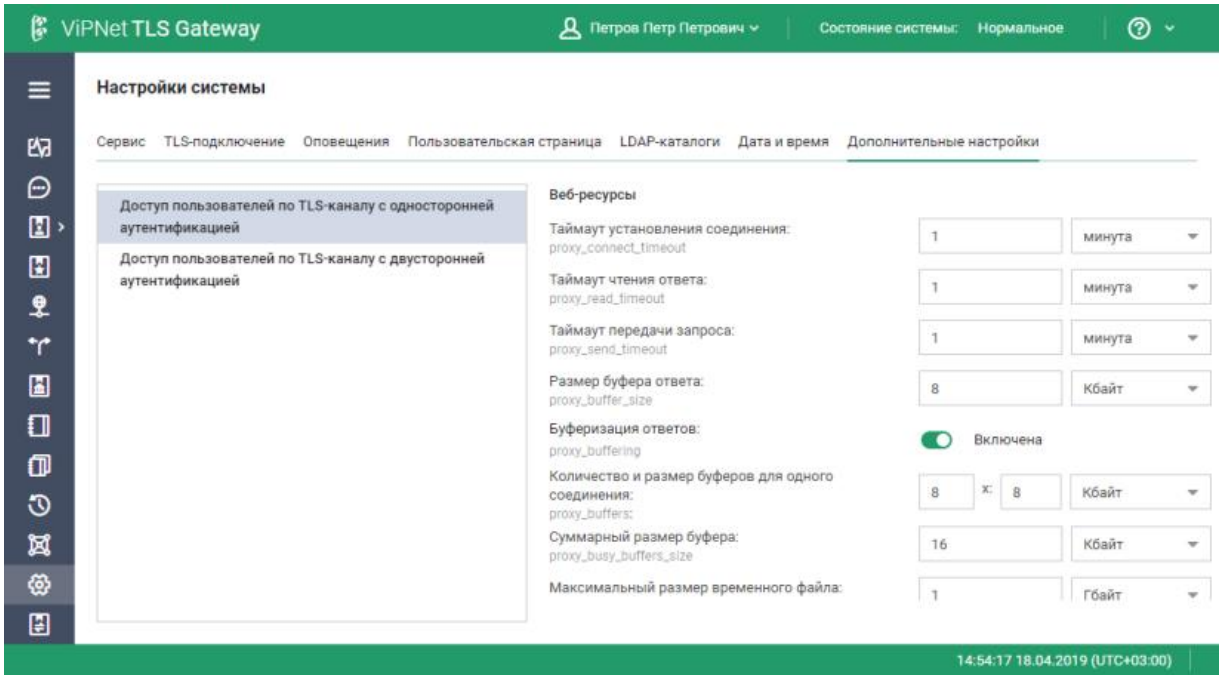

Рисунок 43. Дополнительные настройки ViPNet TLS Gateway

Чтобы изменить дополнительные настройки для конкретного защищаемого ресурса, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора безопасности или администратора доступа.

2 Перейдите в раздел **Ресурсы**.

3 На странице **Ресурсы** выберите ресурс и на панели дополнительных сведений о ресурсе нажмите кнопку **Редактировать**.

4 В окне **Редактирование параметров ресурса** перейдите на вкладку **Дополнительные настройки** и установите флажок **Использовать собственные настройки**.

5 Измените необходимые параметры и нажмите кнопку **Сохранить**.

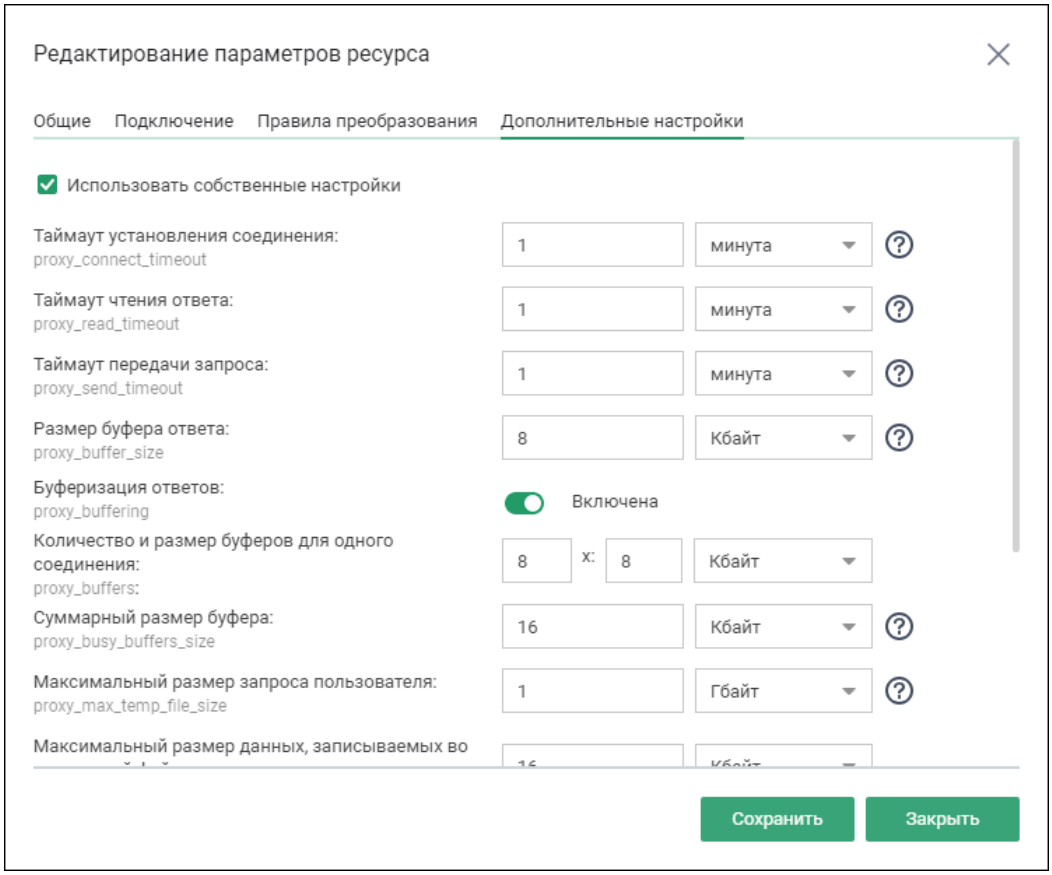

Рисунок 44. Дополнительные настройки защищаемого ресурса

В результате дополнительные настройки защищаемого ресурса будут изменены.

Управление с помощью консоли Linux

Основное управление ViPNet TLS Gateway производится с помощью веб-интерфейса. Однако некоторые действия вы можете выполнить с помощью консоли Linux, подключившись к ViPNet TLS Gateway локально. Например, с помощью консоли Linux вы можете выполнить перезагрузку или выключение ViPNet TLS Gateway.

Действия в консоли Linux производятся администратором с правом локального доступа (см. Администратор с правом локального доступа на стр. 34). Доступны следующие возможности:

- Контроль целостности ПО ViPNet TLS Gateway (на стр. 154).
- Выгрузка служебных журналов для диагностики работы (на стр. 155).
- Повторная инициализация ViPNet TLS Gateway (на стр. 155).
- Обновление и восстановление целостности ПО ViPNet TLS Gateway (на стр. 157).
- Перезагрузка ViPNet TLS Gateway (на стр. 159).
- Выключение ViPNet TLS Gateway (на стр. 159).

Контроль целостности ПО ViPNet TLS Gateway

Вы можете проверить целостность ПО ViPNet TLS Gateway. Например, запустить контроль целостности рекомендуется при проблемах с подключением к веб-интерфейсу ViPNet TLS Gateway.

При необходимости сверить с формуляром контрольные комбинации ОС и ПО ViPNet TLS Gateway вам также потребуется запустить проверку контроля целостности.

Для запуска контроля целостности выполните следующие действия:

1. Подключите к аппаратной платформе ViPNet TLS Gateway монитор и клавиатуру.
2. Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.
3. В строке **Password** введите пароль администратора с правом локального доступа.
4. Из предложенного списка действий выберите контроль целостности (**Check system integrity**). Для этого в командной строке введите `1`.

Запустится процесс контроля целостности, который может занять несколько секунд. Если проверка выполнена успешно, на экране появится соответствующая информация, а также информация о номере версии ViPNet TLS Gateway и значениях контрольных комбинаций ОС и ПО ViPNet TLS Gateway.

Если проверка выявила нарушение целостности, вы можете восстановить целостность ПО путем обновления ПО ViPNet TLS Gateway (см. Обновление и восстановление целостности ПО ViPNet TLS Gateway на стр. 157). При возникновении проблем при восстановлении целостности выгрузите служебные журналы ViPNet TLS Gateway (см. Выгрузка служебных журналов для диагностики работы на стр. 155) и обратитесь в службу технической поддержки ОАО «ИнфоТеКС» для диагностики проблемы.

Выгрузка служебных журналов для диагностики работы

В ViPNet TLS Gateway ведутся служебные журналы, которые могут быть использованы для диагностики работы ViPNet TLS Gateway (см. Подготовка архива служебных журналов для диагностики работы ViPNet TLS Gateway на стр. 133). Если возникли проблемы с удаленным подключением к ViPNet TLS Gateway с помощью веб-интерфейса, вы можете сохранить файлы с журналами на USB-носитель с помощью консоли Linux.

Для этого выполните следующие действия:

1. Подключите к аппаратной платформе ViPNet TLS Gateway монитор, клавиатуру и USB-носитель.
2. Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.
3. В строке **Password** введите пароль администратора с правом локального доступа.
4. Из предложенного списка действий выберите сохранение служебных журналов (**Save logs to usb drive**). Для этого в командной строке введите `2`.
5. Укажите место на подключенном USB-носителе для сохранения журналов диагностики работы ViPNet TLS Gateway. Для этого в строке **Enter folder to store system logs archive** у введите полный путь к каталогу для сохранения файлов с журналами (например, /media/usb0/).

В результате файлы со служебными журналами будут записаны на USB-носитель в указанный каталог.

Повторная инициализация ViPNet TLS Gateway

При возникновении проблем с удаленным подключением к ViPNet TLS Gateway с помощью веб-интерфейса предусмотрена возможность произвести повторную инициализацию ViPNet TLS Gateway, подключившись к нему локально.

При повторной инициализации возможно изменить любые настройки, заданные при первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54), а именно вы можете:

- сменить пароль учетной записи администратора локального доступа (см. Смена пароля администратора локального доступа на стр. 158);

- изменить настройки часового пояса, даты и времени;
- изменить сетевые настройки для обеспечения подключений администраторов и пользователей;
- создать новые транспортные ключи ViPNet TLS Gateway, запросы на новые транспортные сертификаты ViPNet TLS Gateway и загрузить новые сертификаты;
- загрузить новые сертификаты и CRL УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway;
- загрузить новый сертификат администратора безопасности.

Информация о произведенных действиях фиксируется в журнале событий (см. Работа с журналом событий на стр. 127), который можно просмотреть по завершении инициализации, подключившись к веб-интерфейсу ViPNet TLS Gateway.

Чтобы выполнить повторную инициализацию ViPNet TLS Gateway, выполните следующие действия:

1. Подключите к аппаратной платформе ViPNet TLS Gateway монитор, клавиатуру и USB-носитель, если вы планируете загружать какие-либо новые сертификаты.
2. Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.
3. В строке **Password** введите пароль администратора с правом локального доступа.
4. Из предложенного списка действий выберите режим повторной инициализации (**Restart initialization process (backup restore, system settings) of the TLS-Gateway.**). Для этого в командной строке введите `3`. ViPNet TLS Gateway будет перезагружен.
5. Снова авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа.
6. Дальнейшие шаги совпадают с шагами первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).

   Если существующие настройки не требуют изменения, вы можете пропустить соответствующие шаги. Для пропуска шагов в строке **Skip** для каждого шага вводите `y`. Если вы хотите изменить настройки, производимые на шаге, в строке **Skip** для этого шага введите `n` и укажите запрашиваемые данные в соответствии с описанием шага (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).

Внимание! Откажитесь от режима восстановления из резервной копии, когда это будет запрошено, поскольку при выборе режима восстановления из резервной копии все настройки ViPNet TLS Gateway будут сброшены и вам потребуется заново выполнить все вышеуказанные настройки.

Обновление и восстановление целостности ПО ViPNet TLS Gateway

При возникновении проблем с удаленным подключением к ViPNet TLS Gateway с помощью веб-интерфейса предусмотрена возможность произвести обновление ПО, подключившись к ViPNet TLS Gateway локально.

В случае нарушения целостности ПО ViPNet TLS Gateway вы также сможете произвести обновление ПО для восстановления его целостности.

Внимание! Вы можете обновить ПО ViPNet TLS Gateway с целью восстановления его целостности только на ту же версию, которая была установлена.

Для получения файла с обновлением ПО обратитесь в службу технической поддержки ОАО «ИнфоТеКС». Запишите полученный файл с обновлением на USB-носитель.

Чтобы выполнить обновление или восстановление целостности ПО ViPNet TLS Gateway, выполните следующие действия:

1. Подключите к аппаратной платформе ViPNet TLS Gateway монитор, клавиатуру и USB-носитель с файлом обновления ПО.
2. Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.
3. В строке **Password** введите пароль администратора с правом локального доступа.
4. Из предложенного списка действий выберите режим обновления и восстановления целостности ПО (**Installation of the software update or restore of the integrity**). Для этого в командной строке введите `4`.
5. Укажите путь к файлу с обновлением ПО ViPNet TLS Gateway `vipnet_tls_gateway_release-update<XXX>-<YYY>.tar.gz` (где `XXX` — номер версии и сборка, с которой производится обновление, а `YYY` — номер версии и сборка, на которую производится обновление), в зависимости от текущей версии и версии, до которой вы хотите обновить или восстановить ПО, или путь к файлу для восстановления целостности. Для этого в строке **Enter full path to software update or integrity restore archive** введите полный путь к файлу с обновлением. Например, если файл с обновлением находится в корне USB-носителя в файле `vipnet_tls_gateway_release-update1_1_1-683-1_2_0-799.tar.gz`, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/vipnet_tls_gateway_release-update1_1_1-683-1_2_0-799.tar.gz`.

Внимание! Не переименовывайте файлы для обновления и восстановления. Они защищены контрольными суммами и после переименования вы не сможете их использовать.

6 После успешной проверки файла с обновлением ПО запустите процесс обновления (восстановления). Для этого в строке **Do you want to start installation process? During this the system will reboot** введите `y`. После завершения процесса обновления ViPNet TLS Gateway будет перезагружен.

В результате ПО ViPNet TLS Gateway будет обновлено.

Смена пароля администратора локального доступа

Вы можете сменить пароль учетной записи администратора локального доступа, например, в случае увольнения сотрудника, назначенного администратором локального доступа.

Смена пароля администратора локального доступа производится в консоли Linux в процессе повторной инициализации ViPNet TLS Gateway.

Совет. В целях повышения безопасности рекомендуется периодически менять пароль администратора локального доступа.

Чтобы сменить пароль, выполните следующие действия:

1 Подключите к аппаратной платформе ViPNet TLS Gateway монитор, клавиатуру и USB-носитель.

2 Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.

3 В строке **Password** введите пароль администратора с правом локального доступа.

4 Из предложенного списка действий выберите режим повторной инициализации (**Restart initialization process (backup restore, system settings) of the TLS-Gateway**). Для этого в командной строке введите `3`. ViPNet TLS Gateway будет перезагружен.

5 Снова авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа.

6 Откажитесь от пропуска шага "Change root password". Для этого строке **Skip** введите `n`.

7 В строке **Enter new password** введите пароль в соответствии с требованиями к паролю (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и в строке **Repeat password** подтвердите пароль.

Внимание! Запомните новый пароль. Если вы его забудете, восстановить его будет невозможно.

После успешного изменения пароля вы увидите соответствующее сообщение.

8 Дальнейшая последовательность шагов совпадает с шагами первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). Пропустите их, вводя в строке **Skip** для каждого шага символ `y`.

Внимание! Откажитесь от режима восстановления из резервной копии, когда это будет запрошено, поскольку при выборе режима восстановления из резервной копии все настройки ViPNet TLS Gateway будут сброшены и вам потребуется заново выполнить все вышеуказанные настройки.

Перезагрузка ViPNet TLS Gateway

Вы можете перезагрузить ViPNet TLS Gateway, для этого выполните следующие действия:

1 Подключите к аппаратной платформе ViPNet TLS Gateway монитор и клавиатуру.

2 Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.

3 В строке **Password** введите пароль администратора с правом локального доступа.

4 Из предложенного списка действий выберите перезагрузку (**Reboot**). Для этого в командной строке введите `5`.

ViPNet TLS Gateway будет перезагружен.

Выключение ViPNet TLS Gateway

Вы можете выключить ViPNet TLS Gateway, для этого выполните следующие действия:

1 Подключите к аппаратной платформе ViPNet TLS Gateway монитор и клавиатуру.

2 Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.

3 В строке **Password** введите пароль администратора с правом локального доступа.

4 Из предложенного списка действий выберите выключение (**Poweroff**). Для этого в командной строке введите `6`.

ViPNet TLS Gateway будет выключен.

7

Резервное копирование и восстановление данных

Общие сведения 161

Создание резервной копии данных 162

Сохранение резервной копии данных на внешний носитель 163

Восстановление данных из резервной копии после сбоев 165

Общие сведения

Резервное копирование позволяет сохранять данные ViPNet TLS Gateway, восстановление которых может потребоваться в случае возникновения сбоев ViPNet TLS Gateway. При создании резервной копии сохраняется вся необходимая информация из базы данных, за исключением транспортных ключей и соответствующих сертификатов ViPNet TLS Gateway, а также лицензии. Без наличия актуальной резервной копии процедура восстановления данных ViPNet TLS Gateway будет невозможна, в связи с чем рекомендуется регулярно производить резервное копирование данных и сохранять резервные копии на внешний носитель. Создание резервных копий производится администратором доступа с помощью веб-интерфейса.

Процедура восстановления данных зависит от вида сбоя, произошедшего на ViPNet TLS Gateway:

- После аппаратного сбоя (если вышла из строя аппаратная платформа и ViPNet TLS Gateway потерял свою работоспособность) предполагается замена аппаратной платформы и последующее восстановление данных из имеющейся резервной копии в консоли Linux с помощью мастера восстановления (см. Восстановление ViPNet TLS Gateway после аппаратного сбоя на стр. 165).
- После программного сбоя (если работоспособность ViPNet TLS Gateway нарушена из-за повреждения системных файлов или файлов ViPNet TLS Gateway) предполагается повторная установка ПО ViPNet TLS Gateway на аппаратную платформу и последующее восстановление данных из имеющейся резервной копии в консоли Linux с помощью мастера восстановления (см. Восстановление ViPNet TLS Gateway после программного сбоя на стр. 167). Последовательность действий для восстановления данных исполнения TLS VA см. в разделе Восстановление данных исполнения TLS VA (на стр. 172).

Если при обслуживании ViPNet TLS Gateway у вас возникли проблемы с удаленным доступом с помощью веб-интерфейса, для решения проблемы предусмотрена возможность доступа непосредственно на ViPNet TLS Gateway для его повторной инициализации в консоли Linux, которая позволяет задать необходимые настройки с целью восстановления удаленного доступа (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).

Процедура восстановления данных и повторная инициализация на ViPNet TLS Gateway производится администратором с правом локального доступа.

Создание резервной копии данных

Чтобы создать резервную копию данных ViPNet TLS Gateway, выполните следующие действия:

1 Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.

2 Перейдите в раздел **Резервные копии системы**.

3 На панели инструментов страницы **Резервные копии системы** нажмите кнопку **Создать резервную копию**.

В результате на ViPNet TLS Gateway будет создан файл с резервной копией данных. Запись о резервной копии отобразится в списке в разделе **Резервные копии системы**. Для резервной копии будут указаны дата и время создания, кем создана, имя файла, а также размер файла с резервной копией. Чтобы резервную копию можно было использовать для восстановления данных в случае сбоя, сохраните ее на внешний USB-носитель (см. Сохранение резервной копии данных на внешний носитель на стр. 163).

Вы можете удалить резервные копии данных, созданные на ViPNet TLS Gateway, например, если они уже устарели и больше не могут быть использованы.

Примечание. Перед удалением рекомендуется сохранить резервные копии на внешний носитель, если вы не сделали этого ранее (см. Сохранение резервной копии данных на внешний носитель на стр. 163).

Чтобы удалить резервные копии на странице **Резервные копии системы** выберите одну или несколько резервных копий, установив флажки напротив соответствующих резервных копий, и на панели инструментов нажмите кнопку **Удалить резервные копии**.

Сохранение резервной копии данных на внешний носитель

Созданные резервные копии данных хранятся на ViPNet TLS Gateway. Чтобы резервную копию можно было использовать для восстановления данных после сбоя, сохраните ее на внешний носитель (например, USB-носитель).

Примечание. Чтобы не возникло проблем при восстановлении данных из резервной копии, USB-носитель должен быть предварительно отформатирован в одну из следующих файловых систем: ext2, ext3, ext4 или FAT32.

Для сохранения резервной копии данных ViPNet TLS Gateway на USB-носитель выполните следующие действия:

1. Подключитесь к веб-интерфейсу ViPNet TLS Gateway (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69) с полномочиями администратора доступа.
2. Подключите USB-носитель к своему компьютеру.
3. Перейдите в раздел **Резервные копии системы**.
4. На странице **Резервные копии системы** нажмите кнопку **Скачать файл резервной копии** справа от названия резервной копии, которую вы хотите сохранить.
5. Задайте пароль для защиты резервной копии и нажмите кнопку **Скачать архив**.

   Примечание. Пароль должен содержать не менее восьми символов.

6. Укажите место сохранения резервной копии на вашем USB-носителе.

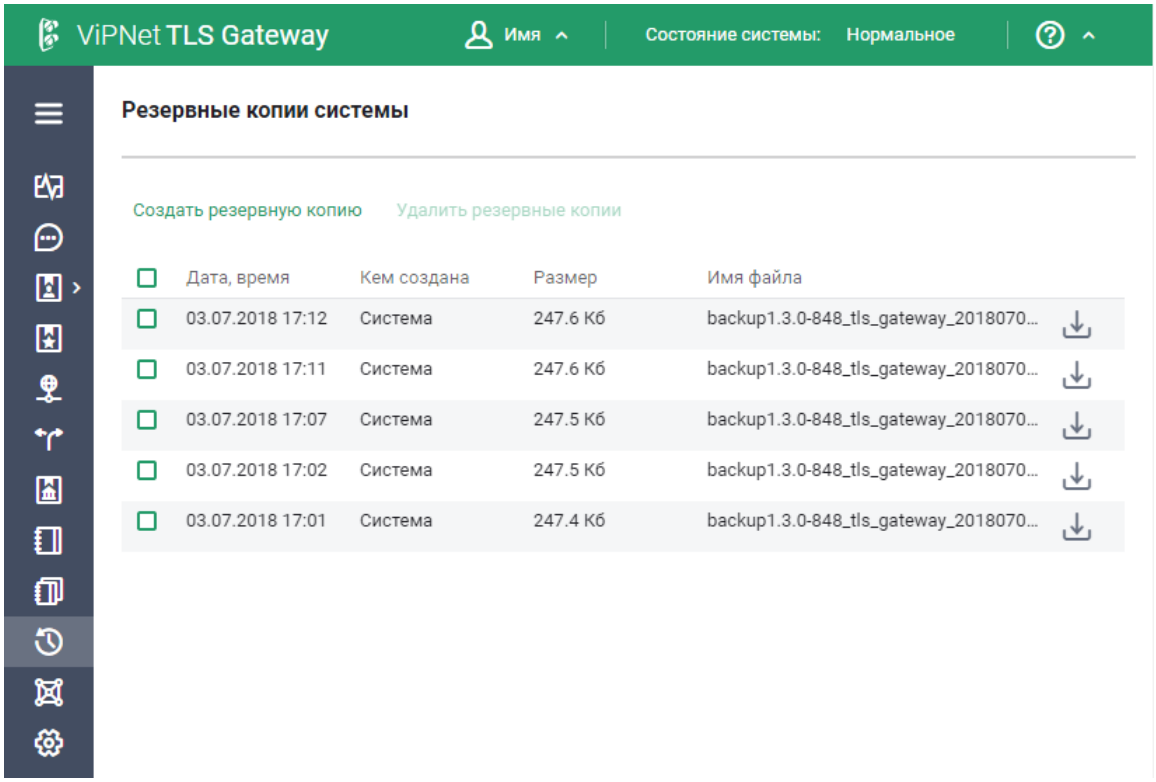

Рисунок 45. Сохранение резервной копии данных

В результате на USB-носителе будет создан файл с резервной копией данных ViPNet TLS Gateway. При необходимости вы можете использовать ее для восстановления данных в случае сбоя (см. Восстановление данных из резервной копии после сбоев на стр. 165).

Внимание! Запомните пароль защиты резервной копии. Если вы его забудете, восстановить его будет невозможно.

Восстановление данных из резервной копии после сбоев

Восстановление ViPNet TLS Gateway после аппаратного сбоя

Если аппаратное исполнение ViPNet TLS Gateway (кроме TLS VA) потеряло свою работоспособность из-за неисправности аппаратной платформы, обратитесь в ОАО «ИнфоТеКС» для замены аппаратной платформы. После получения новой аппаратной платформы вы можете восстановить все данные и настройки ViPNet TLS Gateway из резервной копии. Для восстановления вам потребуется USB-носитель с заранее созданной резервной копией данных (см. Создание резервной копии данных на стр. 162) и пароль.

Совет. Перед восстановлением на USB-носителе, на котором записана резервная копия, создайте каталог для сохранения создаваемых в процессе восстановления файлов с запросами на сертификаты, например, `cert_req`.

Для восстановления данных из резервной копии выполните следующие действия:

1. Подключите аппаратную платформу ViPNet TLS Gateway к электропитанию и к локальной сети.
2. Подключите к аппаратной платформе монитор, клавиатуру и USB-носитель, на котором записана резервная копия данных ViPNet TLS Gateway, а также будут записаны файлы с запросами на новые транспортные сертификаты.
3. Запустите ViPNet TLS Gateway и дождитесь завершения загрузки.
4. На экране появится консоль Linux с приглашением ввести имя учетной записи администратора с правом локального доступа ViPNet TLS Gateway. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.
5. В строке **password** введите технологический пароль `vipnet`.
6. Измените пароль учетной записи администратора с правом локального доступа. Для этого в строке **Enter new password** введите пароль в соответствии с требованиями к паролю (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и в строке **Repeat password** подтвердите пароль. Пароль на экране не отображается.

   Внимание! Запомните новый пароль. Если вы его забудете, восстановить его будет невозможно.

   После успешного изменения пароля вы увидите соответствующее сообщение.

7 Выберите режим восстановления. Для этого в строке **Do you want to restore TLS-Gateway backup** введите `y`.

8 Большая часть дальнейших шагов совпадает с шагами мастера первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54). Следуя подсказкам мастера, выполните следующие действия:

8.1 Задайте часовой пояс, дату и время.

8.2 Запустите создание транспортных ключей.

8.3 Укажите путь к файлу с резервной копией данных ViPNet TLS Gateway, записанному на подключенный USB-носитель, когда это будет предложено. Для этого в строке **Specify the full path to the TLS Gateway database backup** введите полный путь к файлу с резервной копией данных. Например, если файл с резервной копией находится в корне USB-носителя в файле `backup_tls_gateway_2016060600001.tar.gz`, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/backup_tls_gateway_2016060600001.tar.gz`.

8.4 Укажите пароль к файлу с резервной копией. Для этого в строке **Enter password for backup file** введите имеющийся у вас пароль.

8.5 Задайте сетевые настройки ViPNet TLS Gateway или пропустите этот шаг.

Внимание! Если настройки из резервной копии не требуют изменения, вы можете пропустить соответствующие шаги. Для пропуска шагов в строке **Skip** для каждого шага вводите `y`. Если вы хотите изменить настройки, производимые на шаге, в строке **Skip** для этого шага введите `n` и укажите запрашиваемые данные в соответствии с описанием шага (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54).

8.6 Задайте версии протокола TLS для подключения к ViPNet TLS Gateway или пропустите этот шаг.

8.7 Задайте параметры и сформируйте запросы на транспортные сертификаты или пропустите этот шаг.

8.8 Сохраните запросы на сертификаты на USB-носитель и передайте администратору удостоверяющего центра для издания транспортных сертификатов.

8.9 Загрузите сертификат УЦ или пропустите этот шаг.

8.10 Загрузите CRL или пропустите этот шаг.

8.11 Загрузите сертификаты и соответствующие CRL из цепочки доверия к сертификатам или откажитесь от загрузки. При выборе загрузки выполните два предыдущих шага.

8.12 Загрузите транспортные сертификаты и задайте назначения.

8.13 Загрузите сертификат администратора безопасности или пропустите этот шаг.

9 Подтвердите завершение процедуры восстановления. Для этого в строке **Complete TLS-Gateway restore process** введите `y`. Появится сообщение о завершении восстановления.

10 Для продолжения нажмите клавишу **Enter**. ViPNet TLS Gateway будет перезагружен.

11 Отсоедините USB-носитель.

Процедура восстановления завершена. Все данные ViPNet TLS Gateway будут восстановлены.

Восстановление ViPNet TLS Gateway после программного сбоя

Если работоспособность ViPNet TLS Gateway нарушена из-за повреждения каких-либо системных файлов или файлов ViPNet TLS Gateway, вы можете восстановить работоспособность ViPNet TLS Gateway с помощью повторной установки ПО и восстановления данных из резервной копии. Для установки ПО ViPNet TLS Gateway вам понадобится комплект для восстановления: образ ПО в формате IMG и базовая лицензия (см. Лицензирование на стр. 39). Для получения комплекта для восстановления обратитесь в службу технической поддержки ОАО «ИнфоТеКС».

Для восстановления работы и данных ViPNet TLS Gateway после программного сбоя выполните все действия из приведенного ниже списка.

Таблица 17. Порядок восстановления работы ViPNet TLS Gateway после программного сбоя

	Действие	Ссылка
☐	Для восстановления ViPNet TLS Gateway вам потребуются заранее созданная резервная копия данных ViPNet TLS Gateway и пароль к ней. Запишите файл с резервной копией на USB-носитель, чтобы использовать на последующих шагах	Создание резервной копии данных (на стр. 162) Сохранение резервной копии данных на внешний носитель (на стр. 163)
☐	Обратитесь в службу технической поддержки ОАО «ИнфоТеКС» для получения комплекта для восстановления ViPNet TLS Gateway	
☐	Создайте загрузочный носитель с IMG-образом	Запись образа ПО на USB-носитель (на стр. 168)
☐	Установите ПО ViPNet TLS Gateway с помощью IMG-образа	Установка ПО ViPNet TLS Gateway (на стр. 169)
☐	Выполните процедуру восстановления данных из резервной копии	Восстановление данных (на стр. 170)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Запись образа ПО на USB-носитель

Для установки ПО ViPNet TLS Gateway используется образ ПО в формате IMG, который необходимо записать на USB-носитель. Запись образа ПО на USB-носитель можно произвести как в ОС Windows, так и в ОС Linux.

Запись образа ПО в ОС Windows

Для записи образа ПО в ОС Windows можно воспользоваться какой-либо бесплатной программой, например Win32 Disk Imager. Чтобы записать образ, на компьютере с Windows выполните следующие действия:

1 Загрузите исполняемый файл (binary) программы Win32 Disk Imager (https://sourceforge.net/projects/win32diskimager/).

2 Подключите к компьютеру USB-носитель, на который будет записан образ.

3 Запустите программу Win32 Disk Imager от имени администратора.

Примечание. Если при запуске программы первый по порядку съемный диск (например, диск A) не подключен или используется другой программой, появится сообщение об ошибке. В окне сообщения нажмите кнопку **OK** и продолжайте работу.

4 В окне программы Win32 Disk Imager в списке **Device** выберите подключенное устройство.

5 Нажмите кнопку и в окне **Select a disk image** укажите файл образа ПО.

6 Для начала записи нажмите кнопку **Write**.

7 В окне подтверждения нажмите кнопку **Yes**, начнется запись образа на носитель.

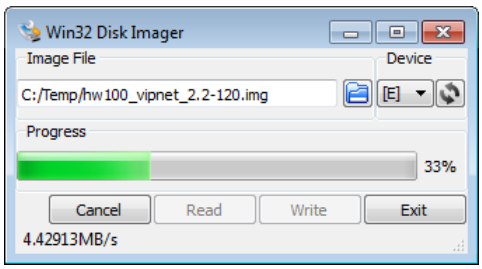

Рисунок 46. Запись образа в программе Win32 Disk Imager

После успешного завершения записи выполните безопасное извлечение устройства. USB-носитель можно использовать для установки ПО.

Запись образа ПО в ОС Linux

Перед записью образа ПО в ОС Linux рекомендуется произвести верификацию образа. Для этого из каталога, в котором находятся образ ПО и его md5-сумма, выполните следующую команду:

```
md5sum -c <имя_файла_md5-суммы>
```

В случае успешной верификации запишите файл образа на USB-носитель. Для этого выполните следующие действия:

1 Подключите к компьютеру USB-носитель, на который будет записан образ.

2 Определите в каталоге `/dev` файл устройства, соответствующий USB-носителю. Для этого выполните команду:

```
dmesg |tail
```

Примечание. Имеется в виду файл физического устройства, а не файл разделов устройства.

---

3 Перейдите в каталог с образом ПО и запишите его на USB-носитель. Для этого выполните команду:

```
sudo dd if=<имя_образа> of=/dev/<имя_файла_устройства>
```

4 После успешного завершения записи выполните безопасное извлечение устройства:

4.1 Посмотрите каталог монтирования USB-носителя с помощью команды: `mount |grep <имя_файла_устройства>`

4.2 Размонтируйте USB-носитель с помощью команды: `sudo umount <каталог_монтирования>`

5 Отсоедините USB-носитель.

USB-носитель можно использовать для установки ПО.

Установка ПО ViPNet TLS Gateway

Чтобы установить ПО ViPNet TLS Gateway, выполните следующие действия:

1 Подключите ViPNet TLS Gateway к электропитанию и к локальной сети.

2 К аппаратной платформе ViPNet TLS Gateway подключите USB-носитель, на котором записан образ ПО (см. Запись образа ПО на USB-носитель на стр. 168).

Внимание! При установке ПО к компьютеру не должны быть подключены никакие другие USB-носители, кроме того, на который записан образ ПО.

---

3 Включите аппаратную платформу и запустите BIOS с помощью клавиши **Del**.

4 Для исполнения TLS 1000 с модулем WAF в подменю **Advanced** > **CPU Configuration** задайте для параметра **Intel Virtualization Technology** значение **Enabled**.

5 Настройте BIOS на загрузку с USB-носителя и нажмите клавишу **F10** для сохранения настроек и выхода из BIOS.

6 Запустится программа установки. В появившейся строке с запросом подтверждения установки ПО подтвердите установку вводом `y`.

7 Появится информация о найденных дисках. Если все верно, подтвердите корректность информации вводом `y`.

8 Появится предупреждение об удалении всех данных с жесткого диска. Подтвердите свое согласие вводом `y`. Запустится установка ViPNet TLS Gateway.

9 После сообщения о завершении установки нажмите клавишу **Enter** и извлеките USB-носитель. ViPNet TLS Gateway будет перезагружен.

Дождитесь завершения загрузки и выполните восстановления данных ViPNet TLS Gateway (см. Восстановление данных на стр. 170).

Восстановление данных

После установки ПО для восстановления работы ViPNet TLS Gateway сначала активируйте лицензию, а затем восстановите все данные из резервной копии ViPNet TLS Gateway. Для этого выполните следующие действия:

1 Запустите ViPNet TLS Gateway (если он еще не запущен) и дождитесь завершения загрузки.

2 К аппаратной платформе ViPNet TLS Gateway подключите USB-носитель, на котором записаны лицензия и резервная копия данных ViPNet TLS Gateway.

3 Авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа. Для этого в строке **login** введите `root` и нажмите клавишу **Enter**.

Примечание. После ввода в командной строке любой команды или последовательности символов для их применения и выполнения необходимо нажимать клавишу **Enter**. В дальнейшем этот шаг подразумевается, но его описание будет опущено.

4 В строке **Password** введите технологический пароль `vipnet`. На экране процесс ввода пароля не отображается.

5 Чтобы установить и активировать лицензию в строке **Do you want to skip TLS Gateway license activation** введите `n`. Если вы хотите установить и активировать лицензию позднее с помощью веб-интерфейса, введите `y` и перейдите к шагу 9.

6 Выберите сетевой интерфейс, через который будет настроен доступ в Интернет для активации лицензии. Для этого подключите сетевой кабель к разъему одного из сетевых портов ViPNet TLS Gateway. На экране появится информация о включении соответствующего сетевого интерфейса с определенным номером (например, информация о включившемся сетевом интерфейсе eth1 будет выглядеть следующим образом: Interface eth1 is UP). Далее в строке **Select network interface for activate license** введите порядковый номер этого интерфейса.

Примечание. Для исполнения TLS VA просто укажите порядковый номер нужного сетевого интерфейса из предложенного нумерованного списка.

7 Произведите настройки этого сетевого интерфейса для доступа к Интернету одним из следующих способов:

- Чтобы получить IP-адрес от DHCP-сервера, в строке **Do you want to use static ip for network interface <название интерфейса>** введите `n` и далее выберите один из следующих способов получения IP-адресов DNS-серверов:
  - Для автоматического получения IP-адресов DNS-серверов в строке **Do you want to use dns servers from dhcp** введите `y`.
  - Для указания IP-адресов DNS-серверов вручную введите `n` и далее в строке **Enter a new DNS servers** введите IP-адреса DNS-серверов. При вводе нескольких значений адресов разделяйте их символом `;` без пробелов. Например, `10.10.10.01;10.10.10.11`. Далее проверьте правильность введенного IP-адреса и, если все верно, в строке **Do you want to select a new DNS servers** введите `n`.
- Если вы хотите задать постоянный IP-адрес интерфейса, в строке **Do you want to use static ip to network interface <название интерфейса>** введите `y` и произведите соответствующие настройки (см. Настройка постоянного IP-адреса сетевого интерфейса на стр. 44).

8 В строке **Enter full path to license file** введите полный путь к файлу с лицензией. Например, если файл с лицензией находится в файле `license.itcslic` в корне USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/license.itcslic`.

Примечание. При вводе путей к файлам соблюдайте регистр букв в названиях каталогов и файлов.

Также работает стандартное в Linux автодополнение команд с помощью нажатия клавиши **Tab**.

Все введенные в текущем сеансе работы консоли Linux команды запоминаются. При необходимости повторного ввода команд для выбора нужных команд из истории можно использовать клавиши со стрелками вверх и вниз.

Запустится процесс активации лицензии. После успешной активации появится соответствующее сообщение.

9 Запустится процесс расчета контрольных комбинаций ОС и ViPNet TLS Gateway. На экране появится информация о номере версии установленного ПО ViPNet TLS Gateway и значения контрольных комбинаций ОС и ViPNet TLS Gateway в строках **TLS Gateway OS checksum is** и **TLS Gateway software checksum is** соответственно. Проверьте, что контрольные комбинации совпадают с имеющимися у вас и нажмите клавишу **Enter** для продолжения.

10 Подтвердите завершение настроек. Для этого в строке **Do you want to complete the factory settings** введите `y`.

11 Откажитесь от выключения ViPNet TLS Gateway. Для этого в строке **Shutdown system** введите `n`.

12 Дальнейшие действия по восстановлению данных аналогичны действиям при восстановлении ViPNet TLS Gateway после аппаратного сбоя, начиная с шага 6 (см. Восстановление ViPNet TLS Gateway после аппаратного сбоя на стр. 165).

Настройка постоянного IP-адреса сетевого интерфейса

Если в процессе первоначальной инициализации или восстановления вам необходимо назначить постоянный IP-адрес для сетевого интерфейса ViPNet TLS Gateway, после выбора соответствующей настройки выполните следующие действия:

1. В строке **Enter a new ip for interface <название интерфейса>** введите IP-адрес сетевого интерфейса. Например, `10.10.10.10`.
2. В строке **Enter a new netmask for interface <название интерфейса>** введите маску сети. Например, `255.255.255.0`.
3. В строке **Enter a new default gateway** введите IP-адрес шлюза по умолчанию.

Если сетевые настройки заданы правильно, сеть будет успешно сконфигурирована и отобразится шаг указания пути к файлу с лицензией.

Восстановление данных исполнения TLS VA

Если работоспособность исполнения TLS VA нарушена, например, из-за повреждения каких-либо системных файлов или файлов ViPNet TLS Gateway, вы можете восстановить работоспособность ViPNet TLS Gateway с помощью повторной установки ПО и восстановления данных из резервных копий. Для установки ПО ViPNet TLS Gateway вам понадобится комплект для восстановления: файл с образом виртуальной машины в формате `OVA` и базовая лицензия.

Для восстановления работы и данных TLS VA после сбоя выполните все действия из приведенного ниже списка.

Таблица 18. Порядок восстановления работы TLS VA

	Действие	Ссылка
☐	Для восстановления TLS VA вам потребуются заранее созданная резервная копия данных ViPNet TLS Gateway и пароль. Запишите ее на USB-носитель, чтобы использовать на последующих шагах	Создание резервной копии данных (на стр. 162) Сохранение резервной копии данных на внешний носитель (на стр. 163)
☐	Заново разверните образ TLS VA на платформу виртуализации с помощью OVA-файла	Развертывание TLS VA (на стр. 44)
☐	Выполните процедуру восстановления данных из резервных копий	Восстановление данных (на стр. 170)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

8

Описание интерфейса Web API

Общие сведения 174

Описание методов Web API 175

Коды ошибок 182

Общие сведения

Данная глава содержит описание интерфейса Web API изделия ViPNet TLS Gateway и предназначена для разработчиков программного обеспечения автоматизированных информационных систем (далее — АИС), взаимодействующих с ViPNet TLS Gateway.

Взаимодействие пользователя с ViPNet TLS Gateway осуществляется с использованием Web API по протоколу HTTPS, который предоставляет набор сервисов с различными методами. Пользователи отправляют на ViPNet TLS Gateway запросы по протоколу HTTPS в формате JSON.

При получении запроса ViPNet TLS Gateway проводит проверку сертификата пользователя согласно правилам (см. Правила автоматического назначения пользователям прав доступа к ресурсам на стр. 109). Если проверка прошла успешно, то по URL-адресу и параметрам запроса выполняется определение соответствующего сервиса (см. Описание методов Web API на стр. 175) и вызов конкретного обработчика. В противном случае формируется сообщение об ошибке (см. Коды ошибок на стр. 182).

Описание методов Web API

Сервис инициализации

Метод «Инициализация веб-приложения»

Адрес запроса: `/services/initialization`

Тип запроса: GET

Описание: Метод возвращает результат операции инициализации веб-приложения или код ошибки сервиса инициализации.

Входные параметры:

Таблица 19. Параметры query string

Имя параметра	Формат	Описание
api_version	String	Версия Web API.

Возвращаемые значения:

Таблица 20. Возвращаемые значения

Имя параметра	Формат	Описание
success	Boolean	Флаг, показывающий результат операции инициализации веб-приложения. Принимает одно из следующих значений: • `true` — инициализация прошла успешно. • `false` — в процессе инициализации произошла ошибка.
errorCode	Number	Код ошибки сервиса инициализации веб-приложения. Передается, если параметр `success=false`. **Примечание.** Перечень ошибок приведен в разделе Коды ошибок (на стр. 182).
authMode	String	Принимает одно из следующих значений: • `oneSideTLS` — для страницы с запросами пользователей с односторонней аутентификацией по протоколу TLS. • `twoSideTLS` — для страницы с запросами пользователей с двусторонней аутентификацией по протоколу TLS.

Имя параметра	Формат	Описание
		Передается, если параметр `success=true`. Не передается для сервиса инициализации веб-приложения администраторов.
certificateInfo	certificateInfo	Информация о сертификате текущего пользователя. Передается, если параметр `success=true`.
userSettings	userSettings	Пользовательские настройки веб-приложения. Передается, если параметр `success=true`. Не передается для сервиса инициализации веб-приложения администраторов.
wafSettings	Объект wafSettings	Настройки модуля WAF. Передается, если присутствует модуль WAF.
softwareVersion	String	Версия программного обеспечения.

Таблица 21. Модель certificateInfo

Имя параметра	Формат	Описание
certificateId	Number, nullable	Идентификатор сертификата.
roles	String [ ]	Роли текущего пользователя. Возможные значения: • `u` — пользователь. • `bu` — заблокированный пользователь.
subjectName	String, nullable	Кому выдан сертификат (поле сертификата **Subject**, **CN**)

Таблица 22. Модель userSettings

Имя параметра	Формат	Описание
headerImageId	String	Уникальный идентификатор изображения, используемого в качестве фона заголовка пользовательских страниц. Если используется заголовок по умолчанию, то передается пустая строка.
bodyImageId	String	Уникальный идентификатор изображения, используемого в качестве фона пользовательских страниц. Если используется фон по умолчанию, то передается пустая строка.
bodyImagePosition	String	Метод позиционирования фонового изображения пользовательских страниц. Передается, если задано фоновое изображение пользовательской страницы.

Имя параметра	Формат	Описание
supportEmail	String	Электронная почта службы поддержки.

Таблица 23. Объект wafSettings

Имя параметра	Формат	Описание
wafSuffix	String	Суффикс подключения для перехода в интерфейс WAF.

Таблица 24. Заголовки ответа

Имя заголовка	Значение	Описание
Set-Cookie	UUID=<уникальный_идентификатор>	CSRF-токен.

Сервис управления запросами на доступ к ресурсам

Метод «Отправка запроса на доступ к ресурсам»

Адрес запроса: `/services/requests?type=send_request`

Тип запроса: POST

Описание: Метод создает запрос на доступ к защищаемым ресурсам.

Входные параметры:

Таблица 25. Параметры query string

Имя параметра	Формат	Описание
api_version	String	Версия Web API.

Таблица 26. Параметры request payload

Имя параметра	Формат	Описание
resourcesIds	Number [ ]	Идентификаторы защищаемых ресурсов, к которым требуется доступ.
requestDescription	String	Текст обращения.
email	String	Электронная почта для обратной

Имя параметра	Формат	Описание
		связи.

Возвращаемые значения:

Таблица 27. Возвращаемые значения

Имя параметра	Формат	Описание
success	Boolean	Результат операции создания запроса. Принимает одно из следующих значений: • `true` — запрос создан. • `false` — запрос не создан.
errorCode	Number	Код ошибки, если параметр `success=false`. **Примечание.** Перечень ошибок приведен в разделе Коды ошибок (на стр. 182).

Метод «Получение информации о запросе доступа к ресурсам для текущего пользователя»

Адрес запроса: `/services/requests?type=load_request`

Тип запроса: GET

Описание: Метод возвращает информацию о запросе доступа к защищаемым ресурсам для текущего пользователя.

Входные параметры:

Таблица 28. Параметры query string

Имя параметра	Формат	Описание
api_version	String	Версия Web API.

Возвращаемые значения:

Таблица 29. Возвращаемые значения

Имя параметра	Формат	Описание
success	Boolean	Результат выполнения операции. Принимает следующие значения: • `true` — информация о запросе доступа к ресурсам получена.

Имя параметра	Формат	Описание
		• `false` — информация о запросе доступа к ресурсам не получена.
errorCode	Number	Код ошибки. Передается, если параметр `success=false`. **Примечание.** Перечень ошибок приведен в разделе Коды ошибок (на стр. 182).
data	data	Объект, содержащий детали запроса доступа к ресурсам. Передается, если параметр `success=true`.

Таблица 30. Модель data

Имя параметра	Формат	Описание
requestDescription	String	Текст обращения. Если нет нерассмотренных запросов на доступ к ресурсам, передается пустая строка.
email	String	Электронная почта для обратной связи. Если нет нерассмотренных запросов на доступ к ресурсам, передается пустая строка.
resourcesIds	Number []	Идентификаторы защищаемых ресурсов, запрос доступа к которым еще рассматривается.

Сервис управления защищаемыми ресурсами

Метод «Получение списка защищаемых ресурсов для пользователя»

Адрес запроса: `/services/proxy_resources?type=user_resources_list`

Тип запроса: POST

Описание: Метод возвращает список защищаемых ресурсов для пользователя

Входные параметры:

Таблица 31. Параметры query string

Имя параметра	Формат	Описание
api_version	String	Версия Web API.

Таблица 32. Параметры request payload

Имя параметра	Формат	Описание
searchText (необязательный)	String	Текст для поиска.
availableForRequest	Boolean	Если `availableForRequest=true`, то будут выданы ресурсы, к которым можно запросить доступ, и ресурсы, доступ к которым запрошен. Если `availableForRequest=false`, то будут выданы ресурсы, к которым уже есть доступ, и ресурсы, доступ к которым запрошен. Является обязательным параметром, если параметр `authMode=twoSideTLS`.
authMode (необязательный)	String	Тип подключения. Принимает одно из следующих значений: • `oneSideTLS` — в этом случае параметр `availableForRequest` игнорируется. • `twoSideTLS` — является обязательным с параметром `availableForRequest`.

Возвращаемые значения:

Таблица 33. Возвращаемые значения

Имя параметра	Формат	Описание
success	Boolean	Результат операции получения списка защищаемых ресурсов.
errorCode	Number	Код ошибки. Передается, если параметр `success=false`. **Примечание.** Перечень ошибок приведен в разделе Коды

Имя параметра	Формат	Описание
		ошибок (на стр. 182).
data	data [ ]	Массив объектов, описывающих защищаемые ресурсы. Если защищаемых ресурсов нет, передается пустой массив. Передается, если параметр `success=true`.

Таблица 34. Модель data []

Имя параметра	Формат	Описание
resourceId	Number	Идентификатор защищаемого ресурса.
resourceName	String	Имя защищаемого ресурса.
resourceDescription	String	Описание защищаемого ресурса.
externalAddress	String	Суффикс подключения.
requestsCount	Number	Статус запроса доступа к ресурсам. Принимает одно из следующих значений: • `0` — запрос рассматривается администратором. • `1` — запрос не рассматривается администратором (доступ разрешен или заблокирован).
tlsGatewayAddress	String [ ] IP:Порт/DNS-Имя	Адрес ViPNet TLS Gateway. Если значение параметра `authMode=twoSideTLS`, то `tlsGatewayAddress=<адрес ViPNet TLS Gateway для подключения по TLS-каналу с двусторонней аутентификацией:порт>`. Если значение параметра `authMode=oneSideTLS`, то `tlsGatewayAddress=<адрес ViPNet TLS Gateway для подключения по TLS-каналу с односторонней аутентификацией:порт>`.
resourceIconId	String	Идентификатор изображения, используемого в качестве пиктограммы ресурса. Если пиктограмма не используется, то передается пустая строка.

Коды ошибок

Таблица 35. Коды ошибок

Значение	Описание
-1	Нет прав на выполнение данного действия
-7	Срок действия сертификата истек
-11	Сертификат с данным серийным номером и именем издателя не зарегистрирован
-16	Пустой аргумент недопустим
-17	Защищаемый ресурс с заданным именем уже существует
-18	Адрес защищаемого ресурса уже используется
-19	Суффикс подключения защищаемого ресурса уже используется
-20	Редактирование объекта невозможно, состояние было изменено
-21	Сертификат имеет неизвестный формат
-22	Ошибка авторизации пользователя
-23	Невозможно удалить последнего администратора безопасности
-24	Невозможно редактировать доступ к ресурсам у заблокированного сертификата
-25	Для данного издателя уже зарегистрирован более новый CRL
-26	Не найден доверенный сертификат УЦ для проверки подписи
-29	Корневой сертификат с заданным ключом уже зарегистрирован
-30	Сертификат был отозван
-31	Не найден CRL для корневого сертификата
-32	Лицензия не загружена
-33	Достигнуто максимальное число пользователей для данной лицензии
-34	Правило доступа с данным именем уже существует
-35	Набор правил не применим к параметрам сертификата
-36	Срок действия сертификата еще на наступил
-37	Невозможно удалить корневой сертификат, подписавший транспортные
-38	Нет доступных слотов
-39	Слот уже активирован
-40	Невозможно удалить себе полномочия администратора безопасности
-41	Невозможно удалить собственный сертификат

Значение	Описание
-43	Превышена максимально допустимая длина поля сертификата
-44	У сертификата отсутствуют обязательные поля
-45	Недостаточно места на диске
-46	Невозможно добавить роль пользователю, сертификат которого просрочен
-47	Невозможно редактировать доступ к ресурсу пользователю, сертификат которого просрочен
-48	Некорректная операция со слотом
-49	Невозможно назначить порт проксирования ресурсу
-50	Невозможно удалить доверенный сертификат УЦ при наличии дочерних доверенных
-51	Невозможно назначить ресурс для подключения пользователей по TLS-каналу с двусторонней аутентификацией на порт. Превышен максимально допустимый размер CRL.
-52	Невалидна цепочка корневых сертификатов, выпустивших данный сертификат
-100	Внутренняя ошибка при выполнении
-106	Ошибка обработки входных данных
-107	Объект уже существует
-108	Редактирование не допускается
-109	Нет прав на выполнение данного действия
-110	Объект не найден
-111	Проверка подписи сертификата неуспешна
-112	У сертификата отсутствует идентификатор ключа
-113	У сертификата отсутствует идентификатор ключа издателя
-114	Некорректный файл лицензии
-115	Задача уже находится в процессе выполнения
-116	Ошибка создания резервной копии
-117	Резервная копия не существует
-118	Ошибка перезагрузки конфигурации NGINX
-119	Ошибка инициализации криптографического модуля
-120	Ошибка создания запроса на сертификат
-121	Запрос на транспортный сертификат не сгенерирован
-122	Транспортный сертификат недействителен

Значение	Описание
-123	CRL недействителен
-124	Ошибка ввода в действие транспортного ключа
-125	Загружаемый CRL не новее загруженного
-126	Нет транспортных сертификатов, сохраненных в базе данных
-128	Попытка активировать транспортный ключ для нецелевого модуля NGINX
-129	Нет зарезервированных слотов для транспортного ключа
-130	Ошибка при активации слота в базе данных
-131	Ошибка при попытке привести конфигурацию NGINX в исходное состояние
-132	Ошибка при очистке предыдущего активного слота
-133	Не найдена директория для резервного копирования
-134	Ошибка при создании директории
-135	Ошибка при создании архива резервной копии
-136	Ошибка при расчете чек-суммы архива резервной копии
-137	Ошибка при регистрации резервной копии в базе данных
-143	Неопределенный тип аутентификации
-144	Ошибка при удалении защищаемого ресурса
-145	Ошибка при получении сетевых настроек
-146	Отсутствует сетевой интерфейс
-147	Ошибка при обновлении сетевого интерфейса
-148	Тип сетевых настроек не определен
-149	Ошибка при обновлении основных сетевых настроек
-150	Не найдена директория для архивов технических логов
-151	Ошибка при создании архива технических логов
-152	Ошибка при получении атрибутов архива технических логов
-153	Ошибка загрузки файла
-156	Неизвестный тип файла
-157	Неправильная подпись файла
-158	Превышен максимально допустимый размер файла
-159	Недостаточно свободного места для записи файла
-160	Ошибка формата файла
-161	Файл уже существует

Значение	Описание
-162	Невалидный XML список доверенных корневых сертификатов
-163	Не найден файл с обновлением ПО
-164	Ошибка в процессе обновления ПО
-165	Проверка подписи файла обновления ПО неуспешна
-166	Не найден скрипт обновления
-167	Не найден файл с информацией об обновлении
-168	Не найдена версия обновления
-169	Невозможно преобразовать адрес ресурса
-170	Серийный номер лицензии отличается от базовой
-171	Загружен пустой CRL
-172	Полученный файл не является CRL
-173	Не удалось загрузить CRL
-174	Истекла сессия (отсутствует или устарел csrf_token)
-175	Не удалось изменить статические маршруты
-176	Выполнение команды диагностики завершено с ошибкой
-177	Не удалось включить/отключить WAF
-178	Отсутствует действительная лицензия на работу с WAF
-179	Версия обновления несовместима с текущей версией ПО
-180	Неизвестный тип обновления
-181	Нарушена целостность файла обновления
-182	Не удалось активировать лицензию
-183	Лицензия недействительна
-184	Внутренняя ошибка системы лицензирования
-185	Недоступен сервер активации
-199	Внутренняя ошибка
-200	Ошибка соединения с базой данных

9

Возможные неполадки и способы их устранения

Невозможно подключиться к веб-интерфейсу ViPNet TLS Gateway 187

Некорректное отображение иконок и меню в веб-интерфейсе 189

Отображается ошибка при изменении конфигурационного файла веб-сервера 190

Невозможно подключиться к веб-интерфейсу ViPNet TLS Gateway

Если вы не можете подключиться к ViPNet TLS Gateway посредством веб-интерфейса, для решения проблемы подключитесь к ViPNet TLS Gateway локально и выполните одно или несколько следующих действий:

1 Перезагрузите ViPNet TLS Gateway (см. Перезагрузка ViPNet TLS Gateway на стр. 159).

2 Если проблема сохраняется, произведите контроль целостности ViPNet TLS Gateway (см. Контроль целостности ПО ViPNet TLS Gateway на стр. 154). Если проверка выполнена неуспешно, то произведите выгрузку служебных журналов (см. Выгрузка служебных журналов для диагностики работы на стр. 155) и обратитесь в службу технической поддержки ОАО «ИнфоТеКС» для диагностики проблемы. В этом случае скорее всего поможет только восстановление ViPNet TLS Gateway после программного сбоя (на стр. 167).

3 Если проверка контроля целостности выполнена успешно, произведите выгрузку служебных журналов (см. Выгрузка служебных журналов для диагностики работы на стр. 155) и выполните повторную инициализацию ViPNet TLS Gateway (см. Повторная инициализация ViPNet TLS Gateway на стр. 155). В процессе повторной инициализации может быть несколько вариантов исправления проблемы:

   3.1 Если при повторной инициализации был запущен биометрический датчик случайных чисел (электронная рулетка) **Press different keys**, следуйте указаниями мастера инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и нажимайте произвольные клавиши на клавиатуре для работы электронной рулетки до появления сообщения **Done**. Остальные шаги следует пропустить. После завершения инициализации попробуйте подключиться к веб-интерфейсу ViPNet TLS Gateway. Если проблема не решилась, обратитесь в службу технической поддержки ОАО «ИнфоТеКС» для диагностики проблемы, передав ей архив служебных журналов.

   3.2 Если при повторной инициализации биометрический датчик случайных чисел не был запущен, возможно несколько вариантов проблем и путей решения в процессе повторной инициализации:

   - Некорректно заданы сетевые настройки. В этом случае может помочь повторный ввод сетевых настроек. Для этого в мастере инициализации откажитесь от пропуска шага "Change network settings" (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и задайте правильные настройки сети.

Внимание! Если были заданы статические маршруты (см. Настройка статических маршрутов на стр. 138), они могут быть сброшены.

- Истек срок действия CRL. В этом случае может помочь повторная загрузка CRL. Для этого в мастере инициализации откажитесь от пропуска шага "Load CRL" (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и загрузите новый файл с CRL.
- Истек срок действия транспортных сертификатов. В этом случае может помочь обновление транспортных сертификатов. Для этого в мастере инициализации откажитесь от пропуска шага "Create certificate request" (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и создайте новые запросы на сертификаты, а затем следуя подсказкам мастера, загрузите новые сертификаты.
- Закончились доступные транспортные ключи. В этом случае может помочь формирования новых транспортных ключей и обновление транспортных сертификатов. Для этого в мастере инициализации откажитесь от пропуска шага "Generate keys" (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и сформируйте новые транспортные ключи. Затем следуя подсказкам мастера, сформируйте запросы на транспортные сертификаты и загрузите новые сертификаты.

4 Если вы подключаетесь к ViPNet TLS Gateway с использованием ViPNet CSP, внесите изменения в системный реестр Windows, для этого:

4.1 В меню **Пуск** выберите пункт **Выполнить**.

4.2 В окне **Выполнить** в поле **Открыть** введите `regedit` и нажмите кнопку **OK**.

Внимание! Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

4.3 В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL` задайте параметру `DisableClientExtendedMasterSecret` значение `1`. При отсутствии указанного параметра создайте его вручную, используя тип **DWORD**.

Если ни один из способов не помог решить проблему, обратитесь в службу технической поддержки ОАО «ИнфоТеКС» для диагностики проблемы, передав ей архив служебных журналов.

Некорректное отображение иконок и меню в веб-интерфейсе

При возникновении ошибки очистите кэш вашего веб-браузера и выполните повторную загрузку страницы веб-интерфейса (например, если вы используете веб-браузер Internet Explorer, нажмите сочетание клавиш **Ctrl+F5**).

Отображается ошибка при изменении конфигурационного файла веб-сервера

Если в журнале событий и в окне мониторинга появились события с ошибкой при изменении конфигурационного файла веб-сервера, это означает, что превышен суммарный размер файлов CRL, добавленных на ViPNet TLS Gateway (см. Установление доверия к одному или нескольким удостоверяющим центрам на стр. 92), и для некоторых пользователей ограничен доступ к защищаемым ресурсам по каналу TLS с двусторонней аутентификацией. Для решения проблемы выполните одно или несколько следующих действий:

- Если вы используете исполнение TLS VA, убедитесь, что указаны рекомендуемые настройки виртуальной машины (см. Программная реализация TLS VA на стр. 16). Если настройки отличаются, то выполните их в соответствии с рекомендуемыми.

Внимание! После изменения настроек виртуальной машины суммарный размер файлов CRL будет увеличен. Изменения вступят в силу после выполнения одного из следующих действий: загрузки нового CRL вручную или автоматически, удаления или добавления сертификата УЦ и соответствующего CRL (см. Управление сертификатами доверенных удостоверяющих центров на стр. 92).

- Проверьте, что для всех ранее добавленных защищаемых ресурсов настроены правила преобразования URI ресурса (см. Создание правил преобразования URI ресурса на стр. 88). Если не настроены, то выполните настройку правил. Работа с использованием выделенных портов не поддерживается.
- Если проблема сохраняется, произведите оптимизацию перечня доверенных УЦ с целью уменьшения суммарного размера файлов CRL для удовлетворения условиям максимально разрешенных суммарных размеров файлов CRL, добавленных на ViPNet TLS Gateway.

A

Описание структуры сообщения в формате CEF

В данном приложении описана структура сообщений в формате CEF (Common Event Format), а также приведены перечень и описание поддерживаемых в ViPNet TLS Gateway ключей расширения.

Сообщение в формате CEF имеет следующий формат:

`[Дата и время создания CEF-сообщения] [Имя узла-источника] [Заголовок CEF-сообщения] [Поле расширения]`, где:

- `[Дата и время создания CEF-сообщения]` — дата и время создания сообщения в соответствии с системным временем ViPNet TLS Gateway в формате: `Месяц Дата Число Час:Минута:Секунда`. Например, `Dec 13 10:15:13`.
- `[Имя узла-источника]` — `TLS-Gateway`.
- `[Заголовок CEF-сообщения]` имеет следующий формат:

  `CEF: [Version]|[Device Vendor]|[Device Product]|[Device Version]|[Signature ID]|[Name]|[Severity]|`

  Все поля заголовка являются обязательными. Поля заголовка отделяются друг от друга символом `|`. Последнее поле заголовка также отделено от поля расширения символом `|`. Описание полей заголовка CEF-сообщения представлено в таблице ниже.

  Таблица 36. Описание полей заголовка CEF-сообщения

Наименование поля	Описание поля
Version	Текущая версия формата CEF: `0`
Device Vendor	Наименование ViPNet TLS Gateway: `InfoTeCS`

Наименование поля	Описание поля
Device Product	Наименование исполнения ViPNet TLS Gateway из лицензии. Например, `tls_gateway_1000`
Device Version	Серийный номер ViPNet TLS Gateway из лицензии. Например, `8RTYJ-4GHB-KJHG-HG3J`
Signature ID	Уникальный идентификатор события: `1`
Name	Описание события: `TLS Gateway Status`
Severity	Условный уровень важности сообщения (см. Уровни важности событий на стр. 130) в числовом формате: • `1` — ViPNet TLS Gateway в нормальном состоянии; • `2` — ViPNet TLS Gateway в опасном состоянии; • `4` — ViPNet TLS Gateway в критическом состоянии.

- `[Поле расширения]` имеет следующий формат:

  `[название ключа=значение ключа] [название ключа=значение ключа] [ключ=значение ключа]`

  Поле содержит пары ключ-значение, разделенных пробелами. Все поля расширения являются обязательными.

  Полный перечень и описание поддерживаемых в ViPNet TLS Gateway ключей приведены в таблице ниже.

  Таблица 37. Ключи поля расширения

Название ключа	Название ключа по стандарту CEF	Описание значения ключа
cs1	deviceCustomString1	Ограничение из лицензии ViPNet TLS Gateway на максимальное количество действительных сертификатов пользователей, которые можно добавить на ViPNet TLS Gateway.
cs2	deviceCustomString2	Текущее количество добавленных на ViPNet TLS Gateway сертификатов пользователей.
cs3	deviceCustomString3	Текущее количество подключений по протоколу TLS с односторонней аутентификацией к веб-ресурсам.
cs4	deviceCustomString4	Текущее количество подключений по протоколу TLS с односторонней аутентификацией к туннелируемым ресурсам.
cs5	deviceCustomString5	Текущее количество подключений по протоколу TLS с двусторонней аутентификацией к веб-ресурсам.
cs6	deviceCustomString6	Текущее количество подключений по протоколу TLS с двусторонней аутентификацией к туннелируемым ресурсам.

Название ключа	Название ключа по стандарту CEF	Описание значения ключа
cn1	deviceCustomNumber	Наличие лицензии на использование Web Application Firewall (WAF): • 0 — нет лицензии на WAF; • 1 — есть лицензия на WAF.

Пример CEF-сообщения:

```
Dec 13 10:15:13 TLS-Gateway CEF:0|InfoTeCS|tls_gateway_1000|RTYJ-4GHB-KJHG-HG3J|1|TLS
Gateway Status|4|cs1=3000 cs2=1756 cs3=100 cs4=10 cs5=79 cs6=28 cn1=1
```

B

История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet TLS Gateway.

Новые возможности версии 1.3.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.3.2 по сравнению с версией 1.3.1.

- **Расширен список поддерживаемых версий протокола TLS для подключения к ViPNet TLS Gateway**

  Теперь вы можете подключаться к ViPNet TLS Gateway по протоколу TLS версий 1.0 и 1.1.

- **Добавлена настройка версии протокола TLS для подключения к ViPNet TLS Gateway**

  Теперь вы можете задать версии протокола TLS для разных типов подключения.

- **Добавлена возможность туннелирования TCP-трафика по протоколу TLS с двусторонней аутентификацией**

  Вы можете настроить TLS-туннель для защиты данных в приложениях, которые работают через протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV, SQL и создавать TLS-соединения с двусторонней аутентификацией для туннелирования.

- **Добавлена поддержка Kernel-based Virtual Machine (KVM)**

  Теперь вы можете разворачивать исполнение TLS VA на платформах виртуализации KVM. Для этого в комплект поставки добавлен образ виртуальной машины ViPNet TLS Gateway — `*.qcow2`.

- **Добавлены дополнительные настройки ViPNet TLS Gateway**

  Теперь вы можете выполнить тонкую настройку параметров подключения пользователей к защищаемым ресурсам (см. Дополнительные настройки параметров подключения к ViPNet TLS Gateway на стр. 151).

- **Расширен список поддерживаемых ViPNet TLS Gateway ключей для сообщений в формате CEF**

  Теперь в сообщениях формата CEF передается информация о текущем количестве подключений по протоколу TLS с односторонней и двусторонней аутентификацией к веб-ресурсам и туннелируемым ресурсам (см. Описание структуры сообщения в формате CEF на стр. 191).

- **Изменен интерфейс раздела** **Система**
  - Информация о транспортных сертификатах (см. Обновление транспортных сертификатов ViPNet TLS Gateway на стр. 151) перенесена на вкладку **TLS-подключение**.
  - Настройка передачи данных в формате CEF (на стр. 132) перенесена на вкладку **Оповещения**.
  - Вкладка **Шаблон пользовательской страницы** заменена на **Пользовательская страница**.
  - Добавлена вкладка **Дополнительные настройки** (см. Дополнительные настройки параметров подключения к ViPNet TLS Gateway на стр. 151).

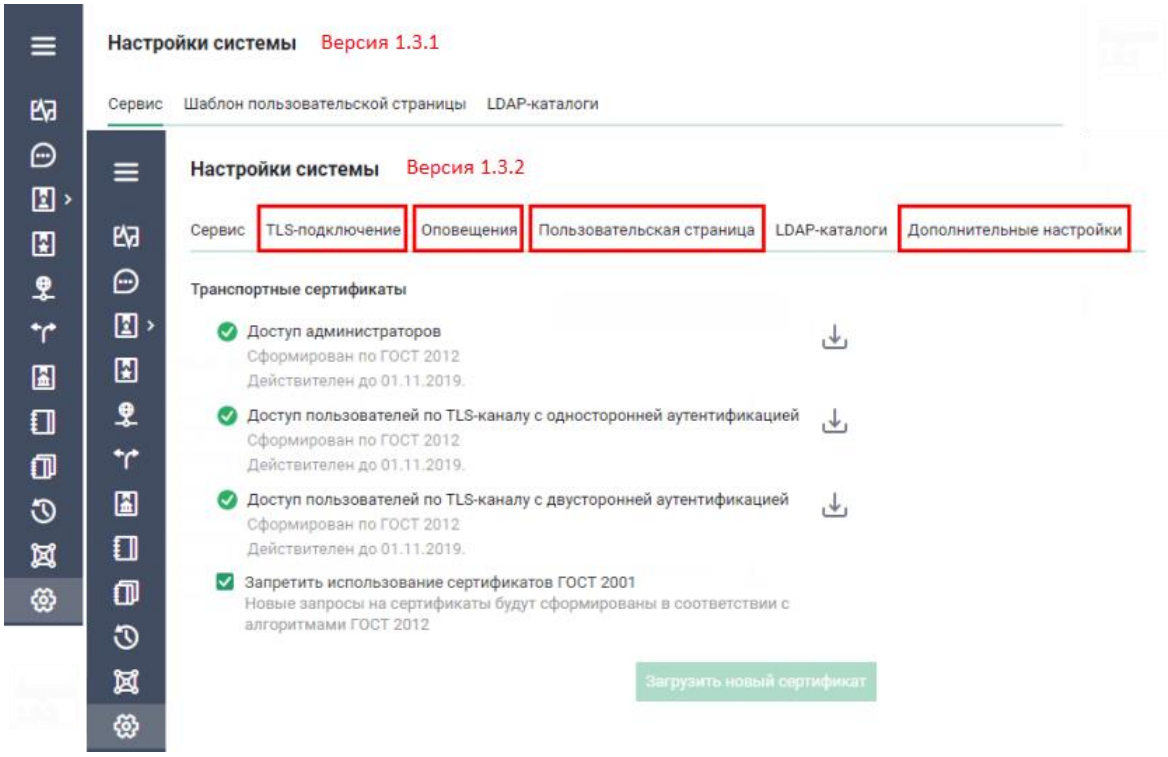

Рисунок 47. Изменение интерфейса в разделе Система

Новые возможности версии 1.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.3.1 по сравнению с версией 1.3.

- **Изменения в системе лицензирования**

  Теперь файл лицензии ограничивает:

  - Максимальное количество одновременных подключений по протоколу TLS с односторонней аутентификацией к веб-ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения.
  - Максимальное количество одновременных подключений по протоколу TLS с односторонней аутентификацией к туннелируемым ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения.
  - Максимальное количество одновременных подключений по протоколу TLS с двусторонней аутентификацией к веб-ресурсам и срок, в течение которого пользователи смогут осуществлять эти подключения.

Новые возможности версии 1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.3 по сравнению с версией 1.2.1.

- **Добавлена возможность туннелирования TCP-трафика по протоколу TLS**

  Вы можете настроить TLS-туннель для защиты данных в приложениях, которые работают через протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и SQL (см. Добавление TLS-туннеля на стр. 85). На компьютере клиента должен быть установлен TLS-клиент, поддерживающий протокол TLS 1.2, например, ViPNet PKI Client версии не ниже 1.3.

- **Изменения в правилах предоставления доступа пользователям к ресурсам**

  - Если в вашей организации используется служба каталогов Active Directory, вы можете импортировать из нее данные сотрудников в ViPNet TLS Gateway и использовать эти данные при создании правил предоставления доступа пользователям к ресурсам.
  - В предыдущей версии ViPNet TLS Gateway правила предоставления доступа к ресурсам применялись только к сертификатам новых пользователей. Теперь они также применяются к сертификатам существующих пользователей. При внесении изменений в правило происходит переназначение прав доступа к ресурсам пользователей, для которых применимо это правило.

- **Добавлена возможность развертывания виртуального образа ViPNet TLS Gateway без файла лицензии**

  Теперь вы можете устанавливать и активировать лицензию с помощью веб-интерфейса после проведения первоначальной инициализации. Например, если вы разворачиваете виртуальный образ на облачном сервере, к которому нет возможности подключить USB-носитель.

- **Обновлен веб-интерфейс**

  Переработан дизайн веб-интерфейса ViPNet TLS Gateway в соответствии с корпоративным стилем.

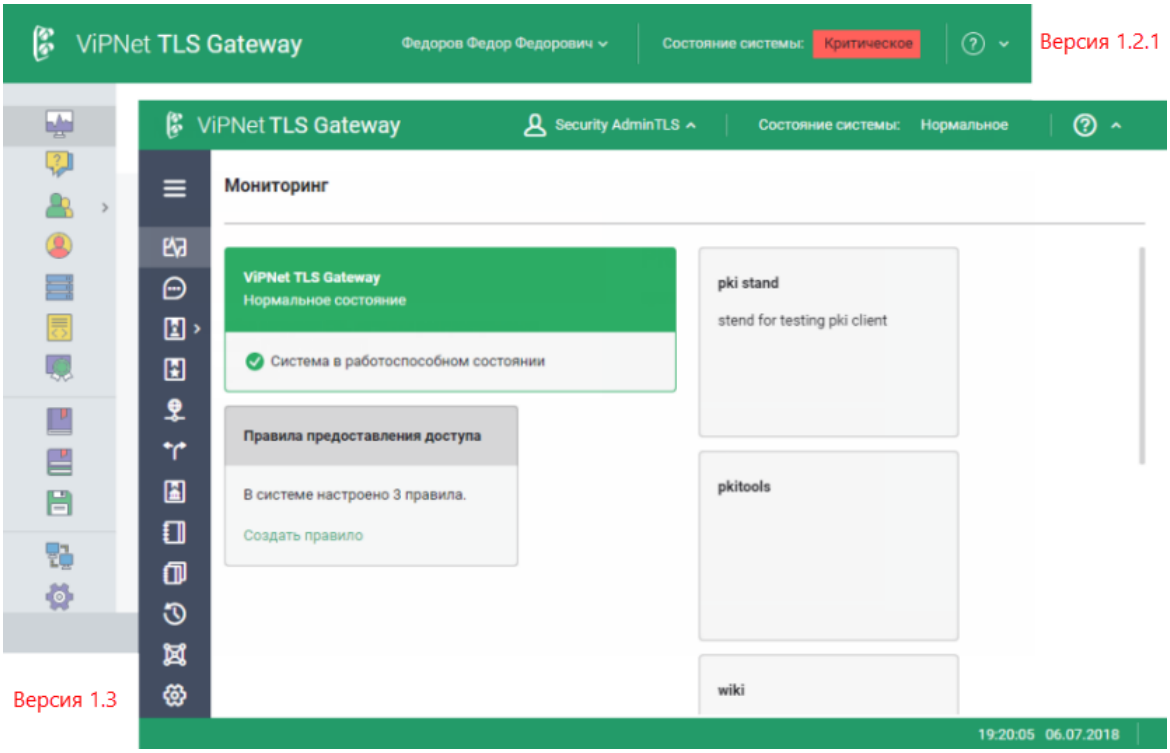

Рисунок 48. Веб-интерфейс ViPNet TLS Gateway 1.3

Новые возможности версии 1.2.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.2.1 по сравнению с версией 1.2.

- **Добавлен модуль Web Application Firewall**

  ViPNet TLS Gateway в исполнении TLS 1000 (см. Аппаратная архитектура TLS 1000 на стр. 13) теперь поставляется совместно с модулем Web Application Firewall (WAF), который обеспечивает защиту веб-ресурсов от известных и неизвестных атак, включая автоматизированные атаки и атаки нулевого дня. Для использования модуля WAF необходима соответствующая лицензия (см. Лицензирование на стр. 39). Подробнее о модуле WAF см. документ «ViPNet TLS Gateway Web Application Firewall. Руководство администратора».

Новые возможности версии 1.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.2 по сравнению с версией 1.1.1.

- **Передача данных в формате CEF**

  Реализована возможность автоматически передавать данные о работоспособности и лицензионных ограничениях ViPNet TLS Gateway в формате CEF в какую-либо систему управления событиями информационной безопасности (SIEM) (см. Настройка передачи данных в формате CEF на стр. 132).

- **Конструктор для создания правил предоставления доступа пользователям к ресурсам**

  Теперь для создания правил предоставления защищенного доступа к ресурсам пользователям по определенному признаку в их сертификате вы можете использовать удобный конструктор правил по различным полям сертификата (см. Задание условий выполнения правила на стр. 113).

- **Обновление ПО ViPNet TLS Gateway при локальном доступе**

  Теперь вы сможете обновить ПО ViPNet TLS Gateway, подключившись к ViPNet TLS Gateway локально (например, если пропал доступ к веб-интерфейсу ViPNet TLS Gateway) (см. Обновление и восстановление целостности ПО ViPNet TLS Gateway на стр. 157).

- **Восстановление целостности ViPNet TLS Gateway**

  Реализована возможность восстановить целостность ПО ViPNet TLS Gateway, подключившись к ViPNet TLS Gateway локально (см. Обновление и восстановление целостности ПО ViPNet TLS Gateway на стр. 157).

- **Совместная работа с ViPNet PKI Client и поддержка новых веб-браузеров**

  Теперь для обеспечения подключения администраторов к веб-интерфейсу ViPNet TLS Gateway низкоуровневые криптографические функции может выполнять ViPNet PKI Client. В этом случае для подключения к веб-интерфейсу ViPNet TLS Gateway реализована возможность помимо веб-браузера Internet Explorer использовать веб-браузеры Google Chrome, Mozilla Firefox, браузер «Спутник» последних версий (см. Требования к компьютеру администратора для подключения к веб-интерфейсу ViPNet TLS Gateway на стр. 68).

- **Использование символов национальных алфавитов (IDN-имен) в адресах защищаемых ресурсов**

  Реализована поддержка формата DNS-имен, содержащих символы национальных алфавитов (IDN-имен), например, статистика.рф. В связи с чем перед добавлением таких адресов защищаемых ресурсов на TLS Gateway нет необходимости преобразовывать их в кодировку Punycode.

- **Активация лицензии с помощью веб-интерфейса**

  Теперь в случае сбоя активации текущей лицензии или при необходимости обновиться на лицензию с другим серийным номером доступна возможность активации лицензии в режиме

реального времени с помощью веб-интерфейса ViPNet TLS Gateway (см. Обновление лицензии на стр. 148).

- **Изменение в интерфейсе**

  Меню **Настройки** перенесено с верхней панели (панели заголовка) в левую панель (панель навигации) главной страницы (см. Веб-интерфейс ViPNet TLS Gateway на стр. 70).

- **Взаимодействие с ViPNet TLS Gateway через Web API**

  Добавлена возможность взаимодействия с ViPNet TLS Gateway через интерфейс Web API (см. Описание интерфейса Web API на стр. 173). Этот интерфейс позволяет разработчикам встраивать в свои веб-приложения следующие функции:

  - Инициализация веб-приложения.
  - Отправка запроса на доступ к ресурсам.
  - Получение информации о запросах доступа к веб-ресурсам.
  - Получение списка защищаемых ресурсов.

Новые возможности версии 1.1.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.1.1 по сравнению с версией 1.1.

- **Безопасный выход администратора**

  Реализована возможность безопасно завершать работу с веб-интерфейсом под учетной записью текущего администратора (см. Подключение к веб-интерфейсу и завершение работы с ним на стр. 69).

- **Выгрузка служебных журналов для диагностики работы ViPNet TLS Gateway при локальном доступе**

  Теперь вы сможете сохранить служебные журналы для диагностики работы на внешний носитель, подключившись к ViPNet TLS Gateway локально (например, если пропал доступ к веб-интерфейсу ViPNet TLS Gateway) (см. Выгрузка служебных журналов для диагностики работы на стр. 155).

- **Контроль целостности ViPNet TLS Gateway**

  Теперь можно в любой момент, подключившись к ViPNet TLS Gateway локально, выполнить контроль целостности ViPNet TLS Gateway и получить контрольные комбинации изделия (ОС и ПО) (см. Контроль целостности ПО ViPNet TLS Gateway на стр. 154), чтобы затем сверить их с указанными в формуляре.

- **Использование ГОСТ Р 34.10-2001 для формирования транспортных ключей**

  Теперь вы можете выбрать, какой алгоритм использовать для формирования запросов на транспортные сертификаты (при первоначальной инициализации (см. Первоначальная инициализация ViPNet TLS Gateway на стр. 54) и при обновлении транспортных сертификатов при помощи веб-интерфейса (см. Обновление транспортных сертификатов ViPNet TLS Gateway на стр. 151)).

- **Настройка статических маршрутов**

  Теперь вы можете задать статические маршруты (см. Настройка статических маршрутов на стр. 138), если требуется явно указать маршрут прохождения сетевых пакетов, адресованных определенным узлам.

- **Защита резервной копии данных паролем**

  Теперь при выгрузке резервной копии данных на внешний носитель (см. Сохранение резервной копии данных на внешний носитель на стр. 163) предусмотрен механизм защиты с помощью пароля, который вводит администратор доступа. ViPNet TLS Gateway шифрует данные резервной копии, используя парольный ключ. При восстановлении из резервной копии необходимо ввести пароль для расшифрования архива резервной копии.

- **Смена пароля администратора локального доступа**

  Теперь при первоначальной инициализации вам необходимо сменить технологический пароль встроенной учетной записи администратора локального доступа на свой пароль, удовлетворяющий требованиям к паролю ViPNet TLS Gateway (см. Первоначальная

инициализация ViPNet TLS Gateway на стр. 54). В процессе работы можно изменять пароль администратора локального доступа с требуемой периодичностью.

- **Использование выделенного порта для перенаправления запросов от пользователей к веб-ресурсу**

  В параметрах веб-ресурса реализована возможность настроить выделенный порт для перенаправления запросов от пользователей к ресурсу (см. Добавление веб-ресурса на стр. 83). Работа через выделенный порт позволяет избежать дополнительной настройки правил преобразования URI ресурса для правильного отображения этого ресурса у пользователей.

Новые возможности версии 1.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet TLS Gateway версии 1.1 по сравнению с версией 1.0.

- **Изменения в лицензировании**

  Теперь базовая лицензия, входящая в комплект поставки, разрешает доступ пользователей к защищаемым ресурсам (см. глоссарий, стр. 209) только с помощью односторонней аутентификации по протоколу TLS. При необходимости обеспечить доступ пользователей к защищаемым ресурсам с помощью двусторонней аутентификации по протоколу TLS вам потребуется приобрести дополнительную лицензию на необходимое количество пользователей. Дополнительные лицензии можно запросить у службы технической поддержки ОАО «ИнфоТеКС».

- **Самотестирование**

  В ViPNet TLS Gateway реализована процедура самотестирования, которая заключается в проверке целостности ПО ViPNet TLS Gateway и контроле корректности его работы. Процедура самотестирования запускается автоматически при запуске ViPNet TLS Gateway и по расписанию один раз в 24 часа. Также администратор безопасности и администратор доступа могут запустить процедуру самотестирования вручную посредством веб-интерфейса ViPNet TLS Gateway (см. Самотестирование на стр. 133).

- **Повторная инициализация ViPNet TLS Gateway в случае проблем в обслуживании**

  При возникновении проблем в удаленном обслуживании ViPNet TLS Gateway с помощью веб-интерфейса теперь есть возможность непосредственно на ViPNet TLS Gateway в консоли Linux вместо полной первичной инициализации произвести повторную инициализацию и заново задать лишь необходимые настройки ViPNet TLS Gateway (см. Повторная инициализация ViPNet TLS Gateway на стр. 155).

- **Роль Администратор с правом локального доступа**

  Роль "Сервисный инженер" теперь называется "Администратор с правом локального доступа" и имеет ряд дополнительных полномочий (см. Администратор с правом локального доступа на стр. 34).

- **HTTPS-подключение ViPNet TLS Gateway к защищаемому ресурсу**

  Реализована возможность настроить подключение ViPNet TLS Gateway к защищаемому ресурсу для перенаправления запросов от пользователей по протоколу HTTPS (например, если защищаемый ресурс принимает запросы только по протоколу HTTPS).

- **Настройка логотипа ресурса**

  Теперь для каждого защищаемого ресурса вы можете загрузить логотип ресурса, который пользователи увидят на странице получения доступа к ресурсам рядом с названием ресурса.

- **Настройка шаблона отображения страницы доступа к ресурсам для пользователей**

  Теперь вы можете настроить внешний вид страницы получения доступа к ресурсам, которая отображается пользователям при подключении к ViPNet TLS Gateway. Доступен выбор фона

страницы и фона панели заголовка страницы с помощью загрузки графических файлов с необходимым фоном (см. Настройка шаблона отображения пользователю страницы доступа к ресурсам на стр. 89).

- **Импорт сертификатов УЦ из списка аккредитованных УЦ в формате Trust-service Status List (TSL)**

  Если сертификаты пользователей выданы в аккредитованных УЦ (см. глоссарий, стр. 208), вы можете добавить на ViPNet TLS Gateway сразу список сертификатов УЦ, импортировав их из списка аккредитованных УЦ https://e-trust.gosuslugi.ru/CA в формате Trust-service Status List (TSL) (см. глоссарий, стр. 208). Загрузить список аккредитованных УЦ в формате TSL вы можете с портала уполномоченного федерального органа в области использования электронной подписи (Минкомсвязи России) https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0.

- **Изменения в сетевых настройках**

  Реализована возможность задания сетевых настроек для всех доступных интерфейсов ViPNet TLS Gateway (см. Сетевые настройки на стр. 136).

- **Обновление ПО ViPNet TLS Gateway**

  Реализована возможность загрузки и установки обновления ПО ViPNet TLS Gateway с помощью веб-интерфейса ViPNet TLS Gateway (см. Обновление ПО ViPNet TLS Gateway на стр. 149).

C

Глоссарий

IP-адрес

Адрес узла в сети, построенной на основе протокола IP.

MAC-адрес

В большинстве технологий локальных сетей для однозначной адресации интерфейсов используются MAC-адреса (Media Access Control — управление доступом к среде). MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы сетевого уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, протокол разрешения адресов — Address Resolution Protocol, ARP).

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

TLS

Криптографический протокол, обеспечивающий защищенную передачу данных между узлами в Интернете. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Trust-service Status List (TSL)

Список доверенных поставщиков услуг. Задает формат доверенных списков аккредитованных УЦ. Список может содержать не только корневые сертификаты аккредитованных УЦ, а также включать в себя описания и ссылки на другие сервисы, предоставляемые аккредитованными УЦ, к которым относятся сервисы штампов времени (TSP), сервисы онлайн-проверки статусов сертификатов (OCSP) и другие.

URI

От англ. Uniform Resource Identifier — унифицированный (единообразный) идентификатор ресурса в сети. Последовательность символов, идентифицирующая абстрактный или физический ресурс.

ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей электронной подписи.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

Аккредитованный удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти http://minsvyaz.ru/ru/activity/govservices/2/#section-list-of-accredited-centers в соответствии с требованиями Федерального закона от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является

тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Доверенная зона

Доверенная зона содержит сетевые узлы, которые считаются безопасными друг для друга. Понятие доверенной зоны определяется политикой безопасности организации, эксплуатирующей ViPNet TLS Gateway. Например, доверенной зоной может считаться периметр помещения, в котором установлен ViPNet TLS Gateway.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Защищаемый ресурс

Веб-ресурс, к которому с помощью ViPNet TLS Gateway организуется защищенный удаленный доступ пользователей по протоколу TLS.

Квалифицированный сертификат

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Корневой сертификат

Сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

Расширения сертификата ключа проверки электронной подписи

Дополнительные атрибуты сертификата, такие как использование ключа, политики сертификата, базовые ограничения, ограничения имени и другие. Расширение может быть критичным или некритичным. Система, использующая сертификаты, должна отвергать сертификат, если она встретила критичное расширение, которое не в состоянии распознать; однако некритичные расширения могут игнорироваться, если они не распознаются. Каждое расширение сертификата должно иметь соответствующий идентификатор объекта (OID).

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Системы управления событиями информационной безопасности

Системы управления событиями информационной безопасности (SIEM, ESM и т.д.) — предназначены для сбора и анализа сообщений, поступающих от различных источников: систем обнаружения вторжений, межсетевых экранов, антивирусных систем, сетевых устройств, операционных систем, различных приложений и т.д., и дальнейшего выявления отклонений от норм информационной безопасности по заданным критериям. При выявлении отклонений производится оповещение операторов системы о выявленных инцидентах.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Транспортный сертификат ViPNet TLS Gateway

Сертификат серверной аутентификации при взаимодействии по протоколу TLS между ViPNet TLS Gateway и пользователями (или администраторами). Представляет собой сертификат ключа проверки электронной подписи, в котором указан IP-адрес (или DNS-имя) сетевого интерфейса ViPNet TLS Gateway для подключения пользователей (или администраторов) и который имеет расширение «Расширенное использование ключа» с назначением ключа «Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)». Для ViPNet TLS Gateway издаются следующие транспортные сертификаты: сертификат для подключения администраторов, сертификат для подключения пользователей по TLS-каналу с односторонней аутентификацией, сертификат для подключения пользователей по TLS-каналу с двусторонней аутентификацией.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Цепочка доверия к сертификатам

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. При криптографических операциях каждый сертификат из цепочки проверяется на следующем сертификате. Сертификат считается действительным, если цепочка доверия полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, который позволяет инициализировать датчик случайных чисел на основе действий пользователя. Полученная последовательность используется при формировании ключей узла.