ViPNet SIES MC

Установка и обслуживание

infotecs

© ОАО «ИнфоТеКС», 2020

ФРКЕ.00194-02 90 01

Версия продукта 2.2.2

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 6
О документе 7
Для кого предназначен документ 7
Комплект документации ViPNet SIES MC 7
Соглашения документа 7
Обратная связь 9

Глава 1. Подготовка к эксплуатации 10
Порядок действий 11
Установка ПАК ViPNet SIES MC 13
Установка ViPNet SIES MC VA 14
Инициализация ПАК ViPNet SIES MC 15
Инициализация ViPNet SIES MC VA 22

Глава 2. Организация работы администраторов ViPNet SIES MC 23
Организация защищенного подключения администратора к веб-интерфейсу ViPNet SIES MC 24
Порядок действий 24
Подготовка рабочего места администратора 25
Начало работы с веб-интерфейсом 26
Описание веб-интерфейса 27
Управление доступом администраторов к веб-интерфейсу ViPNet SIES MC 29
Добавление нового администратора 29
Просмотр сведений об администраторах 31
Управление ролями администратора 32
Изменение полномочий администратора по управлению группами 33
Обновление сертификата администратора 34
Удаление администратора 35
Компрометация администратора 36

Глава 3. Управление и настройка 37
Управление и настройка из веб-интерфейса 38
Сетевые настройки 38
Изменение сетевых настроек 38
Активация дополнительного сетевого интерфейса 40
Службы доставки защищенных конвертов 40

Добавление службы 41
Изменение параметров службы 42
Удаление службы 43
Сертификаты и ключи 44
Просмотр сертификатов и ключей 44
Экспорт сертификатов 45
Выпуск и обновление сертификатов и ключей 46
Мониторинг работоспособности 51
Просмотр сообщений мониторинга 52
Подготовка архива служебных журналов 53
Работа с журналами событий 54
Просмотр журнала событий 54
Экспорт архива записей о событиях 55
Удаление архива записей о событиях 56
Просмотр лицензии 56
Обновление и активация лицензии 56
Обновление ПО 58
Контроль целостности ПО из веб-интерфейса 59
Управление и настройка из консоли Linux 61
Выгрузка служебных журналов 61
Контроль целостности ПО ViPNet SIES MC 62
Создание резервной копии ключевой информации 63
Повторная инициализация ViPNet SIES MC 64
Смена пароля администратора с правом локального доступа 65
Изменение уровня детализации записей служебных журналов 66
Перезагрузка ViPNet SIES MC 67
Выключение ViPNet SIES MC 67
Подготовка к выводу из эксплуатации 67

Глава 4. Резервное копирование и восстановление данных 69
Общие сведения 70
Создание резервной копии рабочей информации 72
Экспорт резервной копии рабочей информации 73
Восстановление данных из резервной копии 75
Восстановление данных после программного сбоя 75
Восстановление данных после аппаратного сбоя 76

Приложение А. Уровни критичности событий 79

Приложение B. Возможные неполадки и способы их устранения **80**

Администратор не может подключиться к веб-интерфейсу 81

Не удается загрузить веб-интерфейс ViPNet SIES MC 83

Не удается загрузить веб-интерфейс ViPNet SIES MC с использованием ViPNet PKI Client TLS Unit 84

Блокировка работы ViPNet SIES MC 85

Сообщение о превышении лицензионных ограничений 86

Не удается создать прикладной мастер-ключ 87

Приложение C. Глоссарий **88**

Введение

О документе 7

Обратная связь 9

О документе

В данном документе вы найдете информацию по установке и настройке центра ViPNet® SIES MC, управляющего компонентами комплекса ViPNet SIES в индустриальной системе.

Документ содержит методику установки и настройки ViPNet SIES MC и рабочих мест администраторов ViPNet SIES MC, методику резервного копирования и восстановления данных ViPNet SIES MC.

Для кого предназначен документ

Данный документ предназначен для администраторов, устанавливающих, настраивающих и управляющих ViPNet SIES MC.

Предполагается, что администратор обладает базовым представлением о криптографической защите данных, а также об устройстве компьютерных и индустриальных систем, опытом работы с Linux в качестве пользователя.

Комплект документации ViPNet SIES MC

В комплект документации ViPNet SIES MC входят следующие документы:

1. ViPNet SIES MC. Быстрый старт.
2. ViPNet SIES MC. Общее описание.
3. ViPNet SIES MC. Установка и обслуживание.
4. ViPNet SIES MC. Руководство администратора.
5. ViPNet SIES MC. Руководство разработчика.
6. ViPNet SIES MC. Лицензионные соглашения на компоненты сторонних производителей.

Совет. Рекомендуем вам знакомиться с документами в указанном порядке.

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.

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

Подготовка к эксплуатации

Порядок действий 11

Подготовка цепочки сертификатов 12

Подготовка списка аннулированных сертификатов **Ошибка! Закладка не определена.**

Установка ПАК ViPNet SIES MC 13

Установка ViPNet SIES MC VA 14

Инициализация ViPNet SIES MC 15

Порядок действий

Ввод ViPNet SIES MC в эксплуатацию выполняется администратором с правом локального доступа.

Чтобы ввести в эксплуатацию ViPNet SIES MC, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 3. Порядок подготовки к эксплуатации ViPNet SIES MC

	Действие	Ссылка
☐	Распределите роли администраторов ViPNet SIES MC между сотрудниками вашей организации, которым назначены определенные задачи управления SIES-узлами.	ViPNet SIES MC. Общее описание > Полномочия администраторов.
☐	Если в сценариях защиты данных будут использоваться ViPNet SIES Core или ViPNet SIES Unit, из числа администраторов ViPNet SIES MC с ролью администратора группы выделите сотрудника для выполнения инициализации ViPNet SIES Core или ViPNet SIES Unit с помощью ViPNet SIES Workstation.	См. там же.
☐	Если вы планируете создать в ViPNet SIES MC структуру групп защищаемых устройств и SIES-узлов (например, отражающих структуру индустриальной системы), из числа администраторов ViPNet SIES MC с ролью администратора группы выделите сотрудников для управления отдельными группами элементов.	ViPNet SIES MC. Общее описание > Полномочия администраторов > Администратор группы.
☐	Подготовьте рабочие места администраторов ViPNet SIES MC независимо от назначенной роли.	Подготовка рабочего места администратора (на стр. 25).
☐	На рабочем месте супер-администратора создайте запрос на сертификат (см. глоссарий, стр. 89) администратора.	• См. документацию на используемый криптопровайдер (см. глоссарий, стр. 91). • См. ViPNet SIES MC. Общее описание > Ключевая информация и сертификаты > Требования к сертификатам пользовательской ключевой подсистемы.
☐	Доверенным способом (см. глоссарий, стр. 89) передайте запрос на сертификат администратору удостоверяющего центра для издания сертификата администратора ViPNet SIES MC.	

	Действие	Ссылка
☐	На рабочем месте супер-администратора установите: • цепочку сертификатов (см. глоссарий, стр. 93) для корневого сертификата пользовательской ключевой подсистемы ViPNet SIES (см. глоссарий, стр. 91); • список аннулированных сертификатов удостоверяющего центра (см. глоссарий, стр. 92); • изданный сертификат администратора (см. глоссарий, стр. 92).	См. документацию на используемый криптопровайдер.
☐	На USB-носитель с любой файловой системой, кроме NTFS, запишите: • цепочку сертификатов для корневого сертификата пользовательской ключевой подсистемы ViPNet SIES; • список аннулированных сертификатов удостоверяющего центра; • изданный сертификат администратора.	
☐	Установите ViPNet SIES MC.	• Установка ПАК ViPNet SIES MC (на стр. 13). • См. ViPNet SIES MC VA. Руководство по развертыванию.
☐	Выполните инициализацию ViPNet SIES MC.	• Инициализация ПАК ViPNet SIES MC (на стр. 15). • См. ViPNet SIES MC VA. Руководство по развертыванию.
☐	На рабочем месте супер-администратора подключитесь к веб-интерфейсу ViPNet SIES MC.	• Начало работы с веб-интерфейсом (на стр. 26). • См. документацию на используемый криптопровайдер.
☐	Если в сценариях защиты данных будут использоваться ViPNet SIES Core или ViPNet SIES Unit, добавьте оператора ViPNet SIES Workstation с ролью администратора группы.	Добавление нового администратора (на стр. 29).
☐	На рабочем месте супер-администратора откройте список аннулированных сертификатов пользовательской ключевой системы ViPNet SIES. Запланируйте обновление списка аннулированных сертификатов на дату, предшествующую дате в поле **Следующее обновление**.	• Обновление списка аннулированных сертификатов (на стр. 48). • Автоматическое обновление списка аннулированных сертификатов из точки распространения (на стр. 48).

После ввода в эксплуатацию ViPNet SIES MC вы можете перейти к добавлению защищаемых устройств индустриальной системы и SIES-узлов. Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».

Установка ПАК ViPNet SIES MC

Чтобы установить ПАК ViPNet SIES MC:

1. Разместите ПАК ViPNet SIES MC в контролируемой зоне (см. глоссарий, стр. 90), исключающей неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска в соответствии с требованиями безопасности, применяемыми в вашей организации.
2. К ПАК ViPNet SIES MC подключите монитор и клавиатуру.

   При подключении устройств соблюдайте требования, приведенные в разделе «Правила работы с ПАК ViPNet SIES MC» главы «Организация работы ViPNet SIES MC» документа «ViPNet SIES MC. Общее описание».
3. Подключите коммутационный шнур Ethernet к коммуникационному порту на передней панели ПАК ViPNet SIES MC. Подробнее см. документ «ViPNet SIES MC. Общее описание».
4. Подключите ПАК ViPNet SIES MC к электропитанию.
5. Включите ПАК ViPNet SIES MC.
6. Дождитесь загрузки Linux и старта мастера инициализации.
7. Переходите к инициализации ViPNet SIES MC (на стр. 15).

Установка ViPNet SIES MC VA

Действия по вводу в эксплуатацию программного исполнения ViPNet SIES MC VA приведены в документе «ViPNet SIES MC VA. Руководство по развертыванию».

Инициализация ПАК ViPNet SIES MC

Чтобы ввести ViPNet SIES MC в эксплуатацию, выполните инициализацию ViPNet SIES MC.

Инициализация выполняется уполномоченным сотрудником вашей организации, которому назначена роль администратора с правом локального доступа.

Перед началом инициализации ViPNet SIES MC у администратора локальной сети получите:

- IP-адрес для подключения ViPNet SIES MC;
- маску подсети, к которой принадлежит IP-адрес;
- IP-адрес сетевого шлюза по умолчанию;
- IP-адрес DNS-сервера.

Чтобы инициализировать ViPNet SIES MC:

1. Подключите USB-носитель версии 2.0 с файловой системой FAT32 для экспорта запроса на сертификат ViPNet SIES MC для подключения администраторов к аппаратной платформе с инициализируемым ПО ViPNet SIES MC.
2. Авторизуйтесь в консоли Linux:
   - на приглашение **login** введите `root` и нажмите клавишу **Enter**;
   - на приглашение **Password** введите технологический пароль `vipnet` и нажмите клавишу **Enter**.

> **Примечание.** Ввод любой последовательности символов следует завершать клавишей **Enter**. В дальнейшем описании последовательности инициализации упоминание этого шага опущено.

3. Задайте новый пароль учетной записи администратора с правом локального доступа:

Внимание! Пароль должен соответствовать следующим требованиям:

- иметь длину от 8 до 32 символов;
- содержать хотя бы одну цифру от 0 до 9;
- содержать хотя бы одну букву латинского алфавита от «A» до «Z» или от «a» до «z».

Пароль может содержать символы «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}».

Дополнительно не рекомендуется использовать:

- три и более символа, расположенные подряд на клавиатуре;
- три и более символа, идущие подряд в алфавитном порядке;
- один и тот же символ более двух раз.

3.1 На запрос **Enter new password** введите пароль.

3.2 На запрос **Confirm password** повторно введите тот же пароль.

4 Из предложенного списка действий выберите первичную инициализацию **First initialization**, введя символ `1`.

Примечание. В случае перезагрузки ViPNet SIES MC в процессе инициализации, мастер инициализации предложит вам пропустить ранее пройденные шаги. Если вы уверены в заданных настройках, на запрос **Skip** о каждом ранее пройденном шаге инициализации введите символ `y` для пропуска шага.

5 Задайте часовой пояс, дату и время. Для этого:

5.1 На запрос выбора континента **Please select a continent or ocean** введите номер вашего континента из предложенного списка. Например, Российская Федерация отнесена к континенту **Europe** (Европа), поэтому введите значение `8`.

5.2 На запрос выбора страны **Please select a country** введите номер вашей страны из предложенного списка. Например, чтобы выбрать **Russia** (Россия), введите значение `39`.

5.3 На запрос выбора часового пояса **Please select one of the following time zone regions** введите номер вашего часового пояса из предложенного списка. Например, чтобы выбрать часовой пояс **Moscow area** (Московский регион) введите значение `2`.

5.4 На запрос **Is the above information OK** введите `y`, если заданные вами значения верны или введите символ `n` для повторного ввода значений часового пояса.

5.5 На запрос **Enter new system date** введите дату и время согласно всемирному координированному времени (UTC) и локальному часовому поясу с погрешностью не более 1 минуты. Новые значения вводите в формате в формате `Год-месяц-день часы:минуты:секунды`. Если изменять дату и время не требуется, нажмите клавишу **Enter**.

6 Задайте сетевые настройки ViPNet SIES MC и параметры подключения администраторов к веб-интерфейсу ViPNet SIES MC по TLS-каналу. Для этого:

6.1 На запрос **Enter ViPNet SIES MC web interface port** введите номер порта подключения администраторов к веб-интерфейсу ViPNet SIES MC, если вы хотите изменить установленное по умолчанию значение порта, указанное в скобках (`443`). Если изменять номер порта не требуется, нажмите клавишу **Enter**.

6.2 На запрос **Choose network interface for ViPNet SIES MC web interface** из предложенного списка введите номер сетевого интерфейса, через который администраторы ViPNet SIES MC будут подключаться к веб-интерфейсу ViPNet SIES MC.

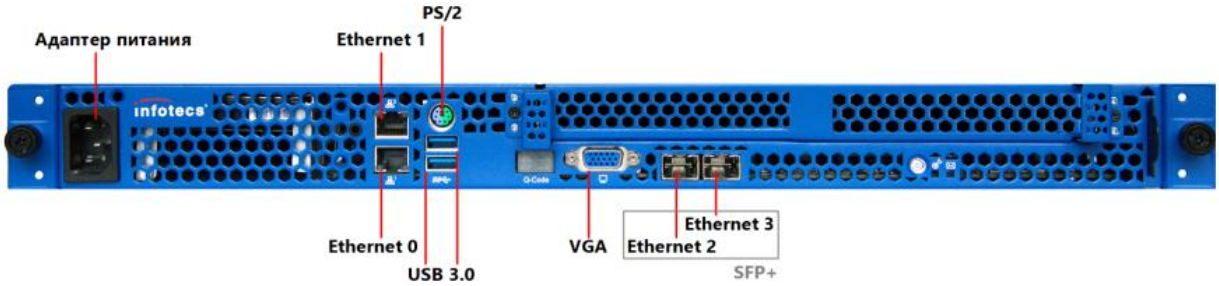

Рисунок 1. Передняя панель ViPNet SIES MC 10000 Q1

Таблица 4. Соответствие наименований портов сетевым интерфейсам аппаратной платформы ViPNet SIES MC 10000 Q1

Наименование порта	Обозначение интерфейса в мастере инициализации
Ethernet 0	enp5s0
Ethernet 1	enp6s0
Ethernet 2	enp3s0f0
Ethernet 3	enp3s0f1

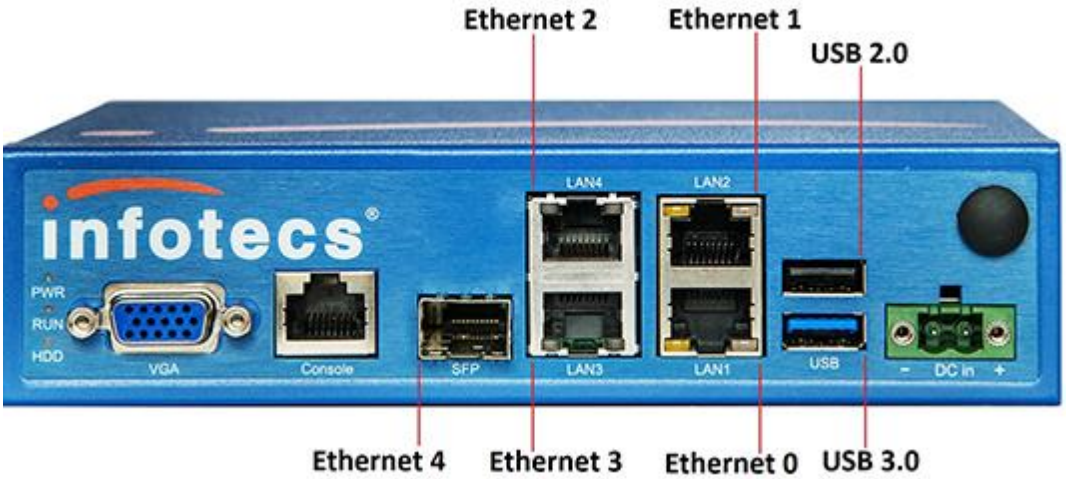

Рисунок 2. Передняя панель ViPNet SIES MC 3000 N1

Таблица 5. Соответствие наименований портов сетевым интерфейсам аппаратной платформы ViPNet SIES MC 3000 N1

Наименование порта	Обозначение интерфейса в мастере инициализации	Обозначение интерфейса на передней панели аппаратной платформы
Ethernet 0	enp1s0	LAN1
Ethernet 1	enp2s0	LAN2
Ethernet 2	enp6s0	LAN4
Ethernet 3	enp5s0	LAN3
Ethernet 4	enp7s0	SFP

6.3 На запрос **Enter new IP address** для заданного сетевого интерфейса введите IP-адрес, полученный у администратора локальной сети.

6.4 На запрос **Enter new netmask** введите маску подсети, полученную у администратора локальной сети.

6.5 На запрос **Enter new default gateway** введите IP-адрес сетевого шлюза по умолчанию, полученный у администратора локальной сети.

6.6 На запрос **Enter new DNS servers** введите IP-адрес DNS-сервера, полученный у администратора локальной сети. При вводе нескольких значений IP-адресов разделяйте их точкой с запятой без пробелов.

6.7 На запрос **Select new DNS servers** введите символ `n`, если заданные вами значения верны или введите символ `y` для повторного ввода значений IP-адреса DNS-сервера.

7 Задайте параметры сертификата ViPNet SIES MC для подключения администраторов к веб-интерфейсу ViPNet SIES MC по TLS-каналу.

На запрос **Enter Subject.CN field value for ViPNet SIES MC administrator connection certificate** введите заданный вами ранее IP-адрес или соответствующее заданному IP-адресу доменное имя узла ViPNet SIES MC.

Введите одно или несколько DNS-имен ViPNet SIES MC или сохраните значение IP-адреса сетевого интерфейса, указанное в скобках, нажав клавишу **Enter**. При вводе нескольких значений DNS-имен или IP-адресов разделяйте их точкой с запятой без пробелов.

Затем запустится процесс создания первичной ключевой информации и ключей электронной подписи.

Внимание! В зависимости от исполнения ViPNet SIES MC процесс создания ключей может занять до полутора часов. Дождитесь окончания процесса создания ключей, не прерывая его.

Признаком окончания создания ключей электронной подписи служит появление на экране следующего запроса мастера инициализации ViPNet SIES MC.

8 На запрос **Do you want to create backup set of keys** введите символ `y`, чтобы создать резервную копию ключевой информации ViPNet SIES MC.

Внимание! Настоятельно рекомендуем создать и сохранить в надежном месте резервную копию ключевой информации. Вы сможете создать резервную копию повторно по завершении инициализации ViPNet SIES MC (на стр. 63). Создание файла с резервной копией ключевой информации может занять до 15 минут.

8.1 На запрос **Enter full path to backup set of keys file** введите полный путь к файлу на подключенном USB-носителе для экспорта резервной копии ключевой информации.

Например, чтобы сохранить резервную копию в файл `keys.backup` в корневом каталоге USB-носителя, введите `/media/usb0/keys.backup`.

Примечание. Все промежуточные каталоги, указанные в пути, следует создать заранее.

8.2 На запрос **Enter password to protect backup file** введите пароль к файлу с резервной копией.

8.3 На запрос **Confirm password** вновь введите тот же пароль.

После подтверждения пароля на USB-носитель будет экспортирована резервная копия ключевой информации ViPNet SIES, которую вы сможете использовать для восстановления работоспособности ViPNet SIES MC после аппаратного или программного сбоя.

9 На запрос **Enter full path to save ViPNet SIES MC administrator connection certificate request file** введите полный путь к каталогу на подключенном USB-носителе для экспорта запроса на сертификат ViPNet SIES MC для подключения администраторов.

Например, чтобы сохранить запрос на сертификат в корневой каталог USB-носителя, укажите каталог автоматического монтирования USB-носителя: `/media/usb0/`.

Примечание. При вводе пути соблюдайте регистр букв в названиях каталогов. Вы можете автоматически дополнять вводимые последовательности символов нажатием клавиши **Tab**. Все введенные вами значения запоминаются в текущем сеансе работы с мастером. Для выбора значения из истории ввода можно использовать клавиши со стрелками вверх и вниз.

После ввода пути на USB-носитель в указанную папку будет экспортирован файл `admin_nginx.p10` с запросом на сертификат ViPNet SIES MC для подключения администраторов.

10 Отключите USB-носитель.

11 Передайте файл `admin_nginx.p10` с запросом на сертификат администратору внешнего удостоверяющего центра для издания сертификата ViPNet SIES MC.

Если в удостоверяющем центре издание сертификата ViPNet SIES MC для подключения администраторов займет длительное время, вы можете прервать инициализацию ViPNet SIES MC и выключить аппаратную платформу с инициализируемым ПО ViPNet SIES MC.

Чтобы прервать инициализацию ViPNet SIES MC:

1 Нажмите клавиши **Ctrl+C**.

2 На запрос **Do you want to quit from initialization process** введите символ `y`.

3 Отключите питание аппаратной платформы с инициализируемым ПО ViPNet SIES MC.

Получив изданный сертификат ViPNet SIES MC для подключения администраторов из удостоверяющего центра:

1 Запишите на USB-носитель следующие файлы:

- изданный внешним удостоверяющим центром сертификат ViPNet SIES MC для подключения администраторов (должен удовлетворять требованиям, приведенным в документе «ViPNet SIES MC. Общее описание»);
- корневой сертификат внешнего удостоверяющего центра;
- список аннулированных сертификатов внешнего удостоверяющего центра;
- сертификат администратора ViPNet SIES MC, которому будет назначена роль супер-администратора.

2 Подключите USB-носитель к аппаратной платформе с инициализируемым ПО ViPNet SIES MC.

3 Если вы выключали аппаратную платформу с инициализируемым ПО ViPNet SIES MC:

3.1 Включите аппаратную платформу с инициализируемым ПО ViPNet SIES MC.

3.2 Дождитесь загрузки Linux.

3.3 Авторизуйтесь в консоли Linux как суперпользователь `root`.

3.4 Из предложенного списка действий выберите первичную инициализацию **First initialization**, введя символ `1`.

3.5 Пропустите все ранее пройденные шаги инициализации. Если вы уверены в заданных настройках, на запрос **Skip** о каждом ранее пройденном шаге инициализации введите символ `y` для пропуска шага.

3.6 На запрос **Load CA certificate and CRL Skip** введите символ `n`.

4 На запрос **Enter full path to CA certificate of ViPNet SIES user key management subsystem file to import** введите полный путь к файлу:

- с корневым сертификатом пользовательской ключевой подсистемы ViPNet SIES;
- с корневым сертификатом головного удостоверяющего центра, если цепочка сертификатов удостоверяющего центра, выдавшего корневой сертификат пользовательской ключевой подсистемы ViPNet SIES, состоит более чем из одного сертификата.

5 На запрос **Enter full path for CRL file to import** введите полный путь к файлу со списком аннулированных сертификатов удостоверяющего центра для сертификата, загруженного на предыдущем шаге.

6 Если цепочка сертификатов удостоверяющего центра, выдавшего корневой сертификат пользовательской ключевой подсистемы ViPNet SIES, состоит более чем из одного сертификата издателей, загрузите промежуточные сертификаты и соответствующие списки аннулированных сертификатов:

6.1 На запрос **Do you want to install other CA certificate and CRL** введите символ `y`.

6.2 На запрос **Enter full path to CA certificate of ViPNet SIES user key management subsystem file to import** введите полный путь к файлу с промежуточным сертификатом цепочки.

6.3 На запрос **Enter full path for CRL file to import** введите полный путь к файлу со списком аннулированных сертификатов, соответствующим загруженному промежуточному сертификату.

6.4 Если нужно загрузить другой промежуточный сертификат и соответствующий список аннулированных сертификатов, на запрос **Do you want to install other CA certificate and CRL** введите символ `y` и повторите шаги 6.2–6.3.

Если все сертификаты цепочки загружены, введите символ `n`.

7 На запрос **Enter full folder path, from which ViPNet SIES MC administrator connection certificate file will be imported** введите полный путь к каталогу с файлом сертификата ViPNet SIES MC для подключения администраторов.

8 На запрос **Enter full path for ViPNet SIES MC Super-administrator certificate file to import** введите полный путь к файлу с сертификатом администратора ViPNet SIES MC, которому будет назначена роль супер-администратора.

9 На запрос **Do you want to complete ViPNet SIES MC initialization** подтвердите завершение настроек, введя символ `y`.

Появится сообщение мастера инициализации о завершении настройки.

10 Отсоедините USB-носитель.

11 Для продолжения нажмите клавишу **Enter**.

Последует перезагрузка Linux и ПО ViPNet SIES MC.

Инициализация ViPNet SIES MC завершена.

Инициализация ViPNet SIES MC VA

Действия по вводу в эксплуатацию программного исполнения ViPNet SIES MC VA приведены в документе «ViPNet SIES MC VA. Руководство по развертыванию».

2

Организация работы администраторов ViPNet SIES MC

Организация защищенного подключения администратора к веб-интерфейсу ViPNet SIES MC 24

Начало работы с веб-интерфейсом 26

Описание веб-интерфейса 27

Управление доступом администраторов к веб-интерфейсу ViPNet SIES MC 29

Организация защищенного подключения администратора к веб-интерфейсу ViPNet SIES MC

Подключение администраторов к веб-интерфейсу ViPNet SIES MC выполняется по каналу передачи данных, защищенному протоколом TLS с двусторонней аутентификацией (см. глоссарий, стр. 89) по российским криптографическим алгоритмам в соответствии с ГОСТ Р 34.10-2012.

Порядок действий

Чтобы подключить администратора к веб-интерфейсу ViPNet SIES MC, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 6. Порядок организации подключения администратора к веб-интерфейсу ViPNet SIES MC

	Действие	Ссылка
☐	Подготовьте рабочее место подключаемого администратора.	Подготовка рабочего места администратора (на стр. 25).
☐	На рабочем месте администратора создайте запрос на сертификат администратора.	• См. документацию на используемый криптопровайдер. • См. ViPNet SIES MC. Общее описание > Ключевая информация и сертификаты > Требования к сертификатам пользовательской ключевой подсистемы.
☐	Доверенным способом передайте запрос на сертификат администратору удостоверяющего центра для издания сертификата.	
☐	На рабочем месте подключаемого администратора установите: • цепочку сертификатов для корневого сертификата пользовательской ключевой подсистемы ViPNet SIES; • список аннулированных сертификатов удостоверяющего центра; • изданный сертификат администратора.	• См. документацию на используемый криптопровайдер. • Сертификат администратора должен удовлетворять требованиям, приведенным в документе «ViPNet SIES MC. Общее описание».
☐	На рабочем месте супер-администратора подключитесь к веб-интерфейсу ViPNet SIES MC.	• Начало работы с веб-интерфейсом (на стр. 26). • См. документацию на используемый криптопровайдер.

	Действие	Ссылка
☐	С полномочиями супер-администратора добавьте в ViPNet SIES MC сертификат администратора и назначьте администратору роли управления.	Добавление нового администратора (на стр. 29).
☐	На рабочем месте подключаемого администратора подключитесь к веб-интерфейсу ViPNet SIES MC.	Начало работы с веб-интерфейсом (на стр. 26).

Перечисленные действия выполните на рабочем месте каждого из администраторов ViPNet SIES MC.

Подготовка рабочего места администратора

Перед началом работы с веб-интерфейсом ViPNet SIES MC на рабочем месте:

1. Установите актуальные пакеты обновлений ОС.
2. Обновите браузер до актуальной версии.
3. Установите криптопровайдер, обеспечивающий TLS-соединения с двусторонней аутентификацией и поддерживающий российские криптографические алгоритмы по ГОСТ Р 34.10-2012.
4. Для удобства работы с веб-интерфейсом ViPNet SIES MC установите разрешение экрана монитора не менее 1360 x 768 пикселей.

Начало работы с веб-интерфейсом

С помощью веб-интерфейса ViPNet SIES MC вы можете управлять SIES-узлами и защищаемыми устройствами. Ваши полномочия работы с ViPNet SIES MC определяются назначенной вам ролью управления.

Перед началом работы с веб-интерфейсом ViPNet SIES MC организуйте защищенное подключение к ViPNet SIES MC по TLS-протоколу (на стр. 24).

Чтобы подключиться к веб-интерфейсу ViPNet SIES MC:

1 Откройте браузер и введите адрес `https://<адрес:порт>`, где `<адрес>` — IP-адрес сетевого интерфейса администрирования ViPNet SIES MC.

> **Совет.** Если при инициализации ViPNet SIES MC номер порта защищенных подключений администраторов остался в значении, установленном производителем, то в адресной строке браузера номер порта можно не указывать.

2 По запросу выберите сертификат администратора ViPNet SIES MC, который вы установили в хранилище криптопровайдера.

3 После двусторонней аутентификации установится защищенное соединение по протоколу TLS между вашим рабочим местом и ViPNet SIES MC.

4 Откроется главная страница веб-интерфейса ViPNet SIES MC с функциями ViPNet SIES MC.

> **Совет.** Для удобства работы с веб-интерфейсом ViPNet SIES MC рекомендуется использовать монитор с диагональю экрана не менее 13 дюймов и разрешением не менее 1360 x 768 пикселей.

Чтобы завершить работу с веб-интерфейсом ViPNet SIES MC, закройте окно браузера.

Описание веб-интерфейса

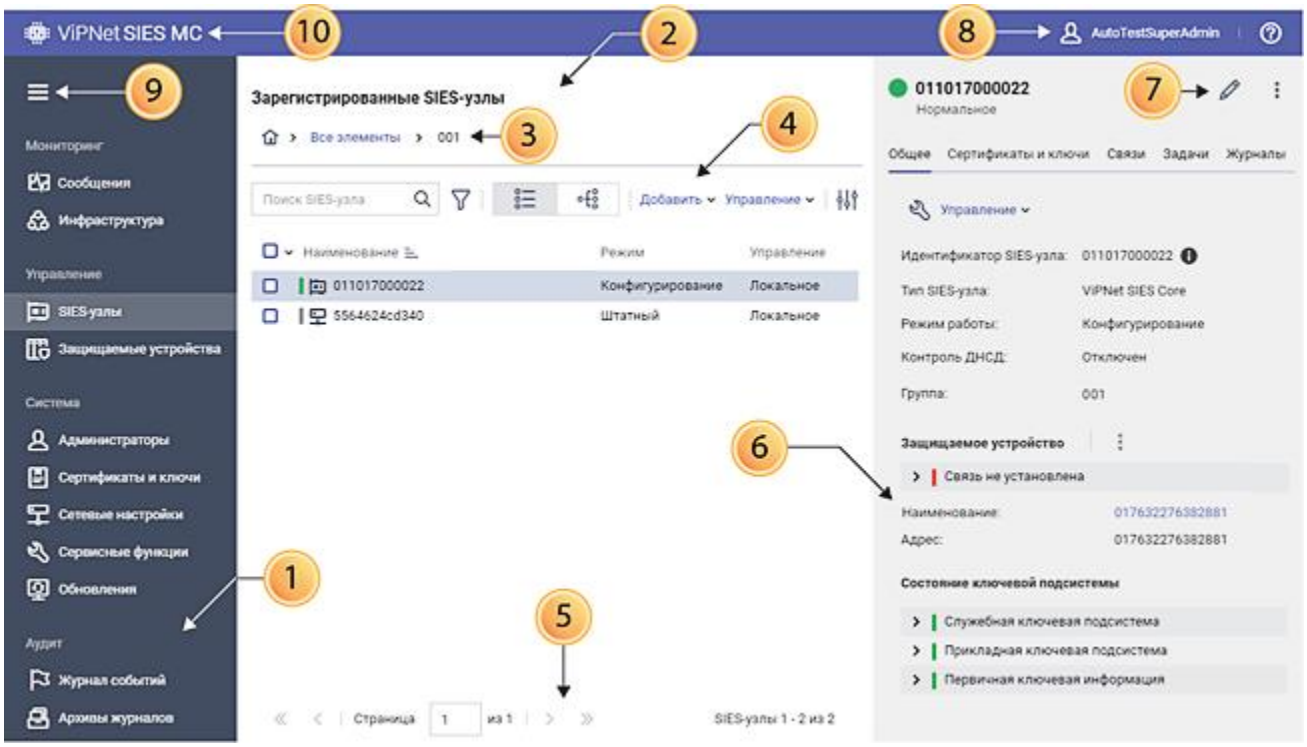

Рисунок 3. Веб-интерфейс ViPNet SIES MC

Цифрами на рисунке обозначены:

1 Панель навигации — содержит разделы ViPNet SIES MC:

- **Сообщения** — предоставляет текущее состояние ViPNet SIES MC и SIES-узлов в виде информационных и предупреждающих сообщений. Отображается в качестве стартовой страницы после загрузки веб-интерфейса ViPNet SIES MC (на стр. 51).
- **Инфраструктура** — отображает структуру индустриальной системы и предназначен для визуального контроля за состоянием SIES-узлов и прикладных связей между защищаемыми устройствами.
- **SIES-узлы** — позволяет управлять SIES-узлами и их группами, зарегистрированными в ViPNet SIES MC.
- **Защищаемые устройства** — позволяет управлять защищаемыми устройствами и их группами, зарегистрированными в ViPNet SIES MC.
- **Администраторы** — позволяет управлять сертификатами администраторов ViPNet SIES MC (на стр. 29).
- **Сертификаты и ключи** — позволяет управлять ключевой информацией ViPNet SIES (на стр. 44).
- **Сетевые настройки** — позволяет задавать сетевые настройки ViPNet SIES MC (на стр. 38) и настройки служб доставки защищенных конвертов ViPNet SIES MC (на стр. 40).

- **Сервисные функции** — содержит функции регламентного обслуживания ViPNet SIES MC.
- **Обновления** — позволяет обновлять ПО ViPNet SIES MC (на стр. 58) и SIES-узлов.
- **Журнал событий** — позволяет просматривать журнал, регистрирующий действия администраторов ViPNet SIES MC (на стр. 54), системные события и автоматические действия ViPNet SIES MC.
- **Архивы журналов** — позволяет экспортировать архивы записей о событиях ViPNet SIES MC из раздела **Журнал событий** (на стр. 55).

2 Панель просмотра — отображает содержимое раздела, выбранного на панели навигации.

3 Панель навигации по группам — отображает текущее положение в структуре элементов ViPNet SIES MC и предназначена для перехода по группам ViPNet SIES MC.

4 Панель инструментов — содержит инструменты управления текущим разделом. Набор инструментов зависит от раздела, выбранного на панели навигации. Для некоторых разделов панель инструментов может отсутствовать.

5 Панель навигации по страницам — позволяет переходить по страницам с элементами текущего раздела.

6 Панель дополнительных сведений — отображает сведения и инструменты управления элементом, выбранным на панели просмотра.

7 Кнопки на панели дополнительных сведений — инструменты управления элементом, выбранном на панели просмотра. Набор инструментов зависит от типа выбранного элемента и текущей вкладки панели.

8 Панель заголовка — содержит информацию об имени подключенного к веб-интерфейсу администратора и кнопку **Справка** .

Кнопка **Справка** содержит меню со следующими пунктами:

- **Справка** — при выборе откроется HTML-справка по ViPNet SIES MC;
- **О программе** — при выборе откроется окно для просмотра информации о продукте.

9 Кнопка скрывает и раскрывает панель навигации.

10 Титул ViPNet SIES MC — кнопка возврата к главной странице веб-интерфейса (раздел **Сообщения**).

Управление доступом администраторов к веб-интерфейсу ViPNet SIES MC

Чтобы управлять SIES-узлами с помощью ViPNet SIES MC, сертификат администратора следует предварительно добавить в ViPNet SIES MC и назначить администратору роль управления.

Сертификат первого супер-администратора ViPNet SIES MC добавляется в консоли Linux (на стр. 15) при вводе ViPNet SIES MC в эксплуатацию. Сертификаты остальных администраторов следует добавить из веб-интерфейса ViPNet SIES MC (на стр. 27).

Добавление нового администратора

Управлять SIES-узлами с помощью ViPNet SIES MC могут несколько администраторов с разными ролями управления в зависимости от потребностей вашей организации. Подробнее о распределении полномочий администратора по ролям управления см. документ «ViPNet SIES MC. Общее описание».

Перед добавлением администратора в ViPNet SIES MC организуйте защищенное подключение администратора к ViPNet SIES MC (на стр. 24).

Чтобы добавить нового администратора ViPNet SIES MC:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.
2. Перейдите в раздел **Администраторы** .
3. Щелкните ссылку **Добавить**.
4. Выберите действующий сертификат администратора на жестком диске вашего компьютера или на внешнем носителе и нажмите кнопку **Далее**.

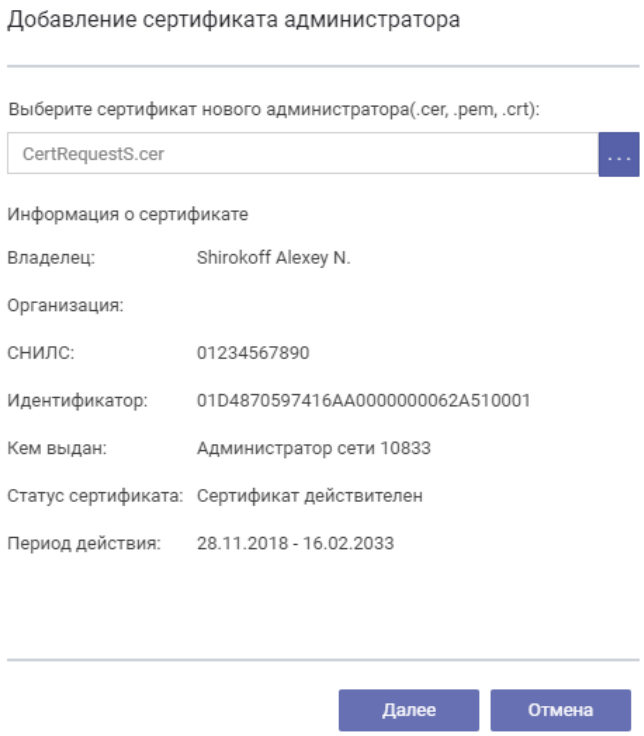

Рисунок 4. Добавление сертификата администратора

5 Задайте полномочия администратора, установив флажки, соответствующие нужным ролям управления.

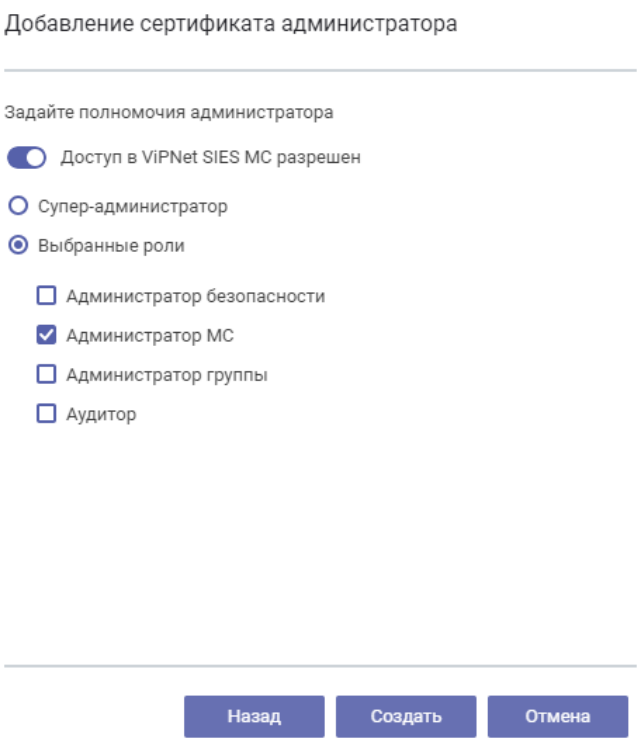

Рисунок 5. Назначение роли администратора

6 Чтобы запретить администратору доступ к ViPNet SIES MC через веб-интерфейс щелкните по переключателю **Доступ в ViPNet SIES MC разрешен**.

7 Если вы выбрали роль управления **Администратор группы**, нажмите кнопку **Далее**. На следующей странице мастера выберите группы, полномочия управления которыми вы делегируете администратору группы.

   Шаг выбора групп можно пропустить, например, если группы еще не добавлены в ViPNet SIES MC.

8 Нажмите кнопку **Создать**.

Новый администратор после выполнения настроек (на стр. 25) на своем рабочем месте может подключиться к веб-интерфейсу ViPNet SIES MC.

Просмотр сведений об администраторах

Вы можете просматривать сведения о сертификатах администраторов, добавленных в ViPNet SIES MC, например, чтобы проверить сроки действия сертификатов.

Чтобы просмотреть сертификат администратора:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора безопасности или аудитора.

2 Перейдите в раздел **Администраторы** .

3 Выберите сертификат или предварительно воспользуйтесь поиском на панели инструментов страницы.

4 На панели дополнительных сведений отобразится информация о заданных ролях управления и доступе в веб-интерфейс ViPNet SIES MC.

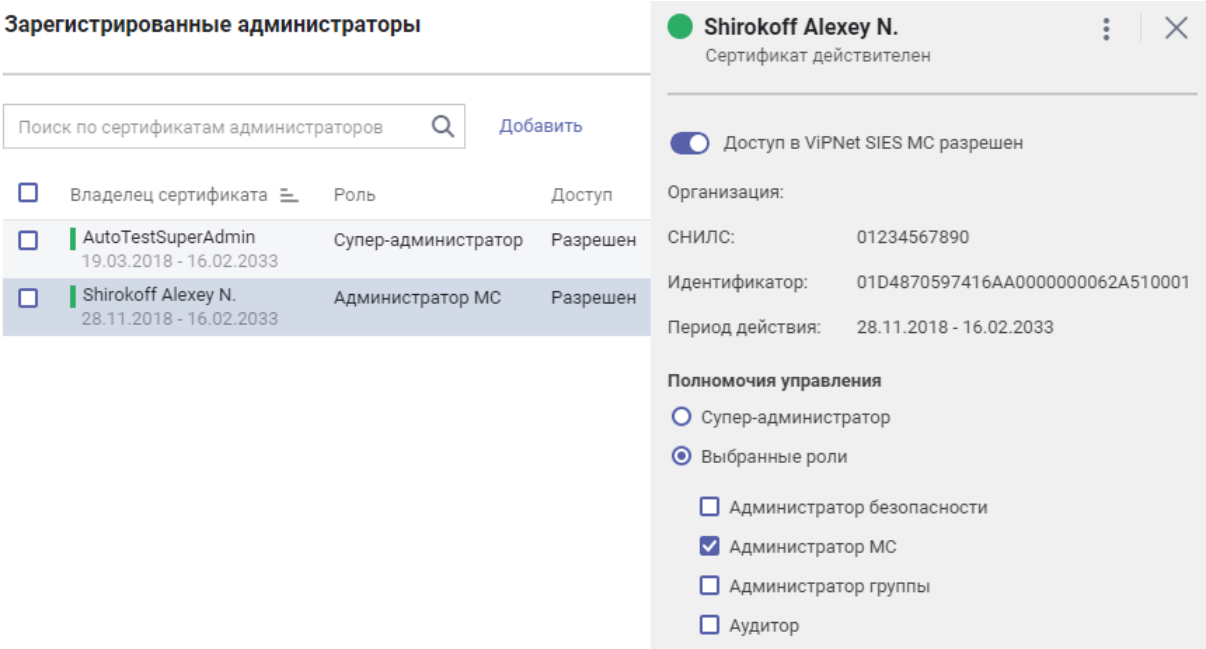

Рисунок 6. Список администраторов ViPNet SIES MC

Для администратора группы дополнительно отображается список групп, полномочия управления которыми делегированы администратору.

5 Чтобы подробнее ознакомиться с параметрами сертификата, на панели дополнительных сведений об администраторе нажмите кнопку и в меню выберите **Выгрузить сертификат**.

6 Укажите место сохранения сертификата в файл `*.cer`.

Управление ролями администратора

В ходе эксплуатации ViPNet SIES MC вы можете менять роли управления, назначенные администраторам ViPNet SIES MC. Изменять роли администраторов вам потребуется в случае перераспределения полномочий управления ViPNet SIES MC между сотрудниками вашей организации.

Чтобы изменить роли администратора ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Администраторы** .

3 Выберите сертификат.

4 На панели дополнительных сведений задайте роли администратора, установив флажки, соответствующие нужным ролям управления.

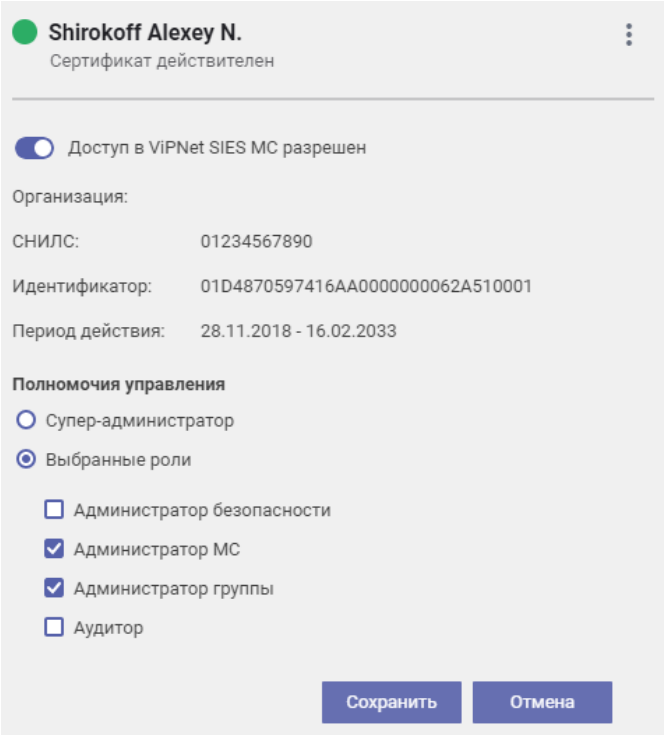

Рисунок 7. Изменение ролей управления

Чтобы отозвать право доступа администратора в веб-интерфейс ViPNet SIES MC, щелкните по переключателю **Доступ в ViPNet SIES MC разрешен**.

Примечание. Сертификаты администраторов, которым закрыт доступ в веб-интерфейс ViPNet SIES MC, не учитываются лицензией.

---

5 На панели дополнительных сведений нажмите кнопку **Сохранить**.

При следующем подключении к веб-интерфейсу ViPNet SIES MC администратор получит полномочия в соответствии с новыми ролями.

Изменение полномочий администратора по управлению группами

В ходе эксплуатации ViPNet SIES MC вы можете менять полномочия администратора по управлению группами ViPNet SIES MC. Изменять полномочия администраторов групп вам потребуется в случае перераспределения полномочий управления группами ViPNet SIES MC между сотрудниками вашей организации.

Супер-администраторы и администраторы МС обладают полномочиями управления всеми группами ViPNet SIES MC без исключения.

Чтобы изменить полномочия администратора группы:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Администраторы** .

3 Выберите сертификат администратора группы.

4 На панели дополнительных сведений в разделе **Администрируемые группы** нажмите кнопку **Изменить**.

5 Выберите группы, полномочия управления которыми вы делегируете администратору группы.

   Нажмите кнопку **OK**.

6 На панели дополнительных сведений нажмите кнопку **Сохранить**.

Обновление сертификата администратора

По истечении периода действия сертификата администратора обновите сертификат в ViPNet SIES MC. Перед обновлением сертификата в ViPNet SIES MC, на рабочем месте администратора создайте запрос на сертификат и получите новый сертификат в удостоверяющем центре, в котором издан корневой сертификат пользовательской ключевой подсистемы ViPNet SIES.

Чтобы обновить сертификат администратора в ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Администраторы** .

3 Выберите сертификат.

4 На панели дополнительных сведений нажмите кнопку и в меню выберите **Обновить сертификат**.

5 Выберите сертификат на жестком диске вашего компьютера или на внешнем носителе.

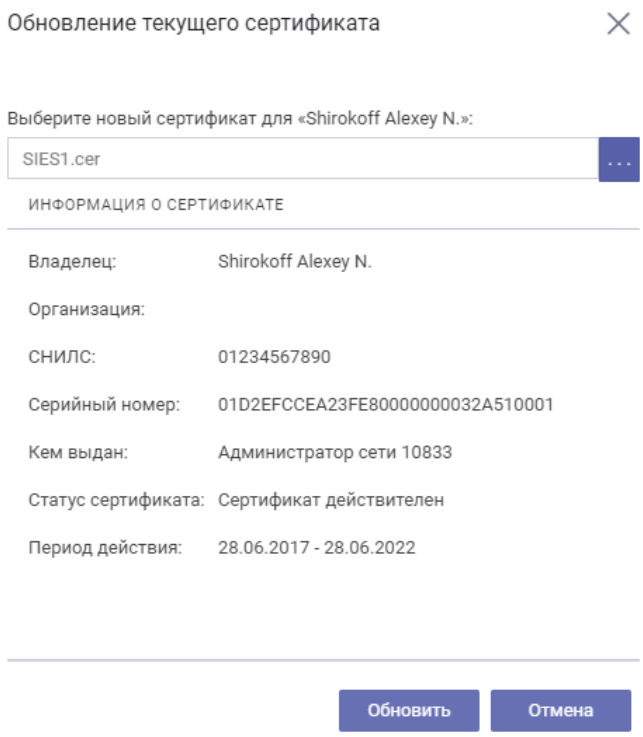

Рисунок 8. Просмотр нового сертификата

6 Нажмите кнопку **Обновить**.

Удаление администратора

Полномочия администратора ViPNet SIES MC можно отозвать, например, в случае увольнения сотрудника, наделенного полномочиями администратора. Чтобы отозвать полномочия администратора, удалите сертификат администратора из ViPNet SIES MC.

Вы не сможете удалить:

- ваш собственный сертификат;
- сертификат супер-администратора, если в ViPNet SIES MC отсутствуют сертификаты других супер-администраторов;
- сертификат администратора, на который не распространяются полномочия назначенной вам роли управления.

Чтобы удалить сертификат администратора ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Администраторы** .

3 Выберите сертификат.

Чтобы выбрать сертификаты нескольких администраторов, установите флажки слева от имен администраторов. Чтобы выбрать сертификаты всех администраторов, установите флажок слева от заголовка **Владелец сертификата**.

4 На панели дополнительных сведений нажмите кнопку и в меню выберите **Удалить сертификат**.

5 Подтвердите удаление сертификата администратора.

Компрометация администратора

В случае компрометации (см. глоссарий, стр. 90) сведения о сертификате скомпрометированного администратора передайте в удостоверяющий центр, издавший сертификат.

Администратор удостоверяющего центра внесет сертификат скомпрометированного администратора в список аннулированных сертификатов удостоверяющего центра (список аннулированных сертификатов пользовательской ключевой подсистемы ViPNet SIES).

При обновлении списка аннулированных сертификатов в ViPNet SIES MC (на стр. 48) доступ скомпрометированного администратора к веб-интерфейсу ViPNet SIES MC автоматически заблокируется.

Чтобы вручную заблокировать доступ скомпрометированного администратора в веб-интерфейс ViPNet SIES MC:

1 Удалите администратора (на стр. 35) или отзовите право доступа администратора в веб-интерфейс ViPNet SIES MC (на стр. 32).

2 Сообщите в удостоверяющий центр о факте компрометации сертификата администратора.

3

Управление и настройка

Управление и настройка из веб-интерфейса 38

Управление и настройка из консоли Linux 61

Управление и настройка из веб-интерфейса

Сетевые настройки

Первоначально сетевые настройки задаются при инициализации ViPNet SIES MC в консоли Linux (на стр. 15). Вы можете:

- при изменениях в структуре локальной сети изменить настройки одного или нескольких сетевых интерфейсов;
- для использования служб доставки защищенных конвертов активировать дополнительные сетевые интерфейсы.

Изменение сетевых настроек

При изменениях в структуре локальной сети вы можете изменить настройки одного или нескольких сетевых интерфейсов.

Чтобы изменить сетевые настройки ViPNet SIES MC:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.
2. Перейдите в раздел **Сетевые настройки** .
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Щелкните по наименованию сетевого интерфейса, настройки которого нужно изменить.

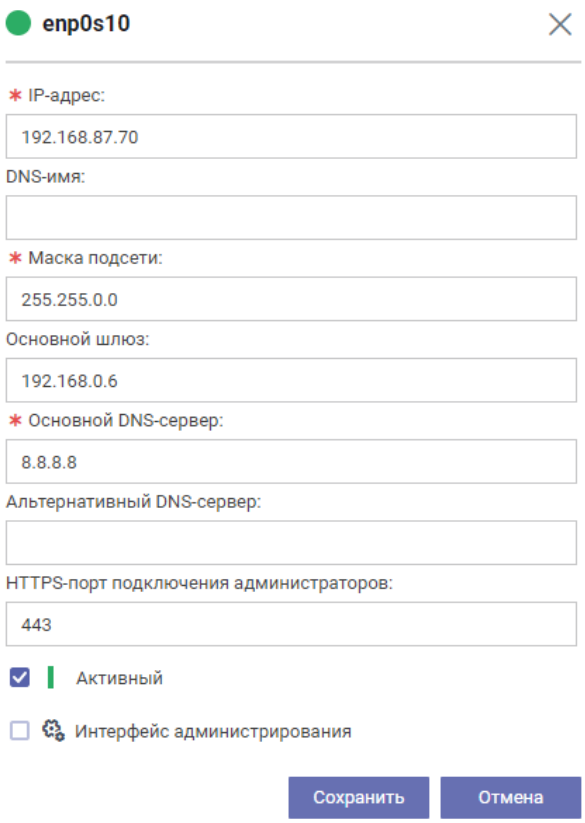

Рисунок 9. Изменение сетевых настроек

5 На открывшейся панели дополнительных сведений измените настройки выбранного сетевого интерфейса ViPNet SIES MC.

Внимание! Не задавайте IP-адрес, принадлежащий широковещательному сегменту, IP-адрес из которого уже задан для другого сетевого интерфейса.

Для сетевого интерфейса с установленным флажком **Интерфейс администрирования** вы можете изменить значения только следующих настроек:

- **Основной шлюз**
- **Основной DNS-сервер**
- **Альтернативный DNS-сервер**
- **HTTPS-порт подключения администраторов**

Внимание! В ViPNet SIES MC используется только одно значение для IP-адреса основного шлюза. При задании нового значения данного поля для других сетевых интерфейсов текущее значение IP-адреса основного шлюза будет перезаписано. Для этого нужно установить флажок **Активный**.

Чтобы запретить доступ ViPNet SIES MC к сети через данный сетевой интерфейс снимите флажок **Активный**.

6 Нажмите кнопку **Сохранить**.

7 Нажмите кнопку **Да**.

Внимание! До окончания применения настроек веб-интерфейс ViPNet SIES MC будет временно недоступен. Нажав в окне кнопку **Нет**, вы можете применить настройки позже на вкладке **Сетевые интерфейсы**.

Активация дополнительного сетевого интерфейса

Вы можете активировать дополнительный сетевой интерфейс, например, для использования службой доставки защищенных конвертов ViPNet SIES MC.

Чтобы активировать сетевой интерфейс ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сетевые настройки** .

3 Перейдите на вкладку **Сетевые интерфейсы**.

4 Щелкните по наименованию сетевого интерфейса.

5 На открывшейся панели дополнительных сведений задайте актуальные настройки для сетевого интерфейса.

Внимание! В ViPNet SIES MC используется только одно значение для IP-адреса основного шлюза. При задании нового значения данного поля текущее значение IP-адреса основного шлюза будет перезаписано.

6 Установите флажок **Активный**.

7 Нажмите кнопку **Сохранить**.

8 Нажмите кнопку **Применить настройки**.

Внимание! До окончания применения настроек веб-интерфейс ViPNet SIES MC будет временно недоступен. Нажав в окне кнопку **Нет**, вы можете применить настройки позже на вкладке **Сетевые интерфейсы**.

Службы доставки защищенных конвертов

Службы доставки защищенных конвертов между ViPNet SIES MC и SIES-узлами используются в режиме удаленного управления SIES-узлами по каналам связи индустриальной системы.

К сетевым портам служб доставки защищенных конвертов подключаются шлюзовые компоненты. Шлюзовые компоненты применяются для организации обмена защищенными конвертами между ViPNet SIES MC и защищаемыми устройствами индустриальной системы. Подробнее см. документ «ViPNet SIES MC. Руководство разработчика».

В ViPNet SIES MC может действовать одновременно несколько служб для доставки защищенных конвертов:

- отдельным SIES-узлам;
- отдельным группам SIES-узлов.

Для удаленного управления SIES-узлами по каналам связи индустриальной системы требуется наличие хотя бы одной активной службы доставки защищенных конвертов ViPNet SIES MC.

В зависимости от исполнения ViPNet SIES MC можно добавить следующее количество служб доставки:

- ViPNet SIES MC 10000 Q1 — 200;
- ViPNet SIES MC 3000 N1 — 100;
- ViPNet SIES MC VA — 100.

Добавление службы

Для удаленного управления SIES-узлами по каналам связи индустриальной системы добавьте в ViPNet SIES MC службу доставки защищенных конвертов.

Чтобы добавить службу доставки:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора MC или администратора группы (без полномочия назначения службы доставки для использования по умолчанию).
2. Перейдите в раздел **Сетевые настройки** .
3. Перейдите на вкладку **Службы доставки команд**.
4. Нажмите кнопку **Добавить**.
5. Задайте **Наименование** службы доставки.

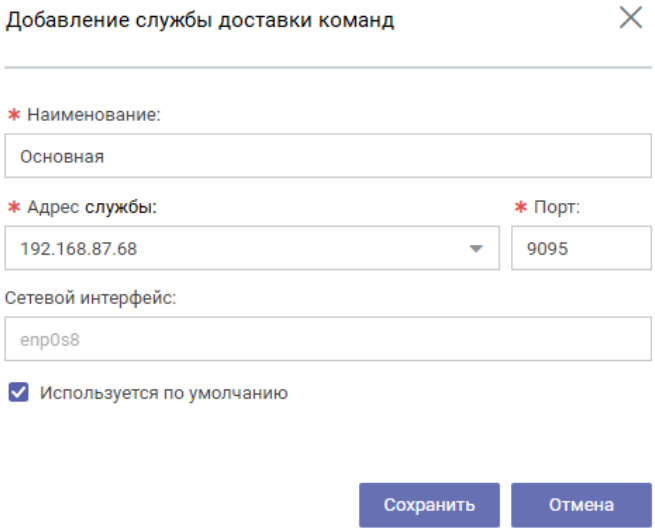

Рисунок 10. Параметры добавляемой службы доставки

В списке **Адрес службы** выберите адрес сетевого интерфейса, к которому будет подключаться шлюзовой компонент. Подробнее см. документ «ViPNet SIES MC. Руководство разработчика».

В поле **Порт** задайте уникальный номер сетевого порта службы доставки ViPNet SIES MC для выбранного ранее адреса сетевого интерфейса. Сетевой порт с заданным номером должен быть свободным.

Если добавляемая служба доставки будет использоваться в ViPNet SIES MC по умолчанию для доставки защищенных конвертов SIES-узлам, установите флажок **Используется по умолчанию**.

Примечание. Если вы не установите флажок **Используется по умолчанию**, а добавленная служба доставки будет единственной в ViPNet SIES MC, то вам придется задавать службу доставки при добавлении в ViPNet SIES MC каждого SIES-узла или защищаемого устройства, если они не помещены в группу с назначенной на нее службой доставки.

Нажмите кнопку **Сохранить**.

6 Для активации добавленной службы доставки нажмите **Применить настройки**.

Примечание. Нажав в окне кнопку **Нет**, вы можете применить настройки позже на вкладке **Службы доставки команд**. В ходе применения настроек ViPNet SIES MC не ведет обмен защищенными конвертами с подключенными шлюзовыми компонентами.

Изменение параметров службы

В ходе эксплуатации ViPNet SIES MC вам может потребоваться изменить параметры службы доставки, например, сетевой порт.

Чтобы изменить параметры службы доставки:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора МС или администратора группы (при наличии права

управления всеми защищаемыми устройствами, SIES-узлами или их группами, на которые назначена данная служба доставки).

2 Перейдите в раздел **Сетевые настройки** .

3 Перейдите на вкладку **Службы доставки команд**.

4 Щелкните по наименованию службы доставки.

5 На открывшейся панели дополнительных сведений задайте новые параметры службы доставки.

Если требуется выбрать данную службу доставки для использования по умолчанию, установите флажок **Используется по умолчанию**.

Совет. Для отмены всех изменений, внесенных в параметры служб доставки, и возврата к последним примененным настройкам на вкладке **Службы доставки команд** нажмите кнопку **Отменить**. Операция недоступна для администратора группы.

---

6 Нажмите кнопку **Сохранить**.

7 Для применения в работе измененных параметров службы нажмите кнопку **Применить настройки**.

Примечание. Нажав в окне кнопку **Нет**, вы можете применить настройки позже на вкладке **Службы доставки команд**. В ходе применения настроек ViPNet SIES MC не ведет обмен защищенными конвертами с подключенными шлюзовыми компонентами.

Удаление службы

Вы можете удалить службу доставки защищенных конвертов, например, если нужно перейти на использование другой службы. После удаления доставка защищенных конвертов будет выполняться через службу, используемую по умолчанию.

Чтобы удалить службу доставки:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора MC или администратора группы (при наличии права управления всеми защищаемыми устройствами, SIES-узлами или их группами, на которые назначена данная служба доставки).

2 Перейдите в раздел **Сетевые настройки** .

3 Перейдите на вкладку **Службы доставки команд**.

4 Щелкните по наименованию удаляемой службы доставки.

5 На панели дополнительных сведений нажмите кнопку и в меню выберите **Отменить назначение службы** (операция недоступна для администратора группы).

6 Нажмите кнопку **Да**.

7 На панели дополнительных сведений нажмите кнопку и в меню выберите **Удалить службу**.

8 Нажмите кнопку **Удалить**.

9 Для применения в работе измененного списка служб щелкните **Применить настройки**.

Сертификаты и ключи

Просмотр сертификатов и ключей

Вы можете просматривать сведения о сертификатах и ключах ViPNet SIES, например, чтобы проверить сроки действия.

Чтобы просмотреть сертификаты или ключи ViPNet SIES:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора MC или аудитора (аудиторам запрещено выгружать сертификаты).

2 Перейдите в раздел **Сертификаты и ключи** .

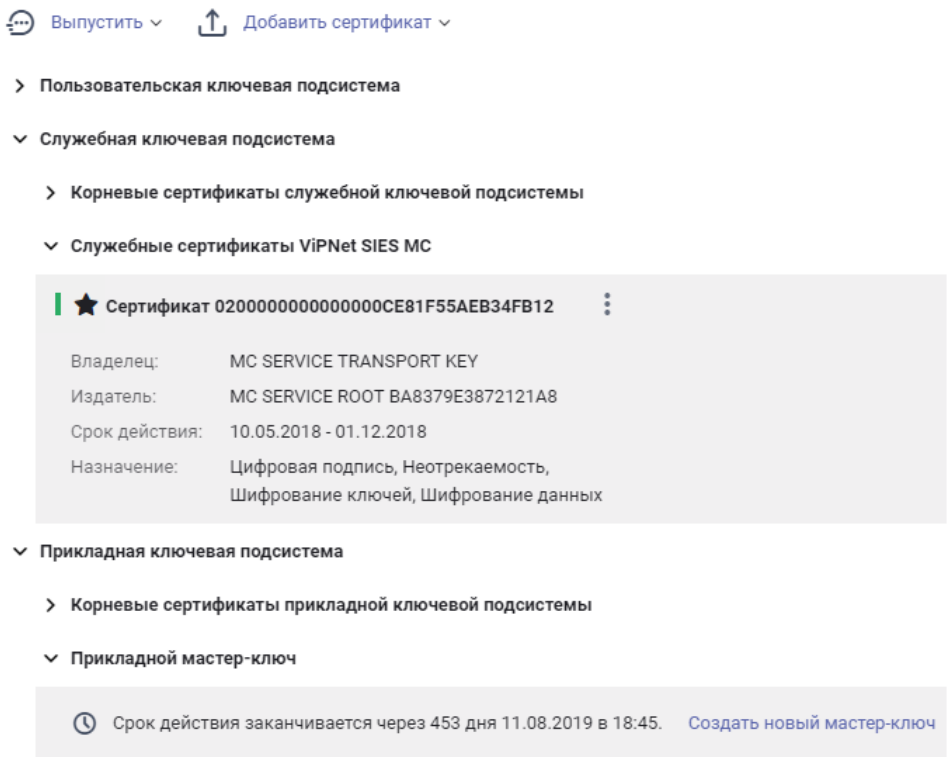

Рисунок 11. Просмотр сертификатов ViPNet SIES MC

3 Щелкните список с наименованием ключевой подсистемы.

4 В раскрывшемся списке ключевой подсистемы щелкните список с наименованием типа сертификата или ключа.

5 В списке щелкните интересующий вас сертификат или ключ.

6 Просмотрите атрибуты выбранного сертификата.

Сертификаты помечаются следующими значками:

— сертификат действителен (см. глоссарий, стр. 89);

— срок действия сертификата истекает;

— срок действия сертификата истек.

Экспорт сертификатов

Для детального ознакомления с атрибутами сертификата ключевой подсистемы ViPNet SIES, вы можете экспортировать сертификат в файл. Также вы можете выгрузить список аннулированных сертификатов (доступен не для всех сертификатов).

Чтобы экспортировать сертификат или список аннулированных сертификатов ключевой подсистемы ViPNet SIES:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сертификаты и ключи** .

3 Щелкните список с наименованием ключевой подсистемы.

4 В раскрывшемся списке ключевой подсистемы щелкните список с наименованием вида сертификата.

5 В списке справа от интересующего вас сертификата нажмите кнопку .

6 Из появившегося меню выберите пункт:

- **Выгрузить на внешний носитель** — для экспорта выбранного сертификата.
- **Выгрузить CRL на внешний носитель** — для экспорта списка аннулированных сертификатов выбранной ключевой подсистемы.

7 Укажите место сохранения сертификата или списка аннулированных сертификатов.

После подтверждения сертификат будет сохранен в файл `*.cer`, список аннулированных сертификатов будет сохранен в файл `*.crl`.

Выпуск и обновление сертификатов и ключей

Заблаговременно добавляйте в ViPNet SIES MC новые сертификаты пользовательской ключевой подсистемы ViPNet SIES MC, изданные сторонним удостоверяющим центром.

Контролируйте актуальность списка аннулированных сертификатов для корневого сертификата пользовательской ключевой подсистемы ViPNet SIES MC.

ViPNet SIES MC заблаговременно уведомит (на стр. 52) вас о наступлении срока обновления сертификатов или списка аннулированных сертификатов.

Обновление сертификата ViPNet SIES MC для подключения администраторов: порядок действий

Чтобы добавить новый сертификат ViPNet SIES MC для подключения администраторов, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 7. Порядок обновления сертификата ViPNet SIES MC для подключения администраторов

	Действие	Ссылка
☐	Создайте запрос на новый сертификат.	Создание запроса (на стр. 46).
☐	Передайте файл с запросом администратору внешнего удостоверяющего центра для издания сертификата.	
☐	Получите из внешнего удостоверяющего центра изданный сертификат.	
☐	Загрузите новый сертификат в ViPNet SIES MC.	Загрузка сертификата (на стр. 47).

Создание запроса

Чтобы создать запрос на новый сертификат ViPNet SIES MC для подключения администраторов:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.
2. Перейдите в раздел **Сертификаты и ключи** .
3. Нажмите кнопку **Выпустить** > **Запрос на сертификат ViPNet SIES MC для подключения администраторов**.
4. Укажите место сохранения файла с запросом.
5. Передайте файл с запросом администратору внешнего удостоверяющего центра для издания сертификата.

Загрузка сертификата

Чтобы загрузить новый сертификат ViPNet SIES MC для подключения администраторов в ViPNet SIES MC:

1 Получите из удостоверяющего центра изданный сертификат.

2 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

3 Перейдите в раздел **Сертификаты и ключи** .

4 Нажмите **Добавить сертификат** > **Сертификат ViPNet SIES MC для подключения администраторов**.

5 Выберите файл с сертификатом на жестком диске вашего компьютера или на внешнем носителе.

6 Нажмите кнопку **Выбрать**.

Новый сертификат вступит в действие автоматически немедленно после загрузки.

Внимание! После загрузки нового сертификата ViPNet SIES MC для подключения администраторов текущие TLS-подключения администраторов к веб-интерфейсу ViPNet SIES MC разорвутся.

Добавление корневого сертификата пользовательской ключевой подсистемы ViPNet SIES

Вы можете добавить корневой сертификат пользовательской ключевой подсистемы ViPNet SIES в ViPNet SIES MC, например, чтобы добавлять в ViPNet SIES MC (на стр. 29) сертификаты администраторов, подписанные новым доверенным сертификатом.

За корневым сертификатом пользовательской ключевой подсистемы ViPNet SIES обратитесь в удостоверяющий центр.

Внимание! Вам следует самостоятельно следить за сроком действия корневого сертификата пользовательской ключевой подсистемы ViPNet SIES с помощью сторонних средств. Если цепочка сертификатов для корневого сертификата состоит более чем из одного сертификата, то обновлять сертификат следует в ходе повторной инициализации (на стр. 64).

Чтобы добавить корневой сертификат пользовательской ключевой подсистемы ViPNet SIES:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Сертификаты и ключи** .

3 Нажмите кнопку **Добавить сертификат** и в меню выберите пункт **Корневой сертификат пользовательской ключевой подсистемы**.

4 Выберите файл с сертификатом на жестком диске вашего компьютера или на внешнем носителе.

5 Нажмите кнопку **Выбрать**.

Обновление списка аннулированных сертификатов

Обновляйте список аннулированных сертификатов пользовательской ключевой подсистемы ViPNet SIES до истечения срока действия текущего списка аннулированных сертификатов. Также вы можете настроить автоматическое обновление списка аннулированных сертификатов (на стр. 48).

Внимание! Вам следует самостоятельно следить за сроком действия списка аннулированных сертификатов пользовательской ключевой подсистемы ViPNet SIES с помощью сторонних средств. Если цепочка сертификатов для корневого сертификата состоит более чем из одного сертификата, то обновлять список аннулированных сертификатов следует в ходе повторной инициализации (на стр. 64). Если список аннулированных сертификатов не будет обновлен в срок, будет запрещен доступ администраторов в веб-интерфейс ViPNet SIES MC.

Чтобы обновить список аннулированных сертификатов:

1 Получите новый список аннулированных сертификатов в удостоверяющем центре.

2 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

3 Перейдите в раздел **Сертификаты и ключи**.

4 Щелкните список **Пользовательская ключевая подсистема**.

5 Щелкните список **Корневые сертификаты пользовательской ключевой подсистемы и CRL**.

6 В раскрывшемся списке справа от действительного сертификата нажмите кнопку и в меню выберите **Загрузить CRL с внешнего носителя**.

7 Выберите файл со списком аннулированных сертификатов на жестком диске вашего компьютера или на внешнем носителе.

8 Нажмите кнопку **Выбрать**.

Автоматическое обновление списка аннулированных сертификатов из точки распространения

Вы можете повысить удобство использования ViPNet SIES MC и сократить время на администрирование, настроив автоматическое обновление списка аннулированных сертификатов

пользовательской ключевой подсистемы ViPNet SIES из точки распространения. Точка распространения должна быть доступна по протоколу HTTP или FTP.

Чтобы настроить автоматическое обновление списка аннулированных сертификатов:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Сертификаты и ключи** .

3 Щелкните список **Пользовательская ключевая подсистема**.

4 В раскрывшемся списке щелкните список **Корневые сертификаты пользовательской ключевой подсистемы и CRL**.

5 В раскрывшемся списке справа от нужного корневого сертификата пользовательской ключевой подсистемы ViPNet SIES нажмите кнопку .

6 В меню выберите **Параметры автоматического обновления CRL**.

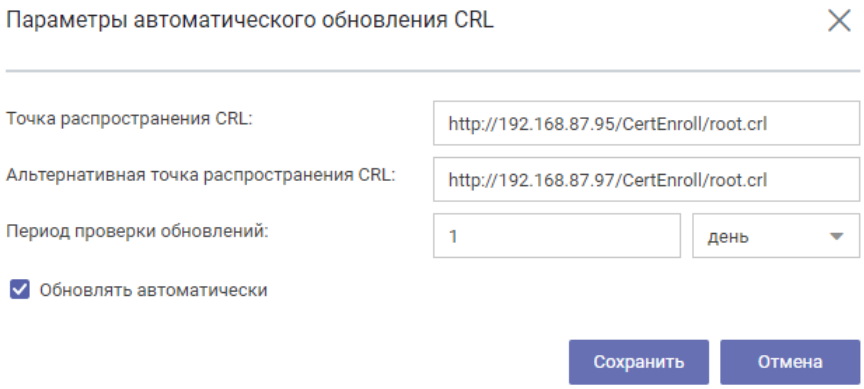

Рисунок 12. Параметры автоматического получения списка аннулированных сертификатов

7 Задайте следующие параметры автоматического обновления списка аннулированных сертификатов:

- **Точка распространения CRL** — адрес в форме `{http | ftp}://<адрес>[:<порт>]`, где:
  - `<адрес>` — IP-адрес или доменное имя точки распространения списка аннулированных сертификатов;
  - `<порт>` — сетевой порт точки распространения списка аннулированных сертификатов.
- **Альтернативная точка распространения CRL** — адрес дополнительной точки распространения списка аннулированных сертификатов.
- **Период проверки обновлений** — частота опроса об обновлениях точки распространения списка аннулированных сертификатов.

Установите флажок **Обновлять автоматически**.

Нажмите кнопку **Сохранить**.

Изменение параметров автоматического получения списка аннулированных сертификатов

Вы можете изменить параметры автоматического обновления списка аннулированных сертификатов, например, отказаться от автоматического обновления.

Чтобы изменить параметры автоматического обновления списка аннулированных сертификатов:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора безопасности.

2 Перейдите в раздел **Сертификаты и ключи** .

3 Щелкните список **Пользовательская ключевая подсистема**.

4 В раскрывшемся списке щелкните список **Корневые сертификаты пользовательской ключевой подсистемы и CRL**.

5 В раскрывшемся списке справа от нужного корневого сертификата пользовательской ключевой подсистемы ViPNet SIES нажмите кнопку .

6 В меню выберите **Параметры автоматического обновления CRL**.

7 Измените параметры автоматического обновления списка аннулированных сертификатов.

   Чтобы отключить автоматическое обновление списка аннулированных сертификатов, снимите флажок **Обновлять автоматически**.

   Нажмите кнопку **Сохранить**.

Выпуск сертификатов служебной и прикладной ключевых подсистем

Заблаговременно до истечения срока действия текущих сертификатов вы можете выпустить следующие сертификаты:

- корневой сертификат служебной ключевой подсистемы ViPNet SIES (см. глоссарий, стр. 91);
- корневой сертификат прикладной ключевой подсистемы ViPNet SIES (см. глоссарий, стр. 91);
- служебный сертификат ViPNet SIES MC (см. глоссарий, стр. 92).

Совет. Перед выпуском прикладных сертификатов SIES-узлов для использования в сценариях защиты данных, выпустите корневой сертификат прикладной ключевой подсистемы ViPNet SIES.

Чтобы выпустить сертификат служебной или прикладной ключевой подсистемы ViPNet SIES:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сертификаты и ключи** .

3 Нажмите кнопку **Выпустить** и в меню выберите пункт, соответствующий наименованию выпускаемого сертификата.

Примечание. При выпуске корневого сертификата служебной ключевой подсистемы ViPNet SIES автоматически выпускается служебный сертификат ViPNet SIES MC. Новый служебный сертификат ViPNet SIES MC следует загрузить на все SIES-узлы для сохранения возможности удаленного управления. Подробнее см. документ «ViPNet SIES MC. Руководство администратора».

Создание прикладного мастер-ключа

Прикладной мастер-ключ (см. глоссарий, стр. 91) ViPNet SIES используется для выработки ключей связи взаимодействующих SIES-узлов. Подробнее об управлении прикладными связями SIES-узлов см. документ «ViPNet SIES MC. Руководство администратора».

Одновременно ViPNet SIES MC может хранить два прикладных мастер-ключа. При отсутствии в ViPNet SIES MC мастер-ключ создается автоматически в ходе синхронизации первой прикладной связи (см. глоссарий, стр. 91) между взаимодействующими SIES-узлами. Вы можете создать мастер-ключ перед добавлением прикладных связей между SIES-узлами.

Чтобы создать мастер-ключ:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сертификаты и ключи**.

3 Щелкните список **Прикладная ключевая подсистема**.

4 В раскрывшемся списке щелкните **Прикладной мастер-ключ**.

5 Щелкните **Создать мастер-ключ** или **Создать новый мастер-ключ**.

Созданный мастер-ключ вступит в действие автоматически по окончании срока действия существующего мастер-ключа, если он есть в ViPNet SIES MC.

Мониторинг работоспособности

В ходе эксплуатации ViPNet SIES MC автоматически контролирует собственное состояние и состояние SIES-узлов, формируя данные о событиях с детальной информацией.

ViPNet SIES MC обрабатывает следующие события:

- общесистемные события ViPNet SIES MC;
- события с сертификатами администраторов ViPNet SIES MC;
- события с корневыми сертификатами ключевых подсистем ViPNet SIES;

- состояние прикладного мастер-ключа ViPNet SIES;
- состояние лицензии ViPNet SIES MC;
- состояние SIES-узлов;
- состояние служебных сертификатов SIES-узлов (см. глоссарий, стр. 92);
- состояние прикладных сертификатов SIES-узлов (см. глоссарий, стр. 91);
- состояние первичной ключевой информации SIES-узлов;
- состояние синхронизации прикладных связей SIES-узлов;
- сроки выгрузки записей журналов аудита SIES-узлов.

Информация о событиях выводится в разделе **Сообщения** . Доступ к конкретным сообщениям зависит от назначенной вам роли управления.

Просмотр сообщений мониторинга

С помощью сообщений мониторинга, предоставляемых в режиме реального времени, вы можете оперативно исследовать и устранять неполадки в работе ViPNet SIES MC и SIES-узлов.

Имеющиеся проблемы группируются по типу и уровню критичности (на стр. 79), что облегчает визуальную оценку состояния.

Чтобы посмотреть сообщения мониторинга:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями любой роли управления.
2. Щелкните титул ViPNet SIES MC в левом верхнем углу страницы текущего раздела веб-интерфейса ViPNet SIES MC или перейдите в раздел **Сообщения** .
3. Просмотрите информацию о SIES-узлах. Состояние SIES-узлов отображается блоком определенного цвета в зависимости от уровня критичности событий, вызвавших это состояние. При наличии событий разного уровня критичности блок примет состояние наиболее критичного из событий.

   При наличии проблем в блоках указываются причины возникновения проблем. Причины возникновения проблем группируются по видам с указанием общего количества причин.

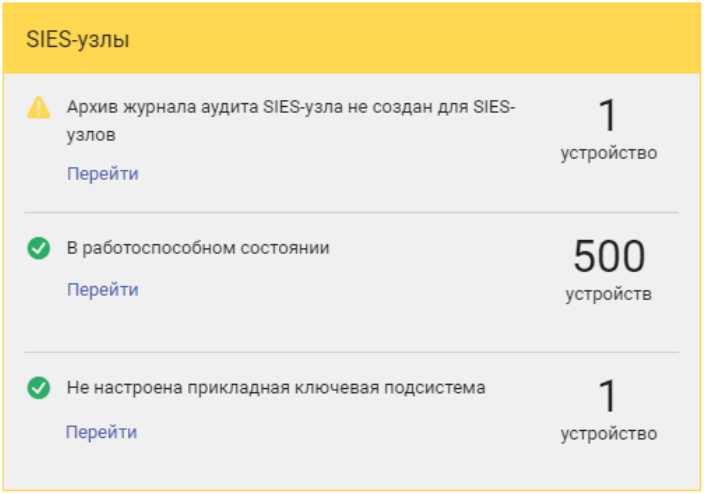

Рисунок 13. Пример блока мониторинга

Чтобы перейти в раздел контролируемых SIES-узлов или получить подробную информацию о событии, щелкните ссылку **Перейти**.

Подготовка архива служебных журналов

В служебных журналах фиксируются события о работе серверного ПО и прикладных модулей ViPNet SIES MC. Служебные журналы помогают исследовать и устранить возможные неполадки в работе ViPNet SIES MC самостоятельно или с привлечением службы технического сопровождения компании ИнфоТеКС.

Чтобы создать или обновить существующий архив служебных журналов ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора безопасности, администратора MC или аудитора.

2 Перейдите в раздел **Сервисные функции** .

3 В разделе **Архив служебных журналов** нажмите кнопку **Создать** или **Обновить**.

Внимание! Формировать архивы служебных журналов одновременно должен только один администратор, поскольку создание архивов одновременно несколькими администраторами может привести к конфликту доступа к файлам журналов.

По окончании создания архива сведения о созданном или обновленном архиве служебных журналов отразятся на панели просмотра.

4 Сохраните архив служебных журналов в файл на вашем рабочем месте, нажав кнопку **Выгрузить**.

5 Укажите место сохранения архива. Архив служебных журналов будет сохранен в файл `*.tar.gz`.

Совет. Перед передачей архива третьей стороне обязательно удостоверьтесь, что архив не содержит файлов с конфиденциальными данными.

Работа с журналами событий

В журнале событий ViPNet SIES MC фиксируется информация обо всех действиях администраторов ViPNet SIES MC, а также обо всех автоматических действиях ViPNet SIES MC. Каждое событие относится к определенной категории.

С журналами событий ViPNet SIES MC можно выполнять следующие действия:

- просматривать журнал событий и искать события по критерию;
- экспортировать архивы записей о событиях;
- удалять архивы записей о событиях.

События, требующие реакции администратора ViPNet SIES MC, выводятся в виде уведомлений в разделе **Сообщения** .

Просмотр журнала событий

Вы можете просматривать события журнала в хронологическом порядке на глубину не более 30 дней. Отображение отдельных категорий событий зависит от назначенной вам роли управления. Чтобы просмотреть события за более ранний период, выгрузите архив событий (на стр. 55).

Чтобы просмотреть записи журнала событий:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями любой роли управления.

2 Перейдите в раздел **Журнал событий** .

3 По умолчанию отображаются все записи журнала о событиях за последнюю неделю.

   Для поиска событий за другой период времени воспользуйтесь фильтром поиска , расположенным на панели инструментов.

4 На открывшейся панели выберите один или несколько критериев поиска событий.

5 Нажмите кнопку **Найти**.

Примечание. После изменения системного времени с помощью повторной инициализации ViPNet SIES MC (на стр. 64) в результат поиска событий за заданный период времени могут попасть лишние записи о событиях или некоторые записи могут отсутствовать.

События обозначены зеленым, желтым или красным цветом в зависимости от их критичности (на стр. 79).

Экспорт архива записей о событиях

Журнал событий ViPNet SIES MC за истекший период автоматически архивируется:

- каждые 30 дней;
- при превышении лимита в 15000000 записей.

Вы можете исследовать архивные записи, выгрузив файл архива.

Чтобы выгрузить файл архива:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или аудитора.
2. Перейдите в раздел **Архивы журналов** .
3. Выберите интересующий вас том архива событий.
4. На панели дополнительных сведений щелкните ссылку **Выгрузить файл архива**.

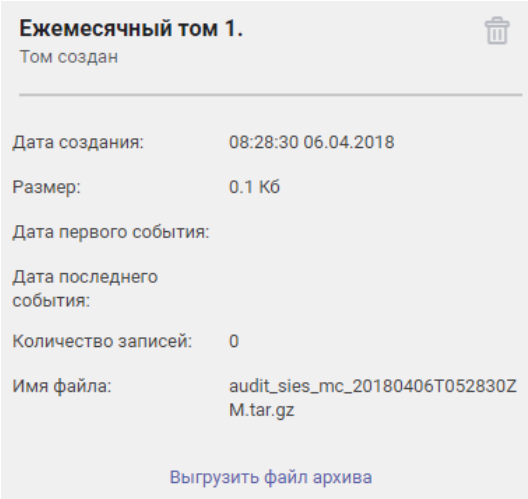

Рисунок 14. Выгрузка файла архива

5. Задайте пароль длиной не менее 8 символов для защиты файла.

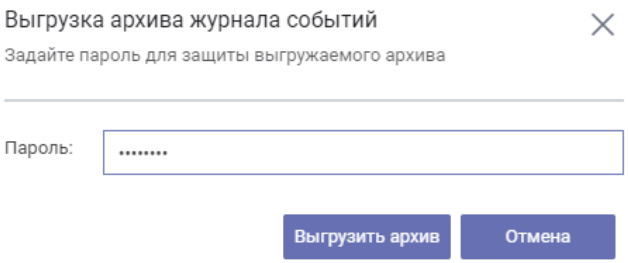

Рисунок 15. Защита паролем тома архива журнала событий

Нажмите кнопку **Выгрузить архив**.

6 Укажите место сохранения архива.

Архив в зашифрованном виде будет сохранен в файл `*.tar.gz`. Информацию о событиях из файла вы можете исследовать с помощью стороннего ПО.

Удаление архива записей о событиях

Удаление архивов записей о событиях поможет вам освободить пространство на жестком диске ViPNet SIES MC. Удалить архив можно только после экспорта.

Чтобы удалить архив событий:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **Архивы журналов** .

3 Выберите один или несколько архивов событий, установив флажки слева от имени файла. Чтобы выбрать все файлы, установите флажок слева от заголовка **Наименование**.

4 Нажмите кнопку **Удалить** .

5 Подтвердите удаление выбранных архивов событий.

Просмотр лицензии

Вы можете просмотреть информацию о текущей установленной лицензии, например, чтобы определить возможность регистрации в ViPNet SIES MC дополнительных SIES-узлов.

Чтобы просмотреть информацию о лицензии:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями любой роли управления.

2 Нажмите кнопку **Справка** и в меню выберите **О программе**.

3 Перейдите на вкладку **Лицензия**.

Обновление и активация лицензии

Обновление лицензии может потребоваться, например, для расширения используемых функций ViPNet SIES MC или при истечении срока действия текущей лицензии. За 60 дней до окончания срока действия лицензии ViPNet SIES MC в сообщении мониторинга предупредит вас о

наступлении срока обновления лицензии. За новой лицензией обратитесь к представителю компании ИнфоТеКС.

Чтобы установить и активировать лицензию:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора МС.

2 Нажмите кнопку **Справка** и в меню выберите **О программе**.

3 Перейдите на вкладку **Лицензия**.

4 Щелкните **Обновить лицензию** и выберите файл с лицензией `*.itcslic`.

5 Проверьте параметры устанавливаемой лицензии. Подробнее о лицензионных объектах см. документ «ViPNet SIES MC. Общее описание».

6 Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Установить.**

7 Если загруженная лицензия требует активации, вам будет предложено отправить запрос на активацию лицензии. Щелкните **Выгрузить запрос** и направьте текст запроса в компанию ИнфоТеКС.

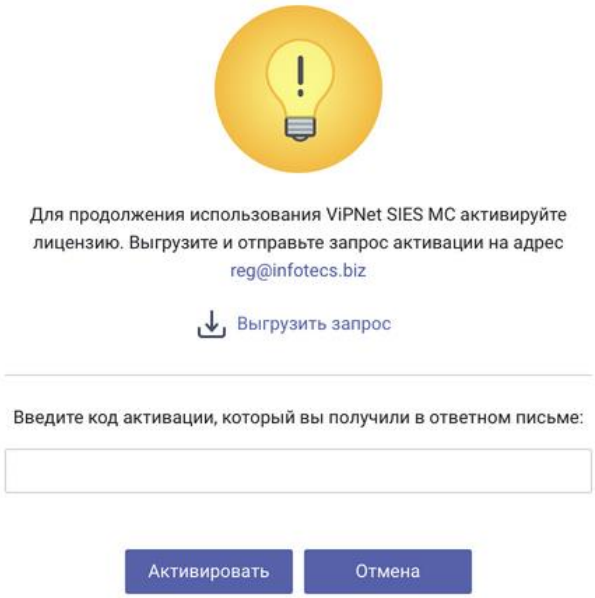

Рисунок 16. Выгрузка запроса на активацию и ввод кода активации

8 После получения ответа на запрос или уже имея код активации лицензии введите его и нажмите кнопку **Активировать**.

Примечание. В ходе активации лицензии ViPNet SIES MC могут возникнуть лицензионные ограничения. О том, как снять их см. в разделе Сообщение о превышении лицензионных ограничений (на стр. 86).

Информацию о результатах обновления лицензии вы можете просмотреть, выбрав на панели навигации раздел **Журнал событий** .

Обновление ПО

По мере реализации новых возможностей компания ИнфоТеКС выпускает обновления ПО ViPNet SIES MC. Вы можете обновить ПО ViPNet SIES MC на новую версию. За обновлением обратитесь в службу технической поддержки компании ИнфоТеКС.

Внимание! После обновления ПО ViPNet SIES MC вам может потребоваться обновление ПО ViPNet SIES Workstation.

Перед обновлением ПО ViPNet SIES MC рекомендуется создать резервную копию данных (на стр. 70).

Совет. Перед обновлением ПО ViPNet SIES MC VA сделайте снимок виртуальной машины.

Чтобы обновить ПО ViPNet SIES MC:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора МС.
2. Перейдите в раздел **Обновления** .
3. В разделе **Обновление системы** нажмите кнопку **Загрузить обновление системы**.
4. Выберите файл `*.tgz` или `*.tar.gz` с обновлением ПО.

   После успешной загрузки и проверки целостности архива во всплывающем окне оповещения отобразится информация о загруженном обновлении и номере устанавливаемой версии ПО.

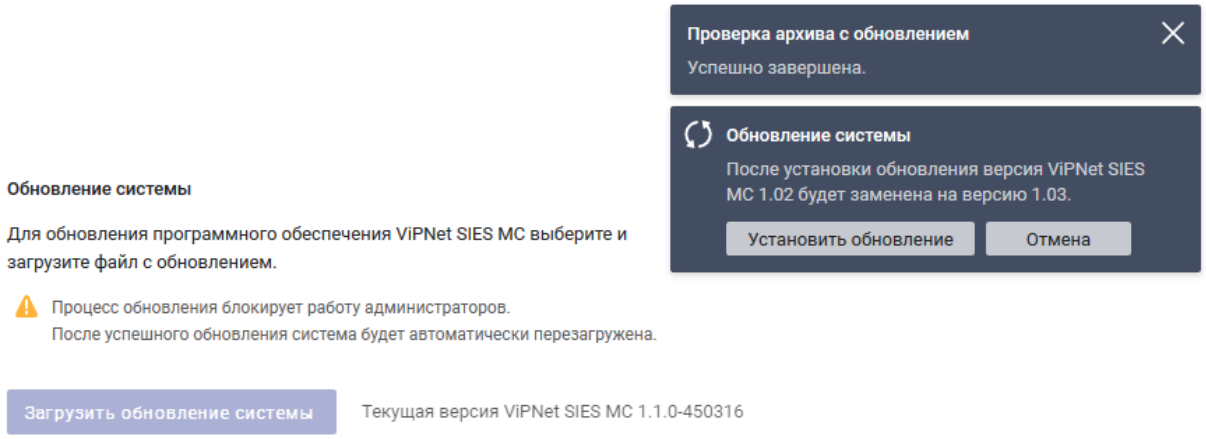

Рисунок 17. Запрос на применение обновления

5 Во всплывающем окне оповещения о загруженном обновлении нажмите кнопку **Установить обновление**.

Для загрузки новой версии веб-интерфейса перезагрузите страницу в браузере, нажав клавиши **Ctrl+R** через 10 минут после начала установки обновления.

По завершении обновления и перезагрузки ViPNet SIES MC номер установленной версии ПО вы можете проверить в окне просмотра информации о продукте, выбрав **О программе** в меню кнопки **Справка** . Также информацию о примененном обновлении вы можете получить, выбрав на панели навигации раздел **Журнал событий** .

Совет. Для корректного отображения элементов интерфейса после обновления ПО ViPNet SIES MC очистите кэш браузеров на рабочих местах администраторов, нажав клавиши **Ctrl+F5**.

Контроль целостности ПО из веб-интерфейса

Для гарантии неизменности ПО ViPNet SIES MC проходит контроль целостности следующих видов:

- стартовый — автоматически каждый раз при загрузке Linux;
- периодический — автоматически через каждые 24 часа функционирования с записью результата в журнал событий;
- регламентный — по запросу администратора с правом локального доступа через консоль Linux или удаленно через веб-интерфейс ViPNet SIES MC с записью результата в журнал событий.

В ходе контроля любого вида проверяется целостность исполняемых модулей и библиотек с помощью контрольных сумм, вычисленных при сборке ПО ViPNet SIES MC.

Чтобы выполнить регламентный контроль целостности ПО ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора, администратора MC или аудитора.

2 Перейдите в раздел **Сервисные функции** .

3 В разделе **Регламентный контроль целостности ПО** нажмите кнопку **Выполнить**.

Запустится проверка целостности, которая может занять несколько секунд.

Если проверка не выявила нарушения целостности, на экране появится соответствующее сообщение.

Если проверка выявила нарушение целостности, ViPNet SIES MC будет автоматически перезагружен. После перезагрузки будет выполнен стартовый контроль целостности. Если стартовый контроль целостности не выявит нарушение целостности, функционирование ViPNet SIES MC будет восстановлено.

Если стартовый контроль целостности повторно выявит нарушение целостности, функционирование ViPNet SIES MC будет заблокировано. Вы сможете выгрузить служебные журналы (на стр. 61) из консоли Linux и обратиться в службу технической поддержки компании ИнфоТеКС для диагностики проблемы.

Управление и настройка из консоли Linux

Мастер инициализации ViPNet SIES MC из консоли Linux позволяет вам выполнить следующие задачи:

- в отсутствие доступа в веб-интерфейс ViPNet SIES MC для анализа работы программных модулей ViPNet SIES MC выгрузить архив служебных журналов;
- при выполнении регламентной проверки в соответствии с документом «ViPNet SIES MC. Правила пользования. ФРКЕ.466219.009ПП» проверить целостность ПО ViPNet SIES MC и контрольные комбинации;
- для восстановления работоспособности ViPNet SIES MC в случае аппаратного или программного сбоя создать резервную копию ключевой информации;
- для изменения сетевых настроек или добавления сертификатов провести повторную инициализацию ViPNet SIES MC;
- перезагрузить ViPNet SIES MC;
- для временного или постоянного вывода из эксплуатации выключить ViPNet SIES MC.

Выгрузка служебных журналов

В ViPNet SIES MC ведутся служебные журналы, которые можно использовать для диагностики работы ViPNet SIES MC. В отсутствие возможности подключиться к ViPNet SIES MC с помощью веб-интерфейса, вы можете сохранить файлы с журналами на USB-носитель с помощью консоли Linux.

Чтобы выгрузить служебные журналы ViPNet SIES MC:

1. Подключите монитор, клавиатуру и USB-носитель к аппаратной платформе ViPNet SIES MC.
2. Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.
3. Из предложенного списка действий выберите сохранение служебных журналов **Create system logs archive**, введя символ `1`.
4. На запрос **Enter full path to save system logs archive** введите полный путь к каталогу для сохранения архива служебных журналов ViPNet SIES MC, например, `/media/usb0/`.

   Архив со служебными журналами будет записан в указанный каталог USB-носителя.
5. Закройте мастер инициализации, введя символ `8`.

Контроль целостности ПО ViPNet SIES MC

Вы можете проверить целостность ПО ViPNet SIES MC. Например, запустить контроль целостности рекомендуется при проблемах с подключением к веб-интерфейсу ViPNet SIES MC.

Чтобы сверить значения контрольных комбинаций ОС и ПО ViPNet SIES MC со значениями из раздела «Контрольные суммы» документа «ViPNet SIES MC. Формуляр. ФРКЕ.466219.009ФО» (регламентный контроль), вам также потребуется выполнить контроль целостности.

Чтобы проверить целостность ПО ViPNet SIES MC:

1. Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.
2. Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.
3. Из предложенного списка действий выберите контроль целостности **Check system integrity**, введя символ `2`.

   Начнется проверка целостности ПО ViPNet SIES MC и расчет контрольных комбинаций ОС и ПО ViPNet SIES MC.

Если проверка не выявила нарушения целостности, на экране появится соответствующее сообщение, а также номер версии ViPNet SIES MC и значения контрольных комбинаций ОС и ПО ViPNet SIES MC, которые следует сверить со значениями из раздела «Контрольные суммы» документа «ViPNet SIES MC. Формуляр. ФРКЕ.466219.009ФО».

Таблица 8. Пример сообщений, выдаваемых при успешном завершении контроля целостности

Сообщение мастера инициализации	Описание
`ViPNet SIES MC system version: 2.0.2-54268`	Версия ПО ViPNet SIES MC.
`System integrity check succeed`	Сообщение об успешном завершении контроля целостности.
`ViPNet SIES MC OS checksum: AE6FA992`	Контрольная комбинация ОС.
`ViPNet SIES MC software checksum: A36DE33A`	Контрольная комбинация ПО ViPNet SIES MC.

Сверив значения, закройте мастер инициализации и завершите сеанс работы в консоли Linux, введя символ `8`.

Если проверка выявила нарушение целостности, функционирование ViPNet SIES MC будет заблокировано. Вы сможете выгрузить служебные журналы (на стр. 61) из консоли Linux и обратиться в службу технической поддержки компании ИнфоТеКС для диагностики проблемы.

Создание резервной копии ключевой информации

ViPNet SIES MC использует ключи в защищенном взаимодействии с рабочими местами администраторов по протоколу TLS. Поэтому резервную копию ключевой информации следует создавать отдельно от резервной копии данных ViPNet SIES MC.

Чтобы создать резервную копию ключевой информации ViPNet SIES MC:

1 Подключите монитор, клавиатуру и USB-носитель к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3 Из предложенного списка действий выберите создание резервной копии ключевой информации **Create backup set of keys**, введя символ `3`.

4 На запрос **Enter full path to backup set of keys file** введите полный путь к файлу для сохранения резервной копии ключевой информации ViPNet SIES MC, например, `/media/usb0/keys.backup`.

5 На запрос **Enter password to protect backup file** введите пароль к файлу с резервной копией.

Внимание! Пароль должен соответствовать следующим требованиям:

- иметь длину от 8 до 32 символов;
- содержать хотя бы одну цифру от 0 до 9;
- содержать хотя бы одну букву латинского алфавита от «A» до «Z» или от «a» до «z».

Пароль может содержать символы «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}».

Дополнительно не рекомендуется использовать:

- три и более символа, расположенные подряд на клавиатуре;
- три и более символа, идущие подряд в алфавитном порядке;
- один и тот же символ более двух раз.

---

6 На запрос **Confirm password** вновь введите тот же пароль.

   Начнется создание файла с резервной копией ключевой информации.

Внимание! Создание файла с резервной копией ключевой информации может занять до 15 минут.

   Созданный файл с резервной копией ключевой информации ViPNet SIES MC будет записан в указанный каталог USB-носителя.

7 Закройте мастер инициализации, введя символ `8`.

Повторная инициализация ViPNet SIES MC

При возникновении проблем с подключением к веб-интерфейсу ViPNet SIES MC предусмотрена возможность изменения сетевых настроек и сертификатов с помощью повторной инициализации ViPNet SIES MC локально в консоли Linux.

При повторной инициализации ViPNet SIES MC сохраняется вся рабочая информация для управления SIES-узлами, зарегистрированными в ViPNet SIES MC.

Повторная инициализация позволит вам:

- изменить сетевые настройки;
- создать новые ключи ViPNet SIES MC, запрос на новый сертификат ViPNet SIES MC для подключения администраторов и загрузить новый сертификат;
- загрузить дополнительный корневой сертификат пользовательской ключевой подсистемы ViPNet SIES и список аннулированных сертификатов удостоверяющего центра, в котором издан сертификат ViPNet SIES MC для подключения администраторов;
- загрузить дополнительный сертификат супер-администратора.

Сведения о выполненных действиях фиксируются в журнале событий, который вы можете просмотреть (на стр. 54) по завершении повторной инициализации из веб-интерфейса ViPNet SIES MC.

Повторная инициализация проводится администратором с правом локального доступа из консоли Linux с помощью мастера инициализации. Все выполняемые действия аналогичны действиям, выполненным в ходе начальной инициализации ViPNet SIES MC.

Чтобы провести инициализацию ViPNet SIES MC повторно:

1. Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.

   Если в ходе инициализации вы планируете экспортировать запрос на новый сертификат ViPNet SIES MC для подключения администраторов или загружать в ViPNet SIES MC какие-либо сертификаты, подключите также USB-носитель.

2. Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3. Из предложенного списка действий выберите повторную инициализацию **Restart initialization**, введя символ `4`.

4. По завершении перезагрузки Linux вновь авторизуйтесь в консоли Linux как суперпользователь `root`.

   Автоматически запустится мастер инициализации ViPNet SIES MC.

5. На запрос **Change root password** для смены пароля суперпользователя введите символ `n` или пропустите шаг, введя символ `y`.

6 Из предложенного списка действий выберите повторную инициализацию **Reinitialization**, введя символ `1`.

Внимание! При выборе режима восстановления из резервной копии (вы ввели символ `y`) все настройки ViPNet SIES MC будут сброшены, и вам потребуется заново выполнить все настройки, как при начальной инициализации ViPNet SIES MC.

---

7 Проведите повторную инициализацию ViPNet SIES MC аналогично начальной инициализации ViPNet SIES MC (на стр. 15).

Внимание! Запрещается менять дату, время и часовой пояс, заданные при начальной инициализации ViPNet SIES MC.

Мастер инициализации ViPNet SIES MC предложит вам пропустить ранее пройденные шаги.

Если заданные настройки не требуют изменений, на запрос **Skip** о каждом ранее пройденном шаге введите символ `y` для пропуска шага.

Если вы хотите изменить настройки, выполняемые на шаге, в строке **Skip** этого шага введите символ `n` и укажите запрашиваемые данные в соответствии с описанием шага.

По окончании повторной инициализации ViPNet SIES MC зафиксируйте факт выполнения повторной инициализации ViPNet SIES MC в бумажном журнале регламентных работ с ViPNet SIES MC от имени администратора с правом локального доступа.

Смена пароля администратора с правом локального доступа

Вы можете сменить пароль администратора с правом локального доступа, например, в случае увольнения сотрудника, назначенного администратором с правом локального доступа.

Смена пароля администратора с правом локального доступа выполняется в консоли Linux в ходе повторной инициализации ViPNet SIES MC.

Совет. Для повышения безопасности рекомендуем периодически менять пароль администратора с правом локального доступа.

Чтобы сменить пароль:

1 Подключите монитор, клавиатуру и USB-носитель к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

3 Из предложенного списка действий выберите режим повторной инициализации **Restart initialization (to restore data and change system settings)**, введя символ `4`.

Последует перезагрузка Linux и ПО ViPNet SIES MC.

4 Снова авторизуйтесь в консоли Linux под учетной записью администратора с правом локального доступа.

5 Откажитесь от пропуска шага **Change root password**. Для этого в строке **Skip** введите символ `n`.

6 В строке **Enter new password** введите пароль в соответствии с требованиями к паролю и в строке **Repeat password** подтвердите пароль.

Внимание! Запомните новый пароль. Забытый пароль восстановить невозможно.

После успешного изменения пароля вы увидите соответствующее сообщение.

7 Дальнейшая последовательность шагов совпадает с шагами начальной инициализации ViPNet SIES MC (на стр. 15). Пропустите их, вводя в строке **Skip** для каждого шага символ `y`.

Внимание! При выборе режима восстановления из резервной копии (вы ввели символ `y`) все настройки ViPNet SIES MC будут сброшены, и вам потребуется заново выполнить все настройки, как при начальной инициализации ViPNet SIES MC.

Изменение уровня детализации записей служебных журналов

Вы можете изменить уровень детализации записей служебных журналов ViPNet SIES MC, например, перед передачей журналов представителю компании ИнфоТеКС для анализа.

Чтобы изменить уровень детализации записей служебных журналов:

1 Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3 Из предложенного списка действий выберите изменение уровня детализации служебных журналов **Change log level**, введя символ `5`.

4 На запрос **Choose log level** введите номер нужного уровня детализации работы программных модулей ViPNet SIES MC в записях журнала (детализация возрастает по мере уменьшения номера уровня):

- `trace` — вывод сообщений обо всех событиях;
- `debug` — вывод отладочных сообщений;

- `info` — вывод уведомлений;
- `warning` — вывод предупреждений;
- `error` — вывод сообщений обо всех ошибках;
- `critical` — вывод сообщений о критических ошибках.

5 Закройте мастер инициализации, введя символ `8`.

Перезагрузка ViPNet SIES MC

Вы можете перезагрузить ViPNet SIES MC, выполнив для этого следующие действия:

1 Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3 Из предложенного списка действий выберите перезагрузку **Reboot**, введя символ `6`.

Выключение ViPNet SIES MC

Вы можете выключить ViPNet SIES MC, выполнив для этого следующие действия:

1 Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3 Из предложенного списка действий выберите выключение **Power off**, введя символ `7`.

Подготовка к выводу из эксплуатации

Перед выводом ViPNet SIES MC из эксплуатации следует очистить ключевую информацию ViPNet SIES MC.

Внимание! После очистки ключевой информации ViPNet SIES MC станет непригодным к дальнейшему использованию.

Чтобы очистить ключевую информацию и подготовить ViPNet SIES MC к выводу из эксплуатации:

1 Подключите монитор и клавиатуру к аппаратной платформе ViPNet SIES MC.

2 Авторизуйтесь в консоли Linux как суперпользователь `root`.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

3. Из предложенного списка действий выберите повторную инициализацию **Restart initialization**, введя символ `4`.
4. По завершении перезагрузки Linux вновь авторизуйтесь в консоли Linux, используя учетную запись суперпользователя `root`.

   Автоматически запустится мастер инициализации ViPNet SIES MC.
5. Из предложенного списка действий выберите вывод из эксплуатации **Decommission**, введя символ `3`.
6. Подтвердите вывод ViPNet SIES MC из эксплуатации, введя символ `y`.
7. Выключите аппаратную платформу ViPNet SIES MC.

Теперь ViPNet SIES MC готов к выводу из эксплуатации.

4

Резервное копирование и восстановление данных

Общие сведения 70

Создание резервной копии рабочей информации 72

Экспорт резервной копии рабочей информации 73

Восстановление данных из резервной копии 75

Общие сведения

Резервное копирование позволяет сохранять данные ViPNet SIES MC, восстановление которых может потребоваться в случае сбоев в работе ViPNet SIES MC.

Совет. Мы рекомендуем регулярно выполнять резервное копирование данных и хранить резервные копии на внешнем носителе.

Полная резервная копия данных ViPNet SIES MC состоит из двух архивов:

- резервная копия рабочей информации — создается (на стр. 72) из веб-интерфейса ViPNet SIES MC супер-администратором или администратором MC;
- резервная копия ключевой информации — создается (на стр. 63) из консоли Linux администратором с правом локального доступа.

Таблица 9. Состав и рекомендуемая периодичность создания резервных копий

Резервная копия рабочей информации	Резервная копия ключевой информации
• Идентификатор версии ПО ViPNet SIES MC • Настройки ViPNet SIES MC • Список и настройки SIES-узлов • Прикладные связи между SIES-узлами • Сертификаты служебной, пользовательской и прикладной ключевых подсистем ViPNet SIES • Отметки об использовании ключей • Сроки действия прикладных симметричных мастер-ключей ViPNet SIES	• Ключи электронной подписи и ключи проверки электронной подписи ViPNet SIES MC • Прикладные симметричные мастер-ключи ViPNet SIES
Критерии создания	**Критерии создания**
• После ввода в эксплуатацию SIES-узла • После регламентного обслуживания защищаемого устройства или SIES-узла • После изменения прикладных связей • После добавления администратора в ViPNet SIES MC • После обновления ключевой информации ViPNet SIES • После изменения настроек ViPNet SIES MC • Перед изменением сетевых настроек ViPNet SIES MC • Перед обновлением ПО ViPNet SIES MC Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».	• После создания прикладного симметричного мастер-ключа ViPNet SIES

Лицензия в резервной копии не сохраняется. Архивы с резервными копиями защищаются шифрованием на пароле, который администратор задает перед созданием каждой резервной копии.

Если при обслуживании ViPNet SIES MC у вас возникли проблемы с удаленным доступом через веб-интерфейс ViPNet SIES MC, то предусмотрена возможность повторной инициализации ViPNet SIES MC (на стр. 64) из консоли Linux, которая позволяет задать настройки для восстановления удаленного доступа к веб-интерфейсу ViPNet SIES MC.

Восстановление данных (на стр. 75) и повторная инициализация ViPNet SIES MC (на стр. 64) выполняется администратором с правом локального доступа.

Создание резервной копии рабочей информации

Чтобы создать резервную копию рабочей информации ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сервисные функции** .

3 В разделе **Резервная копия** нажмите кнопку **Создать**.

   Запустится создание архива с резервной копией рабочей информации ViPNet SIES MC. Создание архива с резервной копией рабочей информации может занять продолжительное время.

Совет. Чтобы резервную копию можно было использовать для восстановления данных в случае сбоя, выгрузите (на стр. 73) резервную копию из ViPNet SIES MC для последующего хранения на внешнем носителе.

Чтобы иметь возможность полностью восстановить данные в случае сбоя, создайте также резервную копию ключевой информации (на стр. 63).

Экспорт резервной копии рабочей информации

Созданные резервные копии рабочей информации хранятся на ViPNet SIES MC. Чтобы резервную копию можно было использовать для восстановления данных после сбоя, сохраните резервную копию на внешнем носителе (например, на USB-носителе).

Совет. Чтобы не возникло проблем при восстановлении данных из резервной копии, используйте внешний носитель USB версии 2.0 с файловой системой FAT32.

Чтобы сохранить резервную копию рабочей информации на вашем компьютере:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC (на стр. 26) с полномочиями супер-администратора или администратора MC.

2 Перейдите в раздел **Сервисные функции** .

3 В разделе **Резервная копия** нажмите кнопку **Выгрузить**.

4 Щелкните по резервной копии, которую хотите сохранить на своем компьютере.

5 Нажмите кнопку **Выгрузить**.

6 Задайте пароль для защиты резервной копии и нажмите кнопку **OK**.

Внимание! Пароль должен соответствовать следующим требованиям:

- иметь длину от 8 до 32 символов;
- содержать хотя бы одну цифру от 0 до 9;
- содержать хотя бы одну букву латинского алфавита от «A» до «Z» или от «a» до «z».

Пароль может содержать символы «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}».

Дополнительно не рекомендуется использовать:

- три и более символа, расположенные подряд на клавиатуре;
- три и более символа, идущие подряд в алфавитном порядке;
- один и тот же символ более двух раз.

7 Подтвердите введенный пароль и нажмите кнопку **OK**.

В результате на вашем компьютере будет создан файл с именем `backupX.X.X-XXXXXX_siesmc_ГГГГММДДТЧЧММССZ.tar.gz` с резервной копией рабочей информации ViPNet SIES MC:

- `X.X.X-XXXXXX` — версия ПО ViPNet SIES MC;

- `ГГГГММДДТЧЧММССZ` — дата и время создания резервной копии в формате ISO 8601 https://ru.wikipedia.org/wiki/ISO_8601.

Вы можете использовать резервную копию для восстановления данных в случае сбоя, предварительно записав резервную копию на USB-носитель.

Внимание! Запомните пароль защиты резервной копии. Если вы забудете пароль, восстановить его будет невозможно.

Восстановление данных из резервной копии

Для восстановления данных вам потребуется USB-носитель, содержащий следующие файлы:

- заранее созданную резервную копию данных (на стр. 72);
- заранее созданную резервную копию ключевой информации (на стр. 63).

Восстановление данных из резервной копии проводит администратор с правом локального доступа.

Восстановление данных после программного сбоя

Необходимость восстановления данных и настроек ViPNet SIES MC из резервной копии может возникнуть в случае программного сбоя при обновлении ПО ViPNet SIES MC.

Чтобы восстановить данные ViPNet SIES MC из резервной копии:

1. Подключите монитор, клавиатуру и внешний носитель USB версии 2.0 с файловой системой FAT32 с резервными копиями рабочей и ключевой информации к аппаратной платформе ViPNet SIES MC.
2. Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.
3. Из предложенного списка действий выберите повторную инициализацию **Restart initialization**, введя символ `4`.
4. По завершении перезагрузки Linux вновь авторизуйтесь в консоли Linux как суперпользователь `root`.
5. Мастер инициализации ViPNet SIES MC запустится автоматически.
6. Из предложенного списка действий выберите восстановление из резервной копии **Restore data from backup**, введя символ `2`.
7. На запрос **Enter full path to ViPNet SIES MC backup you want to restore from** введите полный путь к файлу с резервной копией данных на подключенном USB-носителе. Например, если файл с резервной копией находится в файле `backup_sies_mc_2016060600001.tar.gz` корневого каталога USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/backup_sies_mc_2016060600001.tar.gz`.
8. На запрос **Enter password for backup file** введите пароль к файлу с резервной копией данных.

9 На запрос **Enter full path to ViPNet SIES MC backup set of keys file you want to restore from** введите полный путь к файлу с резервной копией ключевой информации на подключенном USB-носителе. Например, если файл с резервной копией находится в файле `keys.backup.213` корневого каталога USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/keys.backup.213`.

10 На запрос **Enter password for backup file** введите пароль к файлу с резервной копией ключевой информации.

Начнется восстановление рабочей и ключевой информации ViPNet SIES MC из резервной копии.

Дождитесь сообщения **ViPNet SIES MC restored from backup successfully** об успешном завершении восстановления данных ViPNet SIES MC из резервной копии.

11 Дальнейшие шаги совпадают с шагами мастера начальной инициализации ViPNet SIES MC (на стр. 15). Если настройки из резервной копии не требуют изменения, вы можете пропустить соответствующие шаги мастера инициализации. Для пропуска шагов в строке **Skip** для каждого шага вводите символ `y`. Если вы хотите изменить настройки, выполняемые на шаге, в строке **Skip** для этого шага введите символ `n` и запрашиваемые данные в соответствии с описанием шага (на стр. 15).

12 На запрос **Complete ViPNet SIES MC initialization** введите символ `y`, подтверждая завершение восстановления.

Появится сообщение о завершении восстановления.

13 Для продолжения нажмите клавишу **Enter**.

Последует перезагрузка Linux и ПО ViPNet SIES MC.

14 Отсоедините USB-носитель.

После завершения восстановления данных ViPNet SIES MC из резервной копии рекомендуется:

- проверить состояние служебной и прикладной ключевых подсистем ViPNet SIES MC и SIES-узлов и при необходимости обновить ключи и сертификаты;
- обновить состояние каждого SIES-узла, зарегистрированного в ViPNet SIES MC.

Подробнее о выполнении указанных операций см. документ «ViPNet SIES MC. Руководство администратора».

Восстановление данных после аппаратного сбоя

Вы можете восстановить работоспособность ViPNet SIES MC в случае аппаратного или программного сбоя, не вызванного некорректной рабочей или ключевой информацией ViPNet SIES MC.

Чтобы восстановить данные ViPNet SIES MC из резервной копии:

1 У представителя компании ИнфоТеКС получите новую аппаратную платформу с активированной лицензией.

2 Установите ViPNet SIES MC до действия 6 (на стр. 13).

3 Подключите монитор, клавиатуру и внешний носитель USB версии 2.0 с файловой системой FAT32 с резервными копиями рабочей и ключевой информации к аппаратной платформе ViPNet SIES MC.

4 Авторизуйтесь в консоли Linux:

- на приглашение **login** введите `root` и нажмите клавишу **Enter**;
- на приглашение **Password** введите технологический пароль `vipnet` и нажмите клавишу **Enter**.

5 Задайте новый пароль учетной записи администратора с правом локального доступа:

Внимание! Пароль должен соответствовать следующим требованиям:

- иметь длину от 8 до 32 символов;
- содержать хотя бы одну цифру от 0 до 9;
- содержать хотя бы одну букву латинского алфавита от «A» до «Z» или от «a» до «z».

Пароль может содержать символы «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}».

Дополнительно не рекомендуется использовать:

- три и более символа, расположенные подряд на клавиатуре;
- три и более символа, идущие подряд в алфавитном порядке;
- один и тот же символ более двух раз.

5.1 На запрос **Enter new password** введите пароль.

5.2 На запрос **Confirm password** повторно введите тот же пароль.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

6 Из предложенного списка действий выберите восстановление из резервной копии **Restore data from backup**, введя символ `2`.

7 На запрос **Enter full path to ViPNet SIES MC backup you want to restore from** введите полный путь к файлу с резервной копией данных на подключенном USB-носителе. Например, если файл с резервной копией находится в файле `backup_sies_mc_2016060600001.tar.gz` корневого каталога USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/backup_sies_mc_2016060600001.tar.gz`.

8 На запрос **Enter password for backup file** введите пароль к файлу с резервной копией данных.

9 На запрос **Enter full path to ViPNet SIES MC backup set of keys file you want to restore from** введите полный путь к файлу с резервной копией ключевой информации на подключенном USB-носителе. Например, если файл с резервной копией находится в файле `keys.backup.213` корневого каталога USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/keys.backup.213`.

10 На запрос **Enter password for backup file** введите пароль к файлу с резервной копией ключевой информации.

Начнется восстановление рабочей и ключевой информации ViPNet SIES MC из резервной копии.

Дождитесь сообщения **ViPNet SIES MC restored from backup successfully** об успешном завершении восстановления данных ViPNet SIES MC из резервной копии.

11 Дальнейшие шаги совпадают с шагами мастера начальной инициализации ViPNet SIES MC (на стр. 15). Если настройки из резервной копии не требуют изменения, вы можете пропустить соответствующие шаги мастера инициализации. Для пропуска шагов в строке **Skip** для каждого шага вводите символ `y`. Если вы хотите изменить настройки, выполняемые на шаге, в строке **Skip** для этого шага введите символ `n` и запрашиваемые данные в соответствии с описанием шага (на стр. 15).

12 На запрос **Complete ViPNet SIES MC initialization** введите символ `y`, подтверждая завершение восстановления.

Появится сообщение о завершении восстановления.

13 Для продолжения нажмите клавишу **Enter**.

Последует перезагрузка Linux и ПО ViPNet SIES MC.

14 Отсоедините USB-носитель.

После завершения восстановления данных ViPNet SIES MC из резервной копии рекомендуется:

- задать часовой пояс, текущую дату и время, выполнив повторную инициализацию ViPNet SIES MC (на стр. 64);
- проверить состояние служебной и прикладной ключевых подсистем ViPNet SIES MC и SIES-узлов и при необходимости обновить ключи и сертификаты;
- обновить состояние каждого SIES-узла, зарегистрированного в ViPNet SIES MC.

Подробнее о выполнении указанных операций см. документ «ViPNet SIES MC. Руководство администратора».

A

Уровни критичности событий

В ViPNet SIES MC регистрируются все события, происходящие (на стр. 54) в ходе эксплуатации ViPNet SIES MC.

События разделяются по уровням критичности, позволяющим оценивать состояние ViPNet SIES MC и серьезность выявленной проблемы.

Информация о критичности событий отображается в разделе **Журнал событий** , в разделе **Сообщения** и оповещениях различными цветами.

Выделяются следующие уровни критичности:

- **Высокий уровень** (красный цвет) — наиболее критичные события. Выявлены серьезные проблемы, требующие немедленного вмешательства. ViPNet SIES MC в критическом состоянии, работоспособность ViPNet SIES MC нарушена.
- **Средний уровень** (желтый цвет) — ViPNet SIES MC находится в опасном состоянии. Выявлены проблемы, не требующие немедленного вмешательства. Если выявленные проблемы не решить в ближайшем будущем, они могут нарушить работоспособность ViPNet SIES MC.
- **Информационное событие** (зеленый цвет) — события уведомительного характера. ViPNet SIES MC в нормальном состоянии и работает в штатном режиме.

В разделе **Сообщения** выводятся те события, на которые требуется реакция администратора ViPNet SIES MC.

B

Возможные неполадки и способы их устранения

Администратор не может подключиться к веб-интерфейсу

Администратор с рабочего места не может подключиться к веб-интерфейсу ViPNet SIES MC.

Возможная причина № 1

На рабочем месте администратора истекли сроки действия одного или нескольких сертификатов пользовательской ключевой подсистемы ViPNet SIES из-за несвоевременного обновления.

Способ устранения

1. На рабочем месте администратора проверьте сроки действия:
   - корневого сертификата пользовательской ключевой подсистемы;
   - списка аннулированных сертификатов;
   - сертификата администратора.
2. Запросите у администратора безопасности новый сертификат или список аннулированных сертификатов.
3. Воспользовавшись документацией на используемый криптопровайдер, установите новые сертификаты на рабочем месте администратора.
4. Повторите попытку подключения к веб-интерфейсу ViPNet SIES MC.

Возможная причина № 2

На ViPNet SIES MC истекли сроки действия одного или нескольких сертификатов пользовательской ключевой подсистемы ViPNet SIES из-за несвоевременного обновления.

Способ устранения

1. Проведите повторную инициализацию ViPNet SIES MC (на стр. 64), загрузив новые сертификаты.
2. В зависимости от того, какие сертификаты обновлялись, установите новые сертификаты на рабочем месте администратора.
3. Повторите попытку подключения к веб-интерфейсу ViPNet SIES MC.

Возможная причина № 3

Отсутствует доступ в Интернет.

Способ устранения

Проверьте наличие доступа в Интернет на рабочем месте администратора и повторите попытку подключения к веб-интерфейсу ViPNet SIES MC.

Возможная причина № 4

Изменились настройки используемого криптопровайдера.

Способ устранения

1. Воспользовавшись документацией на используемый криптопровайдер, проверьте корректность текущих настроек криптопровайдера на рабочем месте администратора.
2. Повторите попытку подключения к веб-интерфейсу ViPNet SIES MC.

Не удается загрузить веб-интерфейс ViPNet SIES MC

При загрузке веб-интерфейса ViPNet SIES MC с рабочего места администратора выводится бесконечное сообщение **Загрузка**.

Способ устранения

1. Очистите кэш браузера.
2. Перезагрузите веб-интерфейс ViPNet SIES MC в браузере.

Не удается загрузить веб-интерфейс ViPNet SIES MC с использованием ViPNet PKI Client TLS Unit

При загрузке веб-интерфейса ViPNet SIES MC с рабочего места администратора выводится бесконечное сообщение **Загрузка**.

Способ устранения

1. Правой кнопкой мыши щелкните значок в области уведомлений.
2. В меню выберите **Выключить**.
3. Повторите действие 1 и выберите **Очистить кэш сертификатов**.
4. Повторите действие 1 и выберите **Включить**.
5. Для обновления веб-интерфейса ViPNet SIES MC в браузере нажмите клавиши **Ctrl+F5**.
6. Повторно выберите сертификат и подключитесь к веб-интерфейсу ViPNet SIES MC по протоколу TLS.

Блокировка работы ViPNet SIES MC

При работе с веб-интерфейсом ViPNet SIES MC возникают сообщения об ошибках базы данных. В журнале событий ViPNet SIES MC появилась запись об исчерпании дискового пространства.

Возможная причина

Исчерпано свободное дисковое пространство ViPNet SIES MC.

Способ устранения

1. Выгрузите архивы событий из ViPNet SIES MC (на стр. 55).
2. Удалите архивы событий из ViPNet SIES MC (на стр. 56).
3. Выгрузите архивы с записями журнала аудита SIES-узлов из ViPNet SIES MC и удалите архивы записей. См. документ «ViPNet SIES MC. Руководство администратора».
4. Удалите версии ПО SIES-узлов, не используемые на SIES-узлах.

Сообщение о превышении лицензионных ограничений

Выводится сообщение мониторинга о превышении текущих лицензионных ограничений по SIES-узлам или администраторам. При попытке обновить лицензию выводится перечень лицензионных ограничений, которым не соответствует ViPNet SIES MC.

Возможная причина

Текущее количество объектов превышает указанное в лицензии количество объектов по одному или нескольким критериям из следующих:

- максимальная версия ПО ViPNet SIES Core;
- количество ViPNet SIES Core;
- количество прикладных связей ViPNet SIES Unit;
- количество ViPNet SIES Unit;
- количество администраторов ViPNet SIES MC.

Способ устранения

1. Исключите из управления ViPNet SIES Core с более высокой версией ПО по сравнению с указанной в лицензии версией ПО.
2. Временно исключите из управления избыточные ViPNet SIES Core. См. документ «ViPNet SIES MC. Руководство администратора».
3. Временно сократите количество прикладных связей ViPNet SIES Unit.
4. Удалите избыточные ViPNet SIES Unit.
5. Временно отзовите право доступа части администраторов в веб-интерфейс ViPNet SIES MC.

Для снятия лицензионных ограничений обратитесь к представителю компании ИнфоТеКС за расширением дополнительной лицензии на SIES-узлы или количество администраторов.

Не удается создать прикладной мастер-ключ

При создании прикладного мастер-ключа или при синхронизации прикладных связей SIES-узлов в журнале событий программно-аппаратного исполнения ViPNet SIES MC и в разделе **Сообщения** появилось уведомление **Не удалось создать мастер-ключ**.

Возможная причина

Повышенная вибрация в области размещения аппаратной платформы ViPNet SIES MC, приведшая к кратковременному отключению датчика случайных чисел.

Способ устранения

Перезагрузите ViPNet SIES MC.

C

Глоссарий

RESTful API

REST (Representational State Transfer) — архитектурный стиль взаимодействия компонентов распределенного приложения в сети. Это согласованный набор ограничений (веб-API), учитываемых при проектировании распределенной гипермедиа-системы. Удаленный вызов процедуры — HTTP-запрос (обычно «GET» или «POST» — REST-запрос). Данные передаются в параметрах запроса.

SIES-узел

Компонент комплекса ViPNet SIES, развернутый в индустриальной системе, выполняющий прикладные криптографические операции над данными индустриальной системы и централизованно управляемый с помощью ViPNet SIES MC.

TLS (Transport Layer Security)

Криптографический протокол защищенной передачи данных между узлами в Интернете с применением асимметричной криптографии для аутентификации, симметричного шифрования для конфиденциальности и кодов аутентичности для сохранения целостности сообщений. Используется для подключения рабочего места администратора к веб-интерфейсу ViPNet SIES MC и для подключения рабочего места оператора ViPNet SIES Workstation к ViPNet SIES MC.

ViPNet SIES (Security for Industrial and Embedded Solutions)

Комплекс продуктов компании ИнфоТеКС для защиты информации в индустриальных системах.

ViPNet SIES Core

Компонент комплекса ViPNet SIES. Программно-аппаратный комплекс, встраиваемый в защищаемое устройство. Взаимодействует с защищаемым устройством через аппаратный интерфейс в качестве ведомого устройства и выполняет функции SIES-узла.

ViPNet SIES MC

Система управления SIES-узлами. Отправляет SIES-узлам защищенные команды управления и мониторинга по каналам связи индустриальной системы. Выполняет роль центра управления ключевой системой ViPNet SIES.

ViPNet SIES Workstation

Автоматизированное рабочее место локального обслуживания SIES-узлов, функционирующее совместно с ViPNet SIES MC.

Аутентификация

Процедура проверки подлинности на основе сравнения данных, предоставленных субъектом и данных, хранящихся на объекте.

Действительность сертификата

Сертификат считается действительным, если на текущую дату он не аннулирован, а срок его действия уже начался и еще не истек.

Доверенный способ передачи данных

Канал, исключающий компрометацию данных при передаче между взаимодействующими сторонами.

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).

Защищаемое устройство

Техническое средство обработки информации индустриальной системы, интегрированное с SIES-узлом.

Защищенный конверт

Команда управления или мониторинга ViPNet SIES MC или ответ SIES-узла, упакованный в криптографический контейнер, защищенный от прочтения и подмены данных.

Индустриальная система

Комплекс средств, обеспечивающий полный цикл функционирования производства или отдельного технологического процесса в различных областях экономики.

Инициализация SIES-узла

Загрузка служебной ключевой информации на SIES-узел для организации защищенного канала управления SIES-узлом из ViPNet SIES MC перед началом использования прикладных криптографических функций SIES-узла. Может выполняться в ручном или автоматическом режимах в зависимости от типа SIES-узла.

Ключ SIES-узла

Симметричный криптографический ключ прикладной ключевой подсистемы SIES-узла, выработанный в ViPNet SIES MC на прикладном мастер-ключе для связанных SIES-узлов. Передается на связанные SIES-узлы для криптографической обработки данных, передаваемых между взаимодействующими защищаемыми устройствами.

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.

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Контролируемая зона

Территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

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.

Корневой сертификат пользовательской ключевой подсистемы ViPNet SIES

Доверенный сертификат ключа проверки электронной подписи внешнего удостоверяющего центра. Удостоверяет сертификаты администраторов ViPNet SIES MC, сертификаты ViPNet SIES MC для подключения администраторов по протоколу TLS.

Корневой сертификат прикладной ключевой подсистемы ViPNet SIES

Сертификат ключа проверки электронной подписи (самоподписанный сертификат ViPNet SIES MC или доверенный сертификат внешнего удостоверяющего центра), удостоверяющий прикладные сертификаты SIES-узлов, издаваемые ViPNet SIES MC.

Корневой сертификат служебной ключевой подсистемы ViPNet SIES

Самоподписанный сертификат ключа проверки электронной подписи, издаваемый ViPNet SIES MC. Удостоверяет служебные сертификаты SIES-узлов и ViPNet SIES MC, издаваемые ViPNet SIES MC.

Криптопровайдер

Независимый программный модуль, позволяющий выполнять криптографические функции в операционной системе.

Прикладная связь

Набор криптографических параметров и ключевой информации, с помощью которого защищаемое устройство может выполнять криптографические операции над данными. Прикладная связь задается с помощью ViPNet SIES MC и хранится на SIES-узлах взаимодействующих защищаемых устройств.

Прикладной мастер-ключ ViPNet SIES

Симметричный криптографический ключ прикладной ключевой подсистемы ViPNet SIES, на котором вырабатываются ключи SIES-узлов. Хранится в ViPNet SIES MC.

Прикладной сертификат SIES-узла

Сертификат ключа проверки электронной подписи SIES-узла. Используется в криптографических операциях с данными защищаемого устройства индустриальной системы.

Программно-аппаратный комплекс (ПАК)

Набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Программное обеспечение (ПО)

Совокупность программ системы обработки информации и программных документов для эксплуатации этих программ.

Сертификат ViPNet SIES MC для подключения администраторов

Сертификат ключа проверки электронной подписи ViPNet SIES MC. Используется для проверки подлинности ViPNet SIES MC на стороне администратора при TLS-подключении рабочего места администратора к веб-интерфейсу ViPNet SIES MC.

Сертификат администратора ViPNet SIES MC

Сертификат ключа проверки электронной подписи администратора ViPNet SIES MC. Издается внешним удостоверяющим центром и передается администратору ViPNet SIES MC для аутентификации при TLS-подключении рабочего места администратора к веб-интерфейсу ViPNet SIES MC.

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.

Служебный сертификат SIES-узла

Сертификат ключа проверки электронной подписи SIES-узла. Используется при организации обмена защищенными конвертами с ViPNet SIES MC.

Служебный сертификат ViPNet SIES MC

Сертификат ключа проверки электронной подписи ViPNet SIES MC. Используется при организации обмена защищенными конвертами с SIES-узлами.

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.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Файл *.PEM

Текстовый файл с сертификатом, закодированным по схеме Base64. Может иметь расширение `.pem`, `.crt`, `.cer` или `.key` (контейнер с закрытым ключом). Текст PEM-файла начинается с тега `-----BEGIN CERTIFICATE-----` и заканчивается тегом `-----END CERTIFICATE-----`. Теги позволяют отличить сертификат в формате PEM от других форматов.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации 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.