ViPNet SIES MC

Руководство администратора

infotecs

© ОАО «ИнфоТеКС», 2020

ФРКЕ.00194-02 32 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 ... **7**
О документе ... 8
Для кого предназначен документ ... 8
Комплект документации ViPNet SIES MC ... 8
Связанные документы ... 8
Соглашения документа ... 9
Обратная связь ... 11
О работе администратора ViPNet SIES MC ... 12

Глава 1. Управление SIES-узлами ... **13**
Об управлении SIES-узлами ... 15
Добавление SIES-узла в ViPNet SIES MC ... 16
Добавление ViPNet SIES Core ... 16
Добавление ViPNet SIES Core по списку ... 18
Добавление ViPNet SIES Unit по запросу на служебный сертификат ... 19
Добавление пользователя защищаемого устройства ... 20
Добавление другого SIES-узла ... 21
Завершение инициализации SIES-узла ... 23
Отмена инициализации SIES-узла ... 24
Повторное завершение инициализации SIES-узла ... 25
Просмотр сведений о SIES-узле ... 26
Изменение атрибутов SIES-узла ... 28
Смена режима работы SIES-узла ... 30
Смена режима управления SIES-узлом ... 32
Локальное управление SIES-узлом: порядок действий ... 34
Управление ключевой системой SIES-узла ... 35
Настройка прикладной ключевой подсистемы для использования сертификатов: порядок действий ... 36
Настройка прикладной ключевой подсистемы для поддержки аутентификации пользователя защищаемого устройства: порядок действий ... 37
Просмотр сведений о сертификатах SIES-узла ... 39
Создание и загрузка сертификата на SIES-узел ... 41
Загрузка сертификата на SIES-узел ... 42
Получение списка сертификатов SIES-узла ... 44
Удаление сертификата из ViPNet SIES MC ... 44

Удаление сертификата с SIES-узла 45
Импорт запроса на сертификат....46
Экспорт сертификата 47
Обновление инициализирующей последовательности SIES-узла....48
Управление прикладными связями SIES-узла 49
Просмотр прикладных связей....49
Синхронизация прикладных связей....51
Удаление всех прикладных связей на SIES-узле 52
Отмена задачи управления....54
Отмена одной задачи 54
Отмена всех выполняющихся и ожидающих выполнения задач 55
Выгрузка защищенного конверта с командой для SIES-узла....56
Загрузка защищенного конверта с ответом SIES-узла 58
Одновременное управление несколькими SIES-узлами....59
Исключение SIES-узла из управления ViPNet SIES MC....61
Подключение SIES-узла к управлению ViPNet SIES MC....62
Контроль инициализации SIES-узлов 63
Компрометация SIES-узла....64
Фиксация компрометации SIES-узла 64
Просмотр сведений о компрометации SIES-узла 65
Приведение SIES-узла к заводскому состоянию....66
Снятие отметки о компрометации SIES-узла....67
Удаление SIES-узла 68

Глава 2. Управление ViPNet SIES Core....69
Задание связи ViPNet SIES Core с защищаемым устройством 70
Выполнение контроля целостности и версии ПО ViPNet SIES Core 71
Включение датчика контроля доступа к ViPNet SIES Core....72
Отключение датчика контроля доступа к ViPNet SIES Core....73
Управление журналом аудита 74
Получение записей....74
Просмотр записей....75
Очистка журнала 76
Создание архива записей....76
Выгрузка архива записей....77
Удаление архива записей 78
Управление служебным журналом....79
Получение записей....79
Очистка журнала 79

Выгрузка архива записей ... 80
Изменение уровня журналирования ... 80
Управление обновлениями ПО ... 82
Обновление ПО до версии 2.2.1: порядок действий ... 82
Добавление обновления ... 83
Обновление ПО ... 84
Удаление обновления ... 85

Глава 3. Управление ViPNet SIES Unit ... 87
Ручная инициализация ViPNet SIES Unit: порядок действий ... 88

Глава 4. Управление SIES-узлами другого типа ... 89
Ручная инициализация другого SIES-узла: порядок действий ... 90

Глава 5. Управление защищаемыми устройствами ... 91
Об управлении защищаемыми устройствами ... 92
Добавление защищаемого устройства ... 93
Просмотр сведений о защищаемом устройстве ... 96
Изменение параметров защищаемого устройства ... 97
Назначение SIES-узла на защищаемое устройство ... 98
Отмена назначения SIES-узла на защищаемое устройство ... 99
Одновременное управление несколькими защищаемыми устройствами ... 100
Регистрация резервных защищаемых устройств: порядок действий ... 101
Удаление защищаемого устройства ... 103
Управление прикладными связями защищаемого устройства ... 104
Управление парными связями ... 106
Добавление парной связи для защищаемого устройства ... 106
Добавление парной связи для группы защищаемых устройств ... 107
Добавление парных связей между выбранными защищаемыми устройствами ... 109
Управление резервированными парными связями ... 111
Добавление резервированной парной связи ... 111
Добавление защищаемого устройства в резервированную парную связь ... 113
Исключение защищаемого устройства из резервированной парной связи ... 114
Управление мультивещательными связями ... 115
Добавление мультивещательной связи для защищаемого устройства ... 115
Добавление мультивещательной связи для группы защищаемых устройств ... 118
Добавление участника мультивещательной связи ... 119
Исключение участника мультивещательной связи ... 121

Изменение списка отправителей в мультивещательной связи ... 122
Просмотр связей ... 122
Изменение назначений связи ... 124
Удаление связи ... 125

Глава 6. Управление группами защищаемых устройств и SIES-узлов ... 127
О группах ... 128
Создание группы ... 131
Просмотр группы ... 133
Перемещение элемента в группу ... 134
Изменение параметров группы ... 136
Удаление элемента из группы ... 137
Удаление группы ... 138

Глава 7. Визуальное отображение SIES-узлов и прикладных связей ... 139
О структурной схеме индустриальной системы ... 140
Просмотр состояния SIES-узла ... 141
Просмотр состояния прикладной связи защищаемого устройства ... 142

Приложение A. Параметры SIES-узла ... 143
Основные параметры ... 144
Вкладка Общее ... 145
Вкладка Задачи ... 148

Приложение B. Аппаратные платформы ViPNet SIES Core ... 149

Приложение C. Уровни критичности событий ... 150

Приложение D. Возможные неполадки и способы их устранения ... 151
Длительное выполнение команды ... 152
Команды не выполняются на SIES-узле ... 153
Не выполняются криптографические операции в адрес другого SIES-узла ... 154
Не синхронизируется прикладная связь ... 155
Не полностью синхронизируются прикладные связи на ViPNet SIES Core ... 156
Ошибка выполнения задачи синхронизации прикладных связей ... 157
Не удается создать и загрузить сертификат на ViPNet SIES Core ... 158

Приложение E. Глоссарий ... 159

Введение

О документе 8

Обратная связь 11

О работе администратора ViPNet SIES MC 12

О документе

Документ содержит информацию по работе с центром ViPNet® SIES MC, управляющим компонентами комплекса ViPNet SIES.

Документ также содержит методы решения основных задач администратора по централизованному контролю и управлению компонентами комплекса ViPNet SIES.

Для кого предназначен документ

Данный документ предназначен для администраторов, с помощью ViPNet SIES MC управляющих компонентами ViPNet SIES, интегрированными в индустриальную систему.

Предполагается, что администратор обладает базовым представлением о криптографической защите данных, а также об устройстве компьютерных и индустриальных систем, основах резервирования технических систем.

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.

Связанные документы

В таблице ниже перечислены документы, с которыми мы рекомендуем вам также ознакомиться.

Таблица 1. Связанные документы

Документ	О документе
ViPNet SIES MC. Установка и обслуживание	Документ содержит методику установки и настройки ViPNet SIES MC и рабочих мест администраторов ViPNet SIES MC. Документ входит в комплект поставки ViPNet SIES MC.
ViPNet SIES Core. Общее описание	В данном документе вы найдете описание, технические характеристики и методику применения программно-аппаратных комплексов ViPNet SIES Core, входящих в состав комплекса ViPNet SIES. Документ входит в комплект поставки ViPNet SIES Core.
ViPNet SIES Unit. Руководство администратора	В документе приведена методика установки и настройки программного обеспечения ViPNet SIES Unit, входящего в состав комплекса ViPNet SIES и предназначенного для защиты информации, обрабатываемой устройствами верхнего уровня индустриальной и IIoT-системы. Документ входит в комплект поставки ViPNet SIES Unit.

Соглашения документа

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

Таблица 2. 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 3. 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.

Обозначение	Описание
`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.

О работе администратора ViPNet SIES MC

Чтобы начать работу, подключите свое рабочее место к веб-интерфейсу ViPNet SIES MC по протоколу TLS с помощью персонального сертификата администратора ViPNet SIES MC. Подробнее см. документ «ViPNet SIES MC. Установка и обслуживание».

1

Управление SIES-узлами

Об управлении SIES-узлами 15

Добавление SIES-узла в ViPNet SIES MC 16

Завершение инициализации SIES-узла 23

Отмена инициализации SIES-узла 24

Повторное завершение инициализации SIES-узла 25

Просмотр сведений о SIES-узле 26

Изменение атрибутов SIES-узла 28

Смена режима работы SIES-узла 30

Смена режима управления SIES-узлом 32

Локальное управление SIES-узлом: порядок действий 34

Управление ключевой системой SIES-узла 35

Управление прикладными связями SIES-узла 49

Отмена задачи управления 54

Выгрузка защищенного конверта с командой для SIES-узла 56

Загрузка защищенного конверта с ответом SIES-узла 58

Одновременное управление несколькими SIES-узлами 59

Исключение SIES-узла из управления ViPNet SIES MC 61

Подключение SIES-узла к управлению ViPNet SIES MC 62

Контроль инициализации SIES-узлов 63

Компрометация SIES-узла 64

Удаление SIES-узла 68

Об управлении SIES-узлами

С помощью прикладных функций SIES-узлов (см. глоссарий, стр. 159) выполняется криптографическая обработка данных защищаемых устройств в зависимости от реализуемых сценариев защиты данных. Подробнее см. документ «ViPNet SIES. Сценарии работы».

С помощью ViPNet SIES MC вы можете управлять SIES-узлами, функционирующими в индустриальной системе вашей организации и подключенными к ViPNet SIES MC.

Доступный администратору ViPNet SIES MC набор операций зависит от типа SIES-узла и назначенной роли управления:

- ViPNet SIES Core (см. глоссарий, стр. 159);
- ViPNet SIES Unit (см. глоссарий, стр. 159);
- пользователь защищаемого устройства, зарегистрированный в качестве SIES-узла одноименного типа;
- другой тип SIES-узла — сторонний компонент для криптографической обработки данных защищаемого устройства.

В описаниях операций управления применимость конкретной операции к SIES-узлу конкретного типа указана в подразделе «Область применения».

Параметры на панели дополнительных сведений и операции управления отображаются в зависимости от типа выбранного SIES-узла.

Выполнение большинства операций управления по запросу администратора завершается созданием задачи управления (на стр. 148), которую ViPNet SIES MC помещает в очередь. Очередь задач создается для управления каждым SIES-узлом, зарегистрированным в ViPNet SIES MC.

В зависимости от выполняемой операции управления в рамках каждой задачи ViPNet SIES MC готовит одну или несколько команд в защищенных конвертах (см. глоссарий, стр. 161) для последующей доставки SIES-узлу в выбранном режиме управления (на стр. 32).

Если в режиме удаленного управления максимальное время ожидания ответа SIES-узла на команду ViPNet SIES MC превышено, команда автоматически отменяется ViPNet SIES MC.

Контролировать исполнение каждой команды SIES-узлом можно на панели дополнительных свойств, перейдя на вкладку **Задачи**.

Добавление SIES-узла в ViPNet SIES MC

Чтобы задать параметры криптографической обработки данных защищаемого устройства, добавьте SIES-узел в ViPNet SIES MC, используя идентификатор SIES-узла (см. глоссарий, стр. 161):

- В качестве идентификатора ViPNet SIES Core используется уникальный серийный номер, присваиваемый изготовителем и состоящий из 12 цифр. Серийный номер указывается на ViPNet SIES Core и вносится изготовителем в память ViPNet SIES Core.
- В качестве идентификатора ViPNet SIES Unit используется уникальная последовательность из 12 символов, указанная в поле `Subject.CN` запроса на служебный сертификат, созданного ViPNet SIES Unit.

Если вы планируете локально управлять добавленным ViPNet SIES Core или ViPNet SIES Unit, после добавления ViPNet SIES Core или ViPNet SIES Unit в ViPNet SIES MC смените режим управления SIES-узлом (на стр. 32). Подробнее о режимах управления SIES-узлами см. документ «ViPNet SIES. Сценарии эксплуатации».

Примечание. Управлять ViPNet PKI Client SIES Unit из ViPNet SIES MC можно только удаленно.

Таблица 4. Способы добавления SIES-узлов в ViPNet SIES MC

Способ добавления	ViPNet SIES Core	ViPNet SIES Unit	Пользователь	Другой
Автоматически при инициализации (см. глоссарий, стр. 161) с помощью ViPNet SIES Workstation	+	+	—	—
Вручную	+	—	+	+
По списку идентификаторов из файла	+	—	—	—
По запросу на служебный сертификат	—	+	—	—

Добавление ViPNet SIES Core

ViPNet SIES Core автоматически добавляется в ViPNet SIES MC при инициализации с помощью ViPNet SIES Workstation. Вы можете добавить ViPNet SIES Core самостоятельно, например, в ходе регистрации в ViPNet SIES MC структуры индустриальной системы.

Чтобы добавить ViPNet SIES Core в ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Щелкните ссылку **Добавить** > **SIES-узлы** > **ViPNet SIES Core**.

4 Введите идентификатор (см. глоссарий, стр. 161) добавляемого SIES-узла и нажмите кнопку **Далее**.

5 Вы можете ввести наименование и описание SIES-узла. По умолчанию ViPNet SIES MC автоматически задаст в качестве наименования идентификатор добавляемого SIES-узла.

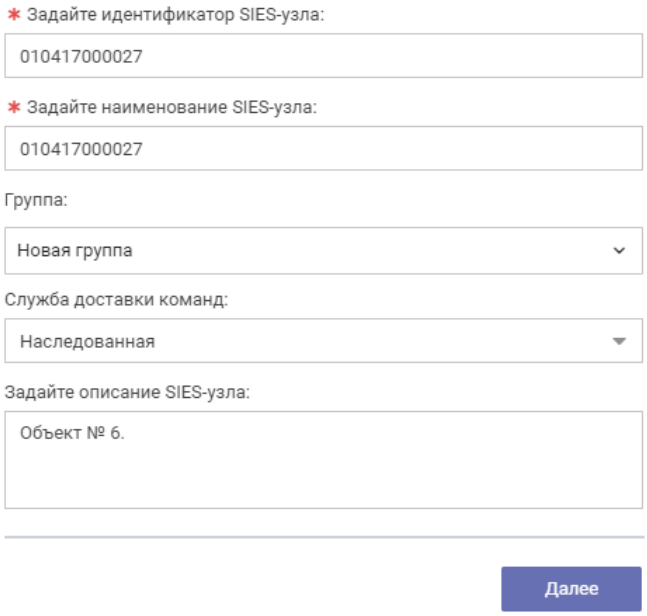

Рисунок 1. Задание атрибутов SIES-узла

В списке **Группа** выберите группу ViPNet SIES MC, в которую следует поместить добавляемый SIES-узел. Если группа не выбрана, SIES-узел будет добавлен в группу **Нераспределенные элементы** (на стр. 128). Вы сможете переместить SIES-узел в нужную группу позднее.

Настройки службы доставки защищенных конвертов ViPNet SIES MC для добавляемого SIES-узла наследуются от группы, в которую помещается SIES-узел. Если для SIES-узла нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

Нажмите кнопку **Далее**.

6 Убедитесь в корректности заданных значений и нажмите кнопку **Добавить**.

7 Ознакомьтесь с отчетом о добавленном SIES-узле и нажмите кнопку **Закрыть**.

Добавление ViPNet SIES Core по списку

Чтобы упростить добавление в ViPNet SIES MC большого числа ViPNet SIES Core, воспользуйтесь возможностью добавления SIES-узлов по списку идентификаторов из файла.

Чтобы добавить в ViPNet SIES MC одновременно несколько SIES-узлов:

1 Подготовьте TXT-файл со списком идентификаторов SIES-узлов, указав в каждой строке файла по одному идентификатору. Файл может содержать идентификаторы SIES-узлов только одного типа.

Внимание! Размер TXT-файла со списком идентификаторов SIES-узлов ограничен 40000 байт (39 Кбайт), что соответствует примерно 2850 идентификаторам SIES-узлов.

---

2 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

3 Перейдите в раздел **SIES-узлы** .

4 Щелкните ссылку **Добавить** > **SIES-узлы** > **ViPNet SIES Core по идентификаторам из файла**.

5 Выберите TXT-файл со списком идентификаторов SIES-узлов на жестком диске вашего компьютера или на внешнем носителе и нажмите кнопку **Далее**.

6 Отобразится список идентификаторов SIES-узлов, загружаемых в ViPNet SIES MC.

В списке **Группа** выберите группу ViPNet SIES MC, в которую следует поместить добавляемые SIES-узлы. Если группа не выбрана, SIES-узлы будут добавлены в группу **Нераспределенные элементы** (на стр. 128). Вы сможете переместить SIES-узлы в нужную группу позднее.

Настройки службы доставки защищенных конвертов ViPNet SIES MC для добавляемых SIES-узлов наследуются от группы, в которую помещаются SIES-узлы. Если для SIES-узлов нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

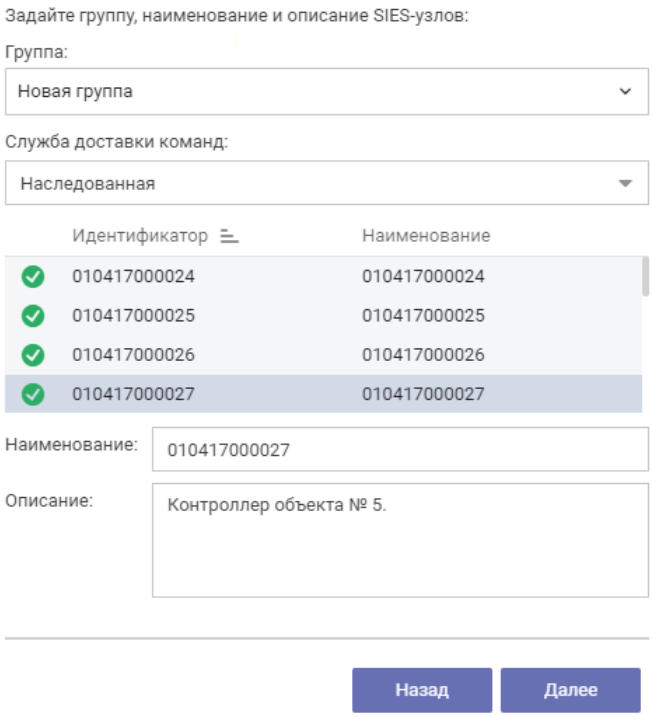

Рисунок 2. Добавление списка SIES-узлов

Также вы можете ввести наименование и описание добавляемых SIES-узлов, щелкнув по идентификатору. По умолчанию ViPNet SIES MC автоматически задаст в качестве наименования идентификатор каждого добавляемого SIES-узла.

Нажмите кнопку **Далее**.

7 Нажмите кнопку **Добавить**.

8 Ознакомьтесь с отчетом о добавленных SIES-узлах и нажмите кнопку **Закрыть**.

Добавление ViPNet SIES Unit по запросу на служебный сертификат

ViPNet SIES Unit автоматически добавляется в ViPNet SIES MC при инициализации с помощью ViPNet SIES Workstation. Вы можете добавить ViPNet SIES Unit по запросу на служебный сертификат в ходе ручной инициализации.

Чтобы добавить ViPNet SIES Unit по запросу на служебный сертификат:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Щелкните ссылку **Добавить** > **SIES-узлы** > **ViPNet SIES Unit по запросу на сертификат**.

4 Выберите файл с запросом на служебный сертификат SIES-узла на жестком диске вашего компьютера или на внешнем носителе и нажмите кнопку **Далее**.

5 Отобразится идентификатор SIES-узла, добавляемого в ViPNet SIES MC.

В списке **Группа** выберите группу ViPNet SIES MC, в которую следует поместить добавляемый SIES-узел. Если группа не выбрана, SIES-узел будет добавлен в группу **Нераспределенные элементы** (на стр. 128). Вы сможете переместить SIES-узел в нужную группу позднее.

Настройки службы доставки защищенных конвертов ViPNet SIES MC для добавляемого SIES-узла наследуются от группы, в которую помещается SIES-узел. Если для SIES-узла нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

Также вы можете ввести наименование и описание добавляемого SIES-узла, щелкнув по идентификатору. По умолчанию ViPNet SIES MC автоматически задаст в качестве наименования идентификатор добавляемого SIES-узла.

Нажмите кнопку **Далее**.

6 Нажмите кнопку **Добавить**.

7 Ознакомьтесь с отчетом о добавленном SIES-узле и нажмите кнопку **Закрыть**.

Добавление пользователя защищаемого устройства

Если реализуемый сценарий защиты данных предполагает участие пользователя защищаемого устройства индустриальной системы, добавьте пользователя в ViPNet SIES MC.

Чтобы добавить пользователя защищаемого устройства в ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Щелкните ссылку **Добавить** > **SIES-узлы** > **Пользователь**.

4 Идентификатор SIES-узла для пользователя защищаемого устройства создается автоматически. Вы можете изменить идентификатор.

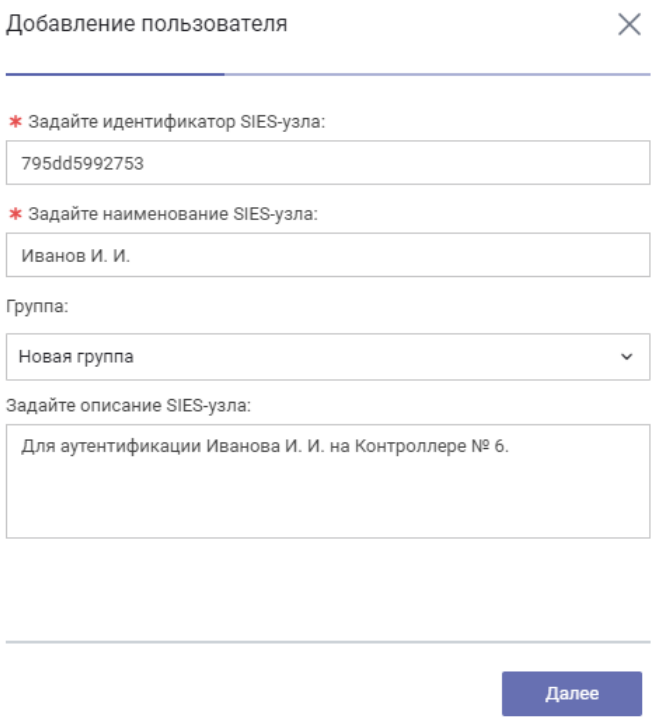

Рисунок 3. Задание атрибутов пользователя

Вы можете ввести наименование и описание SIES-узла. По умолчанию ViPNet SIES MC автоматически задаст в качестве наименования идентификатор добавляемого SIES-узла.

В списке **Группа** выберите группу ViPNet SIES MC, в которую следует поместить добавляемого пользователя. Если группа не выбрана, пользователь будет добавлен в группу **Нераспределенные элементы** (на стр. 128). Вы сможете переместить пользователя в нужную группу позднее.

Нажмите кнопку **Далее**.

5 Убедитесь в корректности заданных значений и нажмите кнопку **Добавить**.

6 Ознакомьтесь с отчетом о добавленном SIES-узле и нажмите кнопку **Закрыть**.

Для реализации сценария аутентификации пользователя на защищаемом устройстве, настройте прикладную ключевую подсистему для пользователя (на стр. 37).

Добавление другого SIES-узла

Другой SIES-узел — это устройство или ПО, выполняющее криптографические операции по запросам защищаемого устройства с использованием ключевой информации (см. глоссарий, стр. 162) ViPNet SIES, но не входящее в состав комплекса ViPNet SIES. Например, криптографические библиотеки стороннего производителя.

Чтобы добавить другой SIES-узел в ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Щелкните ссылку **Добавить** > **SIES-узлы** > **Другой SIES-узел**.

4 Вы можете ввести наименование и описание SIES-узла. По умолчанию ViPNet SIES MC автоматически задаст в качестве наименования идентификатор добавляемого SIES-узла.

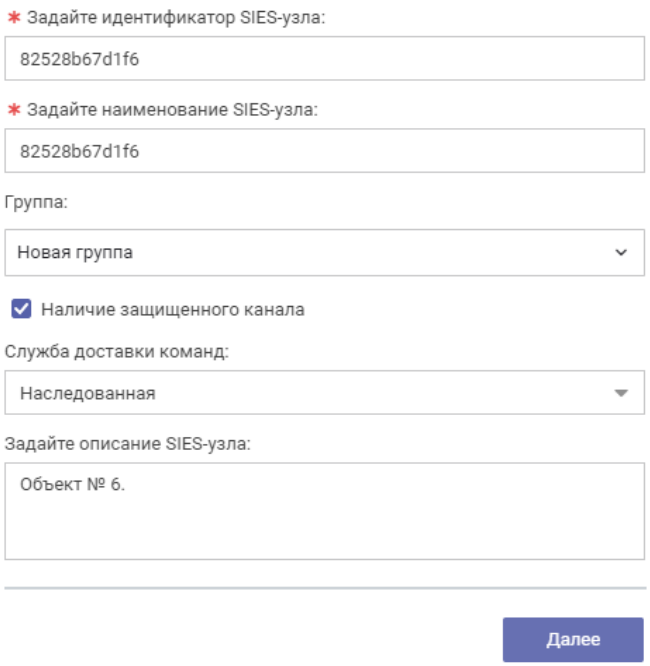

Рисунок 4. Изменение атрибутов SIES-узла

В списке **Группа** выберите группу ViPNet SIES MC, в которую следует поместить добавляемый SIES-узел. Если группа не выбрана, SIES-узел будут добавлен в группу **Нераспределенные элементы**. Вы сможете переместить SIES-узел в нужную группу позднее.

Если защищаемое устройство поддерживает удаленное управление SIES-узлом из ViPNet SIES MC, установите флажок **Наличие защищенного канала**. После этого вы сможете выбрать службу доставки защищенных конвертов ViPNet SIES MC.

Настройки службы доставки защищенных конвертов ViPNet SIES MC для добавляемого SIES-узла наследуются от группы, в которую помещается SIES-узел. Если для SIES-узла нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

Нажмите кнопку **Далее**.

5 Убедитесь в корректности заданных значений и нажмите кнопку **Добавить**.

6 Ознакомьтесь с отчетом о добавленном SIES-узле и нажмите кнопку **Закрыть**.

Завершение инициализации SIES-узла

После ручной инициализации SIES-узла (см. глоссарий, стр. 161) подтвердите в ViPNet SIES MC готовность SIES-узла к дальнейшему удаленному управлению из ViPNet SIES MC.

Область применения

- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений нажмите **Управление** > **Инициализация** > **Завершить инициализацию**.

Для ViPNet SIES Unit будет экспортирован инициализирующий архив с именем `sies_initialization_ГГГГММДДТЧЧММССZ.tar.gz`. Здесь:

- `ГГГГММДДТЧЧММСС` — метка с временем выгрузки архива в UTC-кодировке;
- `T` — разделитель даты и времени;
- `Z` — флаг UTC-кодировки метки времени.

Архив содержит защищенные конверты ViPNet SIES MC для завершения инициализации ViPNet SIES Unit на защищаемом устройстве. Сохраните архив на USB-носителе для последующей передачи администратору ViPNet SIES Unit.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Отмена инициализации SIES-узла

Вы можете отменить инициализацию SIES-узла в ViPNet SIES MC для:

- повторной инициализации SIES-узла в случае истечения срока действия сертификатов, переданных администратору защищаемого устройства, взаимодействующего с SIES-узлом;
- повторной инициализации ViPNet SIES Unit после приведения к заводскому состоянию администратором ViPNet SIES Unit;
- повторного завершения инициализации ViPNet SIES Unit в случае утраты или повреждения инициализирующего архива.

Внимание! Отменив инициализацию, вы не сможете управлять SIES-узлом из ViPNet SIES MC.

Область применения

- ViPNet SIES Unit;
- Другой SIES-узел.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений нажмите **Управление** > **Инициализация** > **Отменить инициализацию**.

Повторное завершение инициализации SIES-узла

После отмены инициализации SIES-узла вы можете снова завершить инициализацию SIES-узла.

Область применения

- ViPNet SIES Unit;
- Другой SIES-узел.

Порядок действий

1. Получите от администратора SIES-узла запрос на новый служебный сертификат SIES-узла.
2. Импортируйте запрос на служебный сертификат (на стр. 46) для существующего SIES-узла.
3. Завершите инициализацию SIES-узла (на стр. 23).

Просмотр сведений о SIES-узле

Вы можете просматривать сведения о SIES-узлах, зарегистрированных в ViPNet SIES MC, например, чтобы проверить текущее состояние SIES-узла.

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.

2 На панели навигации перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

Совет. Чтобы ускорить выбор нужного SIES-узла из большого числа зарегистрированных SIES-узлов, предварительно воспользуйтесь поиском или фильтром на панели инструментов страницы. Строку поиска и параметры фильтра можно сочетать.

Цвет значков SIES-узлов зависит от общего состояния SIES-узлов.

Таблица 5. Общие состояния SIES-узла

Значок	Наименование состояния	Описание состояния
	Нормальное	SIES-узел настроен и функционирует штатным образом.
	Скомпрометирован	В ViPNet SIES MC зафиксирован факт компрометации SIES-узла.
	Готов к восстановлению после компрометации	Завершен процесс компрометации SIES-узла в ViPNet SIES MC. Можно приступать к восстановлению работоспособности SIES-узла после компрометации. Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».
	Прикладная ключевая подсистема не настроена	Инициализация SIES-узла завершена. Прикладная ключевая подсистема SIES-узла не настроена.
	Есть проблемы	SIES-узел в опасном состоянии, но немедленного вмешательства не требуется. Возможно, истек срок действия первичной ключевой информации. В ближайшее время без вмешательства администратора работоспособность SIES-узла нарушится.

Значок	Наименование состояния	Описание состояния
	Критическое	Выявлены серьезные проблемы, требующие немедленного вмешательства. Работоспособность SIES-узла нарушена. Возможно, истекли сроки действия сертификатов одной из ключевых подсистем или первичной ключевой информации SIES-узла.
	Исключен из управления	Состояние SIES-узла не контролируется в ViPNet SIES MC.
	Не настроен	SIES-узел добавлен в ViPNet SIES MC. Требуется инициализация SIES-узла.

4 На панели дополнительных сведений просмотрите параметры выбранного SIES-узла.

Подробнее о параметрах см. Параметры SIES-узла (на стр. 143).

Текущее состояние SIES-узла отображается по информации, хранящейся в ViPNet SIES MC. Чтобы обновить в ViPNet SIES MC информацию о состоянии SIES-узла, на вкладке **Общее** нажмите **Управление** > **Получить состояние**.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Изменение атрибутов SIES-узла

В ходе эксплуатации компонентов комплекса ViPNet SIES, развернутых в индустриальной системе, для удобства управления вы можете изменять следующие атрибуты SIES-узла:

- **Идентификатор** — уникальное обозначение SIES-узла, присваиваемое изготовителем. Длина значения — 12 символов (можно использовать цифры и буквы латинского алфавита, а также символ «–»; символ «пробел» и специальные символы использовать нельзя).

Внимание! Если при добавлении ViPNet SIES Core, ViPNet SIES Unit или другого SIES-узла вы ошиблись в значении идентификатора, вы можете изменить идентификатор в ViPNet SIES MC только до инициализации SIES-узла. Иначе вам придется удалить SIES-узел и добавить заново.

- **Наименование** — уникальное обозначение SIES-узла. Длина значения — до 64 символов.

  Вы можете использовать любое наименование, которое облегчит вам идентификацию SIES-узла в ViPNet SIES MC. Наименование SIES-узла, например, используется при идентификации прикладных связей (на стр. 49) между SIES-узлами.

- **Описание** — неуникальный комментарий о SIES-узле. Длина значения — до 256 символов.

  Вы можете оставить любую дополнительную информацию.

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений нажмите кнопку .

5 Укажите новые атрибуты SIES-узла.

Если для SIES-узла нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

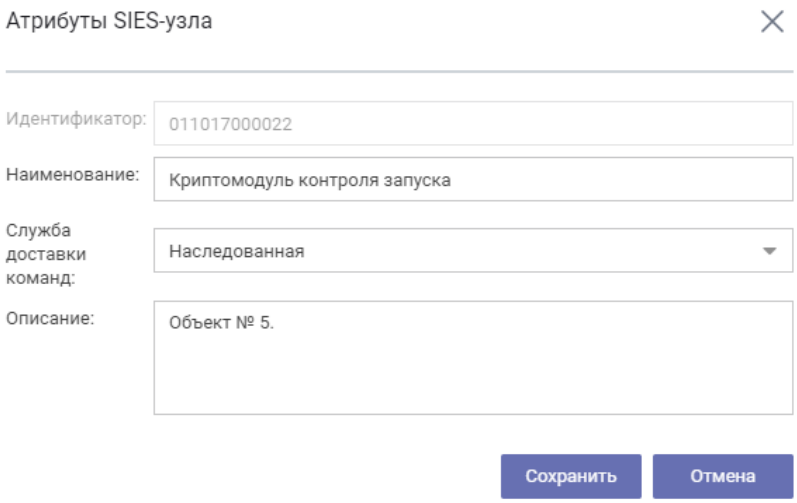

Рисунок 5. Окно изменения атрибутов SIES-узла

6 Нажмите кнопку **Сохранить**.

Смена режима работы SIES-узла

Вы можете принудительно сменить текущий режим работы SIES-узла в следующих случаях:

- регламентное обслуживание SIES-узла в ходе регламентного обслуживания защищаемого устройства — смените режим работы на **Конфигурирование**;
- криптографическая обработка в реализованных сценариях защиты данных защищаемого устройства — смените режим работы на **Штатный**;
- блокирование работы SIES-узла перед регламентным обслуживанием защищаемого устройства — смените режим работы на **Блокировка**.

Внимание! Для ViPNet SIES Core перед первой сменой режима работы на режим «Штатный» по завершении инициализации задайте связь ViPNet SIES Core с защищаемым устройством (на стр. 70).

Область применения

- ViPNet SIES Core (подробнее о режимах работы см. документ «ViPNet SIES Core. Общее описание»);
- ViPNet SIES Unit (подробнее о режимах работы см. документ «ViPNet SIES Unit. Руководство администратора»);
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Таблица 6. Поддерживаемые переходы между режимами работы по типам SIES-узлов

Текущий режим работы	Целевой режим работы	ViPNet SIES Core	ViPNet SIES Unit	Другой SIES-узел
«Начальная загрузка»	«Конфигурирование»	+	—	—
«Инициализация»	«Конфигурирование»	+	—	—
«Конфигурирование»	«Инициализация»	+	—	—
«Конфигурирование»	«Штатный»	+	+	—
«Штатный»	«Конфигурирование»	+	+	—
«Штатный»	«Инициализация»	+	—	—
«Блокировка»	«Конфигурирование»	+	—	—
«Блокировка»	«Штатный»	—	—	+
«Штатный»	«Блокировка»	+	—	+

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Общее**.

5 Нажмите **Управление** > **Сменить режим работы** и в меню выберите новый режим работы SIES-узла.

Примечание. Если ViPNet SIES Core перешел в режим **Блокировка**, для дальнейшей настройки и работы с ViPNet SIES Core смените режим **Блокировка** на режим **Конфигурирование**.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Смена режима управления SIES-узлом

ViPNet SIES MC позволяет вам управлять SIES-узлом в одном из двух режимов:

- удаленном, в котором команды управления (см. глоссарий, стр. 162) и мониторинга (см. глоссарий, стр. 162) доставляются SIES-узлу через защищаемое устройство по каналам связи индустриальной системы (режим включен по умолчанию);
- локальном, в котором команды управления и мониторинга доставляются SIES-узлу через ViPNet SIES Workstation без использования каналов связи индустриальной системы (подробнее о трансляции команд с помощью ViPNet SIES Workstation см. документ «ViPNet SIES Workstation. Руководство по эксплуатации»).

Примечание. Режим удаленного управления SIES-узлом вы можете использовать только при наличии взаимодействия между ViPNet SIES MC и транспортным уровнем индустриальной системы. Подробнее об организации работы ViPNet SIES MC см. документ «ViPNet SIES MC. Общее описание». Для режима **Удаленное** задайте (на стр. 97) **Адрес для служебных сообщений** защищаемого устройства.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Примечание. С помощью ViPNet SIES Workstation вы можете локально управлять только ViPNet SIES Core и ViPNet SIES Unit.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Общее** и нажмите **Управление** > **Режим управления**.

5 В меню выберите новый режим управления SIES-узлом.

6 Подтвердите выбор нового режима, нажав кнопку **Сменить**.

Локальное управление SIES-узлом: порядок действий

Вы можете организовать отправку защищенных конвертов ViPNet SIES MC с командами управления на ViPNet SIES Core или ViPNet SIES Unit без использования каналов связи индустриальной системы. Это можно сделать с помощью ViPNet SIES Workstation в режиме локального управления SIES-узлом.

Подробнее об организации управления см. документ «ViPNet SIES MC. Общее описание».

Чтобы отправить команды ViPNet SIES MC на ViPNet SIES Core или ViPNet SIES Unit через ViPNet SIES Workstation в режиме локального управления, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 7. Порядок локального управления SIES-узлом

	Действие	Ссылка
☐	Смените режим управления SIES-узлом на **Локальное**.	Смена режима управления SIES-узлом (на стр. 32).
☐	Подключите: • ViPNet SIES Core к ViPNet SIES Workstation; • ViPNet SIES Workstation к защищаемому устройству с установленным ViPNet SIES Unit.	См. ViPNet SIES Workstation. Руководство по эксплуатации.
☐	На ViPNet SIES Workstation запустите трансляцию команд ViPNet SIES MC на SIES-узел.	См. там же.
☐	В ViPNet SIES MC выполните намеченные операции по управлению SIES-узлом.	См. там же.
☐	На ViPNet SIES Workstation остановите трансляцию команд ViPNet SIES MC на SIES-узел.	См. там же.
☐	Отключите: • ViPNet SIES Core от ViPNet SIES Workstation; • ViPNet SIES Workstation от защищаемого устройства с установленным ViPNet SIES Unit.	См. там же.
☐	Если транслировать команды ViPNet SIES MC больше не требуется, смените режим управления SIES-узлом на **Удаленное**.	Смена режима управления SIES-узлом (на стр. 32).

Управление ключевой системой SIES-узла

Ключевая система SIES-узла входит в состав ключевой системы ViPNet SIES. Ключевая система SIES-узла состоит из прикладной и служебной ключевых подсистем.

К прикладной ключевой подсистеме SIES-узла относится следующая ключевая информация:

- корневой сертификат прикладной ключевой подсистемы ViPNet SIES;
- прикладной сертификат SIES-узла;
- информация о прикладных связях защищаемого устройства.

Прикладная ключевая подсистема создается в ходе организации защищенного взаимодействия между SIES-узлами при реализации сценариев защиты данных.

К служебной ключевой подсистеме SIES-узла относится следующая ключевая информация:

- служебный сертификат SIES-узла;
- служебный сертификат ViPNet SIES MC.

Служебная ключевая подсистема создается в ходе инициализации при вводе SIES-узла в эксплуатацию.

Подробнее о ключевых подсистемах см. документ «ViPNet SIES MC. Общее описание».

Таблица 8. Задачи управления ключевыми системами SIES-узлов

SIES-узел	Служебная ключевая подсистема	Прикладная ключевая подсистема
ViPNet SIES Core	• Создается автоматически с помощью ViPNet SIES Workstation при инициализации SIES-узла. См. ViPNet SIES. Сценарии эксплуатации > Эксплуатация ViPNet SIES Core > Ввод в эксплуатацию ViPNet SIES Core. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление служебной ключевой информации.	• Создается администратором ViPNet SIES MC в зависимости от реализуемого сценария защиты данных защищаемого устройства. См. ViPNet SIES. Сценарии работы. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление прикладной ключевой информации.
ViPNet SIES Unit	• Создается автоматически с помощью ViPNet SIES Workstation или вручную (на стр. 88) администратором ViPNet SIES Unit и администратором ViPNet SIES MC при инициализации SIES-узла. См. ViPNet SIES. Сценарии эксплуатации	• Создается администратором ViPNet SIES MC в зависимости от реализуемого сценария защиты данных защищаемого устройства. См. ViPNet SIES. Сценарии работы.

SIES-узел	Служебная ключевая подсистема	Прикладная ключевая подсистема
	> Эксплуатация ViPNet SIES Unit > Ввод в эксплуатацию ViPNet SIES Unit. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление служебной ключевой информации.	• Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление прикладной ключевой информации.
Пользователь	Отсутствует.	• Создается администратором ViPNet SIES MC в зависимости от реализуемого сценария защиты данных защищаемого устройства. См. ViPNet SIES. Сценарии работы. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление прикладной ключевой информации.
Другой	• Создается вручную администратором ViPNet SIES MC и администратором SIES-узла при вводе в эксплуатацию SIES-узла. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление служебной ключевой информации.	• Создается администратором ViPNet SIES MC в зависимости от реализуемого сценария защиты данных защищаемого устройства. См. ViPNet SIES. Сценарии работы. • Обновляется администратором ViPNet SIES MC 1 раз каждые 12 месяцев. См. ViPNet SIES. Сценарии эксплуатации > Регламентное обслуживание комплекса ViPNet SIES > Регламентное обновление прикладной ключевой информации.

Настройка прикладной ключевой подсистемы для использования сертификатов: порядок действий

Если в сценариях защиты данных защищаемого устройства используются сертификаты (например, в обмене зашифрованными данными с проверкой электронной подписи), настройте прикладную ключевую подсистему SIES-узла. Подробнее о сценариях защиты данных см. документ «ViPNet SIES. Сценарии работы».

Область применения

Все типы SIES-узлов.

Чтобы настроить прикладную ключевую подсистему SIES-узла для использования сертификатов, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 9. Порядок настройки прикладной ключевой подсистемы SIES-узла

	Действие	Ссылка
☐	Если в ViPNet SIES MC нет действующего корневого сертификата прикладной ключевой подсистемы ViPNet SIES, создайте сертификат.	См. ViPNet SIES MC. Установка и обслуживание.
☐	Если ключевая подсистема настраивается на SIES-узле типа **ViPNet SIES Unit** или типа **Другой**, загрузите на SIES-узел корневой сертификат прикладной ключевой подсистемы ViPNet SIES (см. глоссарий, стр. 162), который удостоверяет прикладной сертификат SIES-узла.	Загрузка сертификата на SIES-узел (на стр. 42).
☐	Создайте прикладной сертификат SIES-узла.	Создание и загрузка сертификата на SIES-узел (на стр. 41).
☐	Добавьте прикладные связи между защищаемыми устройствами с назначением **Шифрование и проверка электронной подписи**.	Добавление связи (на стр. 106).
☐	Синхронизируйте связи на всех взаимодействующих SIES-узлах в течение 45 суток с момента создания прикладного сертификата.	Синхронизация прикладных связей (на стр. 51). Если ключевая подсистема настраивается на SIES-узле типа **Другой**, взаимодействующем с защищаемым устройством, которое не поддерживает удаленного управления SIES-узлом из ViPNet SIES MC, экспортируйте (на стр. 47) и загрузите прикладной сертификат на SIES-узел.

Настройка прикладной ключевой подсистемы для поддержки аутентификации пользователя защищаемого устройства: порядок действий

С помощью ViPNet SIES Core защищаемое устройство может аутентифицировать пользователя, используя криптопровайдер, установленный на персональном ключевом носителе пользователя.

Для этого добавьте пользователя защищаемого устройства в ViPNet SIES MC (на стр. 20), предварительно получив от пользователя запрос на прикладной сертификат.

Запрос должен соответствовать требованиям к прикладным сертификатам SIES-узлов. Подробнее см. документ «ViPNet SIES MC. Общее описание».

Чтобы настроить прикладную ключевую подсистему для пользователя защищаемого устройства, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 10. Порядок настройки прикладной ключевой подсистемы для пользователя

	Действие	Ссылка
☐	Добавьте в ViPNet SIES MC защищаемое устройство.	См. Добавление защищаемого устройства (на стр. 93). Например, задайте следующие значения параметров: • **Наименование** — фамилия, имя и отчество пользователя; • **Адрес** — табельный номер или страховой номер индивидуального лицевого счета (СНИЛС) или любое другое уникальное обозначение пользователя.
☐	Добавьте в ViPNet SIES MC пользователя защищаемого устройства как SIES-узел.	Добавление пользователя защищаемого устройства (на стр. 20).
☐	Назначьте пользователя на защищаемое устройство.	Назначение SIES-узла на защищаемое устройство (на стр. 98).
☐	Импортируйте запрос на прикладной сертификат пользователя защищаемого устройства.	Импорт запроса на сертификат (на стр. 46).
☐	Прикладной сертификат, изданный ViPNet SIES MC для добавленного пользователя, выгрузите на внешний носитель и передайте пользователю защищаемого устройства для загрузки в хранилище персонального ключевого носителя. Шаг можно пропустить, если для аутентификации будет использоваться упрощенный формат.	• Экспорт сертификата (на стр. 47). • См. ViPNet SIES Core SDK. Общее описание.
☐	Добавьте прикладную парную связь между защищаемым устройством пользователя и теми защищаемыми устройствами, на которых предстоит аутентифицироваться пользователю.	См. Добавление парной связи для защищаемого устройства (на стр. 106). Выберите назначение **Шифрование и проверка электронной подписи**. Для аутентификации пользователя на защищаемых устройствах, входящих в резервированную группу (на стр. 163), добавьте резервированную парную связь (на стр. 111) между защищаемым устройством пользователя и резервированной группой (на стр. 163).
☐	Настройте прикладную ключевую подсистему на тех ViPNet SIES Core и ViPNet SIES Unit, с защищаемыми устройствами которых связано защищаемое устройство пользователя.	Настройка прикладной ключевой подсистемы для использования сертификатов: порядок действий (на стр. 36).

	Действие	Ссылка
☐	Синхронизируйте прикладные связи на SIES-узлах тех защищаемых устройств, на которых предстоит аутентифицироваться пользователю. Связи нужно синхронизировать в течение 45 суток с момента создания прикладного сертификата.	Синхронизация прикладных связей (на стр. 51).

Просмотр сведений о сертификатах SIES-узла

Вы можете просматривать сведения о сертификатах SIES-узла, например, чтобы проверить сроки действия сертификатов.

Область применения

Все типы SIES-узлов.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи** и щелкните список с наименованием целевой ключевой подсистемы SIES-узла.

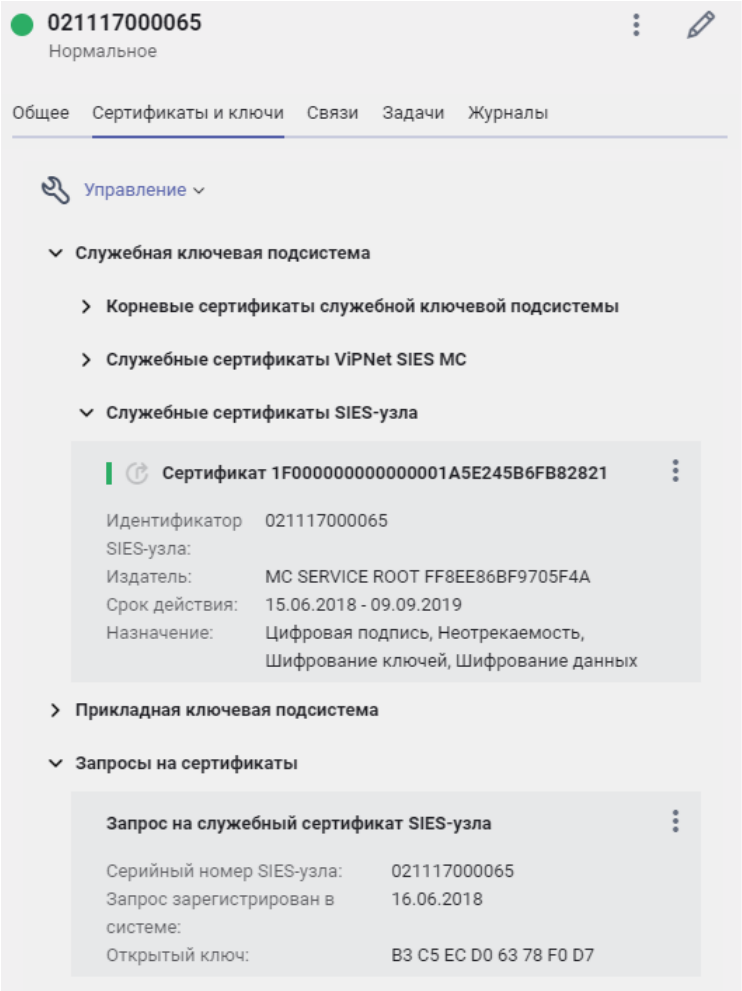

Рисунок 6. Сертификаты ключевой системы SIES-узла

5 В раскрывшемся списке щелкните наименование типа целевого сертификата.

6 В раскрывшемся списке щелкните интересующий вас сертификат и просмотрите атрибуты сертификата.

Сертификаты помечаются следующими значками:

— сертификат действителен (см. глоссарий, стр. 160);

— срок действия сертификата истекает;

— срок действия сертификата истек.

Если срок действия сертификата истекает или истек, вам следует выпустить новый сертификат.

Если истекает или истек срок действия корневого сертификата ключевой подсистемы, в первую очередь вам будет предложено выпустить соответствующий новый корневой сертификат. Подробнее о выпуске корневых сертификатов см. документ «ViPNet SIES MC. Установка и обслуживание».

Создание и загрузка сертификата на SIES-узел

В ходе эксплуатации SIES-узла вам может понадобиться издать и загрузить сертификат на SIES-узел, например, для смены текущего сертификата с истекающим сроком действия. Срок действия сертификата вы можете проверить, просмотрев атрибуты сертификата (на стр. 39).

Новый сертификат SIES-узла создавайте и загружайте до истечения срока действия соответствующего текущего сертификата SIES-узла.

Примечание. Не рекомендуется чаще одного раза в сутки создавать и загружать служебный сертификат на ViPNet SIES Core версии 2.0.2 и выше.

Вы можете создать и загрузить на SIES-узел следующие сертификаты:

- для управления SIES-узлом из ViPNet SIES MC — служебный сертификат SIES-узла.
- для реализации сценариев защиты данных с помощью SIES-узла — прикладной сертификат SIES-узла.

Прикладной сертификат SIES-узла вам следует создавать после инициализации SIES-узла, если в сценариях защиты данных защищаемого устройства используются прикладные связи с назначением **Шифрование и проверка электронной подписи.** Подробнее о сценариях защиты данных см. документ «ViPNet SIES. Сценарии работы».

Служебный сертификат SIES-узла вам следует создавать при истекающем сроке действия служебного сертификата SIES-узла.

Подробнее о видах сертификатов SIES-узла см. документ «ViPNet SIES MC. Общее описание».

Вы можете выполнить указанные действия по очередности или за одну операцию управления, порядок действий по которой приведен ниже.

Область применения

- ViPNet SIES Core;

  Внимание! Перед созданием и загрузкой прикладного сертификата на ViPNet SIES Unit или на SIES-узел типа **Другой**, загрузите на него корневой сертификат прикладной ключевой подсистемы (на стр. 42).

- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи**.

5 На панели дополнительных сведений нажмите **Управление** > **Создать и загрузить сертификат**.

6 В меню выберите тип обновляемого сертификата — **Прикладной** или **Служебный**.

7 Нажмите кнопку **Да**.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Загрузка сертификата на SIES-узел

В ходе эксплуатации SIES-узла вам может понадобиться загрузить сертификат на SIES-узел, например, корневой сертификат прикладной ключевой подсистемы ViPNet SIES на ViPNet SIES Unit.

Вы можете загружать на SIES-узел следующие сертификаты:

- для управления SIES-узлом из ViPNet SIES MC:
  - служебный сертификат ViPNet SIES MC;
  - служебный сертификат SIES-узла.
- для реализации сценариев защиты данных с помощью SIES-узла:
  - корневой сертификат прикладной ключевой подсистемы ViPNet SIES (на ViPNet SIES Core не загружается);
  - прикладной сертификат SIES-узла.

Внимание! Вы не можете загрузить на SIES-узел один и тот же сертификат дважды.

Область применения

- ViPNet SIES Core;

Внимание! Перед загрузкой прикладного сертификата на ViPNet SIES Unit или на SIES-узел типа **Другой**, загрузите на него корневой сертификат прикладной ключевой подсистемы (на стр. 42).

- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи** и щелкните список с наименованием целевой ключевой подсистемы SIES-узла.

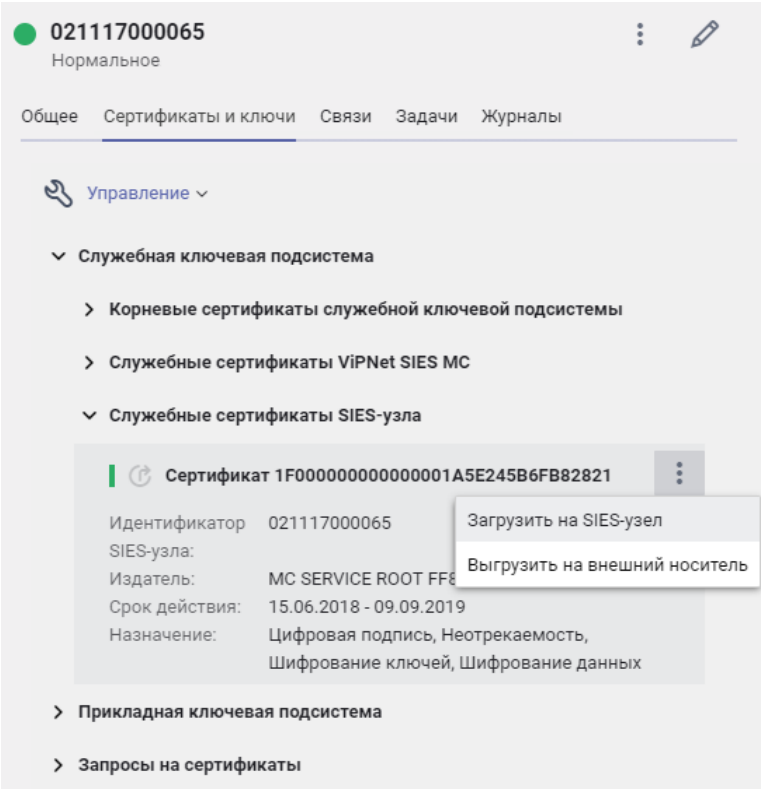

Рисунок 7. Загрузка сертификата в ViPNet SIES Core

5 В раскрывшемся списке щелкните наименование типа целевого сертификата. Раскроется список сертификатов ключевой подсистемы SIES-узла.

Значок означает, что сертификат еще не загружен на SIES-узел.

Значок означает, что сертификат уже загружен на SIES-узел.

6 В списке справа от загружаемого сертификата нажмите кнопку и в меню выберите **Загрузить на SIES-узел**.

Получение списка сертификатов SIES-узла

Вы можете синхронизировать информацию о хранимых сертификатах между SIES-узлом и ViPNet SIES MC.

Область применения

ViPNet SIES Core.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи**.

5 На панели дополнительных сведений нажмите **Управление** > **Получить список сертификатов**.

В результате ViPNet SIES MC отправит SIES-узлу команду на получение списка сертификатов.

По результатам обработки ответа от SIES-узла в ViPNet SIES MC будет обновлена информация о сертификатах. Вы можете ознакомиться с актуальной информацией о сертификатах SIES-узла (на стр. 39).

Удаление сертификата из ViPNet SIES MC

Если сертификат SIES-узла еще не загружался на SIES-узел, вы можете удалить неиспользуемый прикладной или служебный сертификат SIES-узла из ViPNet SIES MC.

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи** и щелкните список с наименованием целевой ключевой подсистемы SIES-узла.

5 В раскрывшемся списке щелкните наименование типа целевого сертификата.

Значок означает, что сертификат еще не загружен на SIES-узел.

Значок означает, что сертификат уже загружен на SIES-узел и вы не можете удалить сертификат из ViPNet SIES MC.

6 В списке справа от незагруженного сертификата нажмите кнопку и в меню выберите **Удалить**.

7 В появившемся окне нажмите кнопку **Удалить**.

Удаление сертификата с SIES-узла

Для ликвидации прикладной ключевой подсистемы (например, если на SIES-узле больше не требуется криптографическая обработка данных в прикладных связях с назначением **Шифрование и проверка электронной подписи**) вы можете удалить прикладной сертификат SIES-узла.

Внимание! Если в сценариях защиты данных защищаемого устройства используются прикладные связи с назначением **Шифрование и проверка электронной подписи**, перед удалением прикладного сертификата с SIES-узла убедитесь в наличии хотя бы одного действительного прикладного сертификата на SIES-узле.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи** и щелкните список с наименованием целевой ключевой подсистемы SIES-узла.

5 В раскрывшемся списке щелкните наименование типа целевого сертификата. Раскроется список сертификатов ключевой подсистемы SIES-узла.

6 В списке справа от удаляемого сертификата нажмите кнопку и в меню выберите **Удалить с SIES-узла**.

7 В появившемся окне нажмите кнопку **Удалить**.

Примечание. При удалении прикладного или служебного сертификата с SIES-узла выбранный сертификат удаляется также из ViPNet SIES MC. Если удаленный прикладной сертификат SIES-узла использовался в прикладных связях с назначением **Шифрование и проверка электронной подписи**, синхронизируйте связи между SIES-узлами.

Импорт запроса на сертификат

С помощью ViPNet SIES MC вы можете в автоматическом режиме издать служебный или прикладной сертификат SIES-узла. Для этого импортируйте в ViPNet SIES MC запрос на сертификат. Запрос должен удовлетворять требованиям к сертификатам ViPNet SIES. Подробнее см. документ «ViPNet SIES MC. Общее описание».

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи**.

5 На панели дополнительных сведений нажмите **Управление** > **Загрузить запрос**.

6 В поле **Имя файла** выберите файл с запросом на сертификат на жестком диске вашего компьютера или на внешнем носителе.

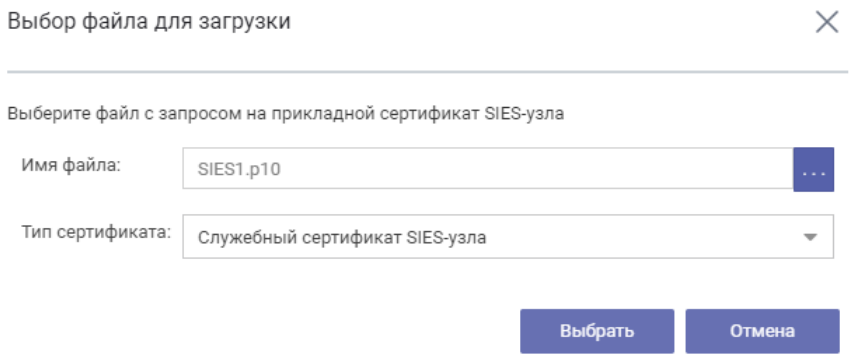

Рисунок 8. Выбор файла с запросом на сертификат

В списке **Тип сертификата** выберите элемент, указывающий на принадлежность добавляемого запроса на сертификат соответствующей ключевой подсистеме SIES-узла.

Нажмите кнопку **Выбрать**.

ViPNet SIES MC автоматически издаст сертификат SIES-узла. Сведения о добавленном запросе на сертификат SIES-узла и изданный сертификат SIES-узла вы можете просмотреть (на стр. 26) на вкладке **Сертификаты и ключи** панели дополнительных сведений.

Экспорт сертификата

Вы можете экспортировать сертификат из ViPNet SIES MC, например, для передачи администратору SIES-узла.

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи** и щелкните список с наименованием целевой ключевой подсистемы SIES-узла.

5 В раскрывшемся списке щелкните наименование типа целевого сертификата.

6 В раскрывшемся списке справа от интересующего вас сертификата нажмите кнопку .

7 В меню выберите пункт **Выгрузить на внешний носитель**.

8 Укажите место сохранения сертификата.

После подтверждения сертификат будет сохранен в файл `*.cer` (см. глоссарий, стр. 164).

Обновление инициализирующей последовательности SIES-узла

Инициализирующая последовательность (см. глоссарий, стр. 161) служит для выработки ключей SIES-узла и имеет ограниченный срок действия. ViPNet SIES MC заблаговременно уведомит вас о наступления срока обновления инициализирующей последовательности SIES-узлов, зарегистрированных в ViPNet SIES MC. Также с состоянием инициализирующей последовательности SIES-узла вы можете ознакомиться на вкладке **Общее** панели дополнительных сведений.

Внимание! После обновления инициализирующей последовательности на ViPNet SIES Core версии 2.1 или 2.0.2 синхронизируйте связи SIES-узла (на стр. 51).

Область применения

- ViPNet SIES Core (перед обновлением инициализирующей последовательности переведите ViPNet SIES Core в режим **Конфигурирование**);
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Сертификаты и ключи**.
5. На панели дополнительных сведений нажмите **Управление** > **Обновить первичную ключевую информацию**.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Управление прикладными связями SIES-узла

Информация о прикладных связях хранится на SIES-узлах, взаимодействующих с защищаемыми устройствами, между которыми добавлены прикладные связи. (на стр. 104)

Для выполнения сценариев защиты данных назначения прикладных связей и ключевую информацию между связанными защищаемыми устройствами следует поддерживать в синхронизированном состоянии с помощью ViPNet SIES MC.

Синхронизация заключается в загрузке актуальной ключевой информации и параметров связи на взаимодействующие SIES-узлы. После синхронизации связанные защищаемые устройства могут взаимодействовать друг с другом защищенным образом в реализованных сценариях защиты данных индустриальной системы.

Просмотр прикладных связей

Вы можете просматривать связи выбранного SIES-узла, например, чтобы проверить состояние синхронизации связей.

Область применения

Все типы SIES-узлов.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Связи**.

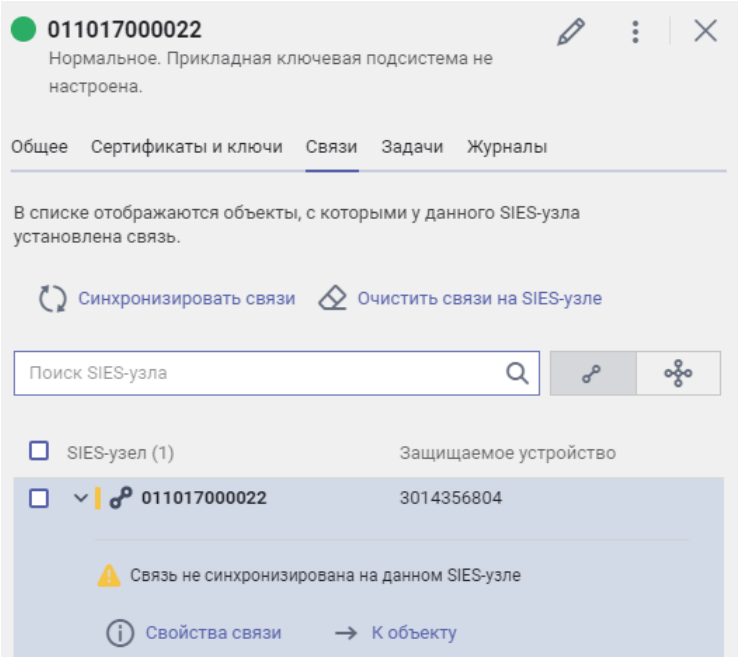

Рисунок 9. Заданные связи SIES-узла

5 Просмотрите прикладные связи, добавленные для SIES-узла.

С помощью кнопок вы можете переключать текущее представление списка связей между отображением парных или мультивещательных связей.

Общие состояния связей помечаются следующими цветами:

— все назначения связи в нормальном состоянии;

— хотя бы у одного назначения связи есть проблемы (например, изменилось назначение связи): следует выполнить синхронизацию связи для восстановления криптографической обработки данных на защищаемых устройствах);

— хотя бы одно назначение связи в критическом состоянии (например, истек срок действия связи): следует выполнить синхронизацию связи для восстановления криптографической обработки данных на защищаемых устройствах;

— состояние назначений связи не контролируется.

Чтобы просмотреть подробности текущего состояния связи с взаимодействующим SIES-узлом, в списке связей щелкните наименование SIES-узла, с которым задана связь.

Совет. При наличии связей с состоянием, отличным от нормального, убедитесь в том, что связи синхронизированы. Если в назначениях связей выбрано **Шифрование и проверка электронной подписи**, перед синхронизацией связей убедитесь в наличии в ViPNet SIES MC действительных прикладных сертификатов SIES-узлов.

---

6 На раскрывшейся панели свойств прикладной связи вы можете:

- просмотреть текущее состояние связи;
- просмотреть назначения связи, щелкнув **Свойства связи**;

- перейти к параметрам удаленного SIES-узла, щелкнув **К объекту**.

Синхронизация прикладных связей

Для возможности выполнения защищаемым устройством криптографических операций синхронизируйте прикладные связи между взаимодействующими SIES-узлами. Синхронизировать связи нужно, когда:

- добавлена новая связь между защищаемыми устройствами;
- изменен адрес одного из взаимодействующих защищаемых устройств;
- сменились ключи или сертификаты;
- истекает срок действия связи;
- изменены назначения связи;
- изменен состав участников мультивещательной связи (см. глоссарий, стр. 163);
- участникам мультивещательной связи делегировано или отозвано право отправки данных;
- изменен мультивещательный адрес (на стр. 163).

Перед синхронизацией связи задайте адреса взаимодействующих защищаемых устройств (на стр. 97).

Внимание! Если среди назначений связи вы выбрали **Шифрование и проверка электронной подписи**, перед синхронизацией связи выпустите прикладные сертификаты SIES-узлов.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Для SIES-узла типа **Пользователь** синхронизация связи не требуется.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

Примечание. Для синхронизации связей с назначениями **Вычисление и проверка имитовставки** и **Шифрование в режиме реального времени** требуется прикладной мастер-ключ ViPNet SIES (см. глоссарий, стр. 163). Создание прикладного мастер-ключа выполняется автоматически при первой синхронизации связей с указанными назначениями, но требует полномочий супер-администратора или администратора МС. Также мастер-ключ можно создать предварительно. Подробнее см. документ «ViPNet SIES МС. Установка и обслуживание».

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Нажмите кнопку **Синхронизировать связи**, которая будет доступна при наличии у SIES-узла связей, требующих синхронизации или удаления.

6 В списке связей щелкните наименование SIES-узла, с которым задана связь.

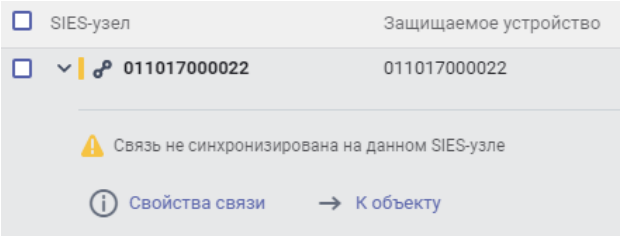

Рисунок 10. Состояние связи

7 На раскрывшейся панели свойств прикладной связи нажмите кнопку **К объекту**.

Совет. Чтобы синхронизировать связи одновременно на всех или нескольких SIES-узлах, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

8 Повторите действие 5, чтобы синхронизировать связь на взаимодействующем SIES-узле.

Примечание. Если после выполнения синхронизации остались связи с состоянием **Связь не синхронизирована на удаленном SIES-узле**, выполните синхронизацию связей на таких SIES-узлах или воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Удаление всех прикладных связей на SIES-узле

Вы можете удалить все прикладные связи на SIES-узле перед:

- использованием ViPNet SIES Core в другом защищаемом устройстве;

- временным выводом ViPNet SIES Core из эксплуатации;
- повторным добавлением связей между защищаемыми устройствами.

В результате также будут удалены соответствующие прикладные связи на взаимодействующих SIES-узлах.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Нажмите кнопку **Очистить связи на SIES-узле**.

6 Нажмите кнопку **Да**.

Для восстановления связей выполните синхронизацию (на стр. 51).

Отмена задачи управления

Вам может потребоваться отменить выполнение задач управления ViPNet SIES MC, сформированных в адрес SIES-узла, например, если вы отдали команды по ошибке. Вы можете отменить выполнение задач со следующими состояниями:

- ожидающих выполнения;
- выполняемых.

Отдельные операции управления ViPNet SIES MC могут включать в себя выполнение списка команд, поэтому команды объединяются в задачи. Подробнее о состояниях и очереди задач см. Задачи (на стр. 148).

Отмена задачи не гарантирует отмену уже выполненных команд по задаче на SIES-узле.

Отмена одной задачи

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Задачи**.
5. Щелкните выполняющуюся или ожидающую выполнения задачу, требующую отмены.
6. Нажмите кнопку **Отменить задачу**.

Отмена всех выполняющихся и ожидающих выполнения задач

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 На панели дополнительных сведений перейдите на вкладку **Задачи**.

5 Нажмите **Управление** > **Отменить все задачи**.

6 Нажмите кнопку **Да**.

Выгрузка защищенного конверта с командой для SIES-узла

Если ViPNet SIES MC не имеет связи с SIES-узлом для удаленной доставки защищенных конвертов, вы можете самостоятельно доставить защищенный конверт с командой управления ViPNet SIES MC на защищаемое устройство, с которым взаимодействует SIES-узел. Перед доставкой на защищаемое устройство предварительно выгрузите защищенный конверт из ViPNet SIES MC.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узел.

4 Выполните операцию управления SIES-узлом.

5 На панели дополнительных сведений перейдите на вкладку **Задачи** и нажмите **Управление** > **Выгрузить команду**.

В результате защищенный конверт ViPNet SIES MC для выбранного SIES-узла будет сохранен в архив с именем `sies_commands_ГГГГММДДТЧЧММССZ.tar.gz`. Здесь:

- `ГГГГММДДТЧЧММСС` — метка с временем выгрузки защищенного конверта;
- `T` — разделитель даты и времени.

Совет. Чтобы выгрузить защищенные конверты для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59). Выгружаемые защищенные конверты будут упакованы в архивы `*.tar.gz` объемом по 100 Мбайт.

Защищенный конверт помещается в архив в виде файла `sies_command_XXXXXXXXXXXX_ГГГГММДДТЧЧММССZ.bin`. Здесь:

- `XXXXXXXXXXXX` — идентификатор SIES-узла;

- `ГГГГММДДТЧЧММСС` — метка с временем выгрузки защищенного конверта;
- `Т` — разделитель даты и времени.

Распакуйте защищенный конверт ViPNet SIES MC из архива перед загрузкой на SIES-узел для обработки.

Загрузка защищенного конверта с ответом SIES-узла

Обработав защищенный конверт ViPNet SIES MC, доставленный вами на защищаемое устройство, SIES-узел выдает ответ, адресованный ViPNet SIES MC. Вам следует загрузить в ViPNet SIES MC защищенный конверт SIES-узла, чтобы:

- узнать результат выполнения команды;
- обновить состояние SIES-узла в ViPNet SIES MC;
- получить следующую команду для доставки SIES-узлу.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Щелкните **Управление** > **Загрузить ответ SIES-узла на команду**.
4. Выберите файл с ответом SIES-узла на жестком диске вашего компьютера или на внешнем носителе.

   Нажмите кнопку **Выбрать**.

Одновременное управление несколькими SIES-узлами

Для экономии времени на однотипных операциях, вы можете выполнить некоторые операции управления одновременно для нескольких SIES-узлов.

Таблица 11. Поддерживаемые операции управления несколькими SIES-узлами

Операция управления	ViPNet SIES Core	ViPNet SIES Unit	Пользователь	Другой SIES-узел
Обновление состояния (на стр. 26)	+	+	—	+**
Завершение инициализации SIES-узла (на стр. 23)	—	+	—	+
Экспорт инициализирующего архива	—	+	—	—
Перемещение между группами (на стр. 134)	+	+	+	+
Создание и загрузка сертификата (на стр. 41)	+	+	—	+**
Синхронизация прикладных связей (на стр. 51)	+	+	—	+**
Смена режима работы (на стр. 30)	+	+	—	+**
Выгрузка защищенного конверта с командой для SIES-узла (на стр. 56)	+	+	—	+**
Создание архива записей аудита (на стр. 76)	+	—	—	—
Выгрузка архива записей аудита (на стр. 77)	+	—	—	—
Выгрузка архива служебного журнала (на стр. 80)	+	—	—	—
Обновление инициализирующей последовательности (на стр. 48)	+	+	—	+**
Обновление ПО (на стр. 84)	+*	—	—	—
Удаление (на стр. 68)	+	+	+	+

* Выбранные SIES-узлы предварительно переведите в режим работы **Конфигурирование**.

** При поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Чтобы применить операции к нескольким SIES-узлам:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите SIES-узлы.

4 Установите флажки слева от наименований тех SIES-узлов, с которыми вы планируете выполнить намеченные операции управления. Чтобы выбрать все SIES-узлы, установите флажок слева от заголовка **Наименование**.

Совет. Чтобы снять флажок выделения со всех выбранных SIES-узлов, нажмите кнопку и в меню выберите **Снять все выделения**.

---

5 На панели дополнительных сведений нажмите кнопку с нужной операцией управления.

6 Следуйте дальнейшим указаниям ViPNet SIES MC в зависимости от выбранной операции управления.

Исключение SIES-узла из управления ViPNet SIES MC

В ходе эксплуатации SIES-узла вам может понадобиться исключить SIES-узел из управления ViPNet SIES MC в одном из следующих случаев:

- временный вывод SIES-узла из эксплуатации для проведения регламентного обслуживания;
- замена вышедшего из строя защищаемого устройства, в которое встроен SIES-узел;
- последующее удаление SIES-узла (на стр. 68) при изменении топологии информационных потоков индустриальной системы.

При исключении SIES-узла из управления ViPNet SIES MC прекращает мониторинг и управление SIES-узлом. Также блокируется выполнение SIES-узлом криптографических операций по запросам защищаемого устройства.

Внимание! Если для защищаемого устройства, взаимодействующего с исключенным из управления SIES-узлом, заданы прикладные связи, вы не сможете выполнить синхронизацию связей вплоть до подключения SIES-узла к управлению ViPNet SIES MC.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора МС или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. Смените режим работы SIES-узла (на стр. 30) на режим **Конфигурирование**.

   Если SIES-узел в режиме **Блокировка**, менять режим работы не нужно.
5. На панели дополнительных сведений нажмите кнопку и в меню выберите **Исключить из управления**.
6. Нажмите кнопку **Да**.

Подключение SIES-узла к управлению ViPNet SIES MC

Вы можете восстановить мониторинг и управление выбранным SIES-узлом, исключенным (на стр. 61) вами из управления ViPNet SIES MC.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений нажмите кнопку и в меню выберите **Подключить к управлению**.

Контроль инициализации SIES-узлов

Вы можете контролировать ход инициализации SIES-узлов, выполняемой с ViPNet SIES Workstation, например, чтобы убедиться в завершении процесса инициализации.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 На панели инструментов щелкните **Управление** > **Инициализация**.

4 Просмотрите состояние инициализации нужного SIES-узла.

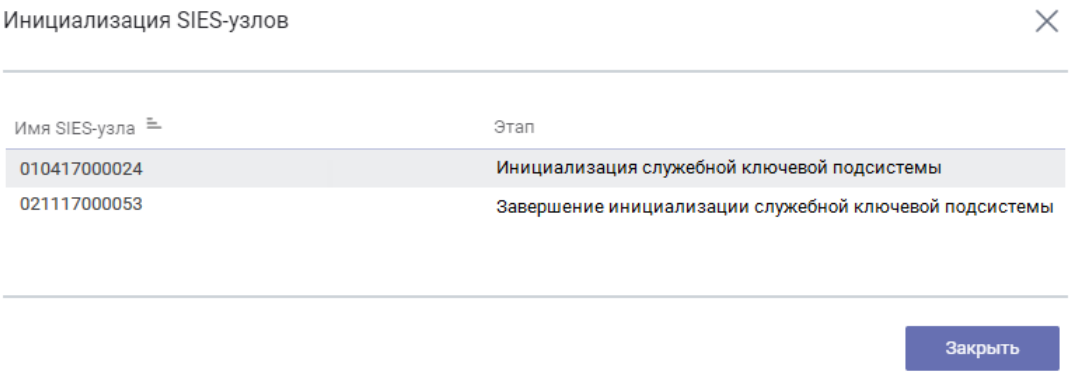

Рисунок 11. Состояние инициализации ViPNet SIES Core

Если инициализация всех SIES-узлов завершена, в окне отобразится сообщение **Нет неинициализированных SIES-узлов**.

Компрометация SIES-узла

При выявлении факта несанкционированного доступа к SIES-узлу данный SIES-узел считается скомпрометированным. После компрометации SIES-узел и выполняемые SIES-узлом криптографические операции перестают быть доверенными. Дальнейшее управление скомпрометированным SIES-узлом из ViPNet SIES MC запрещено.

Фиксация компрометации SIES-узла

При подозрении на компрометацию или при выявленной компрометации следует немедленно перевести SIES-узел в состояние **Скомпрометирован** с помощью ViPNet SIES MC.

ViPNet SIES MC удаляет следующую информацию скомпрометированного SIES-узла:

- прикладные и служебные сертификаты;
- запросы на прикладные и служебные сертификаты;
- записи служебного журнала, выгруженные в ViPNet SIES MC;
- записи журнала аудита, выгруженные в ViPNet SIES MC;
- прикладные связи SIES-узлов, взаимодействующих со скомпрометированным SIES-узлом.

Перед фиксацией факта компрометации экспортируйте из ViPNet SIES MC архивы журнала аудита SIES-узла (на стр. 77), иначе архивы будут утрачены.

Область применения

Все типы SIES-узлов.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите скомпрометированный SIES-узел.
4. Чтобы сократить время работы скомпрометированного SIES-узла в отсутствие возможности оперативно вывести SIES-узел из эксплуатации, приведите SIES-узел к заводскому состоянию (на стр. 66).
5. На панели дополнительных сведений перейдите на вкладку **Общее**.
6. Нажмите **Управление** > **Отметить компрометацию**.
7. Нажмите кнопку **Да**.

8 Периодически просматривайте сведения о компрометации SIES-узла (на стр. 65) вплоть до приведения SIES-узла в состояние **Скомпрометирован**.

Вы можете восстановить SIES-узел после компрометации после того, как SIES-узел будет переведен в состояние **Готов к восстановлению после компрометации**. Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».

Просмотр сведений о компрометации SIES-узла

Вы можете просматривать сведения о компрометации SIES-узла, например, чтобы проверить ход выполнения компрометации SIES-узла в ViPNet SIES MC.

Область применения

Все типы SIES-узлов.

Порядок действий

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите скомпрометированный SIES-узел.

4 На панели дополнительных сведений просмотрите состояние компрометации выбранного SIES-узла.

Под наименованием отображается текущее состояние компрометации:

- Любое из общих состояний SIES-узла (на стр. 26) — SIES-узел не скомпрометирован.
- **Скомпрометирован** — процесс компрометации SIES-узла не завершен. В этом случае ознакомьтесь с состоянием процесса компрометации, в ходе которого на SIES-узлах, взаимодействующих со скомпрометированным SIES-узлом, удаляются прикладные связи.

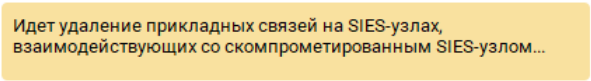

Рисунок 12. Ход процесса компрометации

Если процесс компрометации не был завершен, вы можете продолжить удаление связей, нажав кнопку .

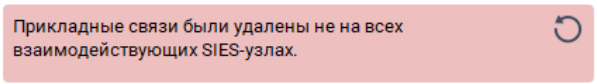

Рисунок 13. Процесс компрометации прерван

- **Готов к восстановлению после компрометации** — процесс компрометации SIES-узла завершен. Вы можете приступить к восстановлению работоспособности SIES-узла. Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».

Приведение SIES-узла к заводскому состоянию

В ходе восстановления работоспособности SIES-узла после компрометации вам потребуется провести повторную инициализацию SIES-узла. Перед повторной инициализацией приведите SIES-узел к заводскому состоянию.

Приводя SIES-узел к заводскому состоянию, ViPNet SIES MC безвозвратно уничтожает следующую информацию как на SIES-узле, так и в ViPNet SIES MC:

- служебные и прикладные сертификаты (на стр. 35);
- очередь задач (на стр. 148) на выполнение команд управления и мониторинга ViPNet SIES MC.

Внимание! После приведения ViPNet SIES Core к заводскому состоянию управление ViPNet SIES Core из ViPNet SIES MC станет невозможным.

Область применения

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел — при поддержке на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Общее**.
5. Нажмите **Управление** > **Привести к заводскому состоянию**.
6. Нажмите кнопку **Да**.

ViPNet SIES MC отправит SIES-узлу команду на приведение к заводскому состоянию.

После завершения обработки команды SIES-узел готов к повторному вводу в эксплуатацию.

Снятие отметки о компрометации SIES-узла

По окончании восстановления работоспособности SIES-узла после компрометации (см. документ «ViPNet SIES. Сценарии эксплуатации») снимите отметку о компрометации SIES-узла, восстановив SIES-узел в ViPNet SIES MC.

Область применения

- Пользователь;
- Другой SIES-узел без поддержки на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Для следующих типов SIES-узлов снятие отметки о компрометации выполняется автоматически после инициализации SIES-узла:

- ViPNet SIES Core;
- ViPNet SIES Unit;
- Другой SIES-узел с поддержкой на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Общее**.
5. Нажмите **Управление** > **Восстановить после компрометации**.

SIES-узел будет переведен в состояние **Не настроен**, как после добавления в ViPNet SIES MC.

Удаление SIES-узла

Удаление SIES-узла из ViPNet SIES MC может потребоваться вам в одном из следующих случаев:

- изменение топологии информационных потоков индустриальной системы с выводом из эксплуатации SIES-узла;
- выход из строя SIES-узла с потерей возможности удаленного управления.

Прежде, чем удалить один или несколько SIES-узлов из ViPNet SIES MC, исключите удаляемые SIES-узлы из управления ViPNet SIES MC (на стр. 61). Перед удалением не нужно исключать ViPNet SIES Core, не прошедшие инициализацию.

Если SIES-узел неработоспособен и не может быть переведен в режим работы «Блокировка» при исключении из управления ViPNet SIES MC, такой SIES-узел можно удалить из ViPNet SIES MC без предварительного исключения из управления, но в этом случае SIES-узел нельзя будет впоследствии восстановить.

Вы можете восстановить управление (на стр. 62) удаленным SIES-узлом, повторно добавив SIES-узел с тем же идентификатором в ViPNet SIES MC. Восстановление возможно лишь в период действия служебного сертификата SIES-узла.

Внимание! Удаление SIES-узла из ViPNet SIES MC может привести к невозможности восстановления функций управления SIES-узлом средствами ViPNet SIES MC.

Область применения

Все типы SIES-узлов.

Порядок действий

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .

   Выберите удаляемый SIES-узел.
3. На панели дополнительных сведений нажмите кнопку и в меню выберите **Удалить**.
4. Подтвердите удаление SIES-узла.

Примечание. Если защищаемое устройство удаленного SIES-узла имело прикладные связи с другими защищаемыми устройствами, синхронизируйте связи (на стр. 51) на защищаемых устройствах, с которыми взаимодействовало защищаемое устройство удаленного SIES-узла.

2

Управление ViPNet SIES Core

Задание связи ViPNet SIES Core с защищаемым устройством 70

Выполнение контроля целостности и версии ПО ViPNet SIES Core 71

Включение датчика контроля доступа к ViPNet SIES Core 72

Отключение датчика контроля доступа к ViPNet SIES Core 73

Управление журналом аудита 74

Управление служебным журналом 79

Управление обновлениями ПО 82

Задание связи ViPNet SIES Core с защищаемым устройством

Заданная связь ViPNet SIES Core с защищаемым устройством позволит перевести ViPNet SIES Core (на стр. 30) в режим работы «Штатный», в котором ViPNet SIES Core будет выполнять криптографическую обработку данных по запросам защищаемого устройства.

Связь ViPNet SIES Core с защищаемым устройством задается путем сохранения серийного номера защищаемого устройства в памяти ViPNet SIES Core и фиксирует принадлежность ViPNet SIES Core к определенному защищаемому устройству.

Совет. Перед заданием связи ViPNet SIES Core с защищаемым устройством задайте (на стр. 97) действительные параметры защищаемого устройства.

Каждый ViPNet SIES Core может быть связан только с одним защищаемым устройством индустриальной системы.

Перед заданием связи назначьте ViPNet SIES Core на защищаемое устройство (на стр. 98). После изменения серийного номера защищаемого устройства связь ViPNet SIES Core с защищаемым устройством будет автоматически задана повторно.

Чтобы задать связь ViPNet SIES Core с защищаемым устройством:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите ViPNet SIES Core.
4. На панели дополнительных сведений перейдите на вкладку **Общее**.

   Текущее состояние принадлежности ViPNet SIES Core к защищаемому устройству отображается на панели дополнительных сведений в разделе **Защищаемое устройство** (на стр. 145).
5. В разделе **Защищаемое устройство** нажмите кнопку и выберите **Задать связь с SIES-узлом**.

Выполнение контроля целостности и версии ПО ViPNet SIES Core

Перед проведением регламентного контроля убедитесь (на стр. 26), что текущая версия ПО ViPNet SIES Core как обновление загружена (на стр. 83) в ViPNet SIES MC. Без загрузки текущей версии ПО ViPNet SIES Core в ViPNet SIES MC вы не сможете провести регламентный контроль.

Чтобы выполнить регламентный контроль целостности и версии ПО ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Общее**.

5 Нажмите **Управление** > **Выполнить регламентный контроль целостности ПО**.

ViPNet SIES MC отправит ViPNet SIES Core команду на запуск регламентного контроля целостности ПО.

6 После завершения выполнения команды на вкладке **Задачи** отобразится информация о результате регламентного контроля целостности ПО и **Контрольный код**, полученный от ViPNet SIES Core.

Сверьте **Контрольный код** ViPNet SIES Core со значением, приведенным в разделе «Контрольные суммы» документа «ViPNet SIES Core. Формуляр. ФРКЕ.466219.011ФО» для версии ПО, встроенного в ViPNet SIES Core.

Совет. Версию ПО ViPNet SIES Core вы можете посмотреть на вкладке **Общее**, нажав кнопку на панели дополнительных свойств.

Если значения контрольного кода в ViPNet SIES MC и в формуляре не совпадают, смените режим работы ViPNet SIES Core на режим «Блокировка» (на стр. 30).

Выполните дальнейшие шаги по выводу ViPNet SIES Core из эксплуатации в соответствии с документом «ViPNet SIES Core. Правила пользования. ФРКЕ.466219.011ПП».

Включение датчика контроля доступа к ViPNet SIES Core

Если защищаемое устройство оборудовано датчиком вскрытия корпуса, подключенным к ViPNet SIES Core, то ViPNet SIES Core может контролировать событие несанкционированного вскрытия корпуса защищаемого устройства. Корпус защищаемого устройства служит корпусом для ViPNet SIES Core, поэтому несанкционированное вскрытие корпуса равнозначно событию несанкционированного доступа к ViPNet SIES Core. Это событие ViPNet SIES Core может контролировать только при включенном датчике.

Чтобы включить датчик:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Общее**.
5. Нажмите **Управление** > **Включить контроль ДНСД**.
6. Нажмите кнопку **Продолжить**.

Внимание! После активации датчика перед санкционированным вскрытием корпуса защищаемого устройства отключите датчик. Иначе ключевая информация будет уничтожена и потребуется повторная инициализация ViPNet SIES Core.

Отключение датчика контроля доступа к ViPNet SIES Core

Перед проведением регламентного обслуживания ViPNet SIES Core или защищаемого устройства временно отключите датчик, подключенный к ViPNet SIES Core, если ViPNet SIES Core контролирует событие несанкционированного вскрытия корпуса защищаемого устройства.

Чтобы отключить датчик:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите SIES-узел.
4. На панели дополнительных сведений перейдите на вкладку **Общее**.
5. Нажмите **Управление** > **Отключить контроль ДНСД**.
6. Нажмите кнопку **Продолжить**.

ViPNet SIES MC отправит ViPNet SIES Core команду на отключение датчика вскрытия корпуса защищаемого устройства. Дождитесь выполнения команды и только потом вскрывайте корпус защищаемого устройства.

Внимание! Включите датчик по окончании регламентного обслуживания ViPNet SIES Core.

Управление журналом аудита

В ходе эксплуатации ViPNet SIES Core в журнале аудита фиксируются значимые события, относящиеся к следующим категориям:

- события самого журнала аудита;
- события хранилища сертификатов и ключевой информации;
- аутентификация (см. глоссарий, стр. 160) пользователей и срабатывание системы защиты от несанкционированного доступа;
- события изменения режима работы ViPNet SIES Core;
- события проверки целостности ПО и аппаратуры ViPNet SIES Core;
- системные события.

С помощью ViPNet SIES MC вы можете управлять журналами аудита ViPNet SIES Core, зарегистрированных в ViPNet SIES MC.

Согласно документа «ViPNet SIES Core. Правила пользования. ФРКЕ.466219.011ПП», следует регулярно выгружать в ViPNet SIES MC журнал аудита ViPNet SIES Core и как минимум один раз в год очищать журнал на ViPNet SIES Core.

Переполнение журнала аудита вызовет автоматический переход ViPNet SIES Core в режим «Системная блокировка». Выполнение криптографических операций с данными защищаемого устройства на ViPNet SIES Core будет запрещено.

Получение записей

Записи журнала аудита хранятся на SIES-узле. Чтобы просмотреть журнал аудита в ViPNet SIES MC, записи аудита следует предварительно загрузить в ViPNet SIES MC.

Совет. Поскольку для хранения записей журнала аудита в ViPNet SIES Core выделен ограниченный объем памяти, вам следует периодически загружать записи в ViPNet SIES MC, не допуская переполнения хранилища журнала. ViPNet SIES MC автоматически уведомит вас о наступлении срока загрузки записей.

Чтобы загрузить в ViPNet SIES MC записи журнала аудита с SIES-узла:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите ViPNet SIES Core.
4. На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Выгрузить журнал с SIES-узла**.

Контролировать исполнение команды SIES-узлом вы можете на панели дополнительных свойств, перейдя на вкладку **Задачи**. Если получить записи аудита не удалось, ViPNet SIES Core следует вывести из эксплуатации.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Просмотр записей

Вы можете просматривать записи журнала аудита ViPNet SIES Core, полученные в ViPNet SIES MC, например, для контроля загрузки сертификатов.

Чтобы просмотреть записи журнала аудита ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **SIES-узлы**.

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Просмотреть**.

6 Если записи журнала аудита ViPNet SIES Core предварительно загружались в ViPNet SIES MC (на стр. 74), то в появившемся окне будут показаны фрагменты журнала аудита, отсортированные по дате первой записи фрагмента. Графа **В Архиве** служит для контроля за архивацией записей (на стр. 76).

   Для просмотра записей журнала аудита щелкните по нужному фрагменту.

Журнал аудита SIES-узла
011017000022

Фрагмент	Записи	Первая запись	Последняя запись	Дата загрузки	Инициатор	В архиве
2	17	28.03.2018 15:35	28.03.2018 16:13	28.03.2018 16:13	AutoTestSuperAdmin	Да
1	22	01.01.2000 03:02	28.03.2018 16:04	28.03.2018 16:04	AutoTestSuperAdmin	Да

Закрыть

Рисунок 14. Фрагменты журнала аудита

7 Просмотрите записи выбранного фрагмента журнала аудита ViPNet SIES Core, загруженные в ViPNet SIES MC.

Примечание. В журнале могут встречаться неполные записи, нарушение целостности которых было выявлено на стороне ViPNet SIES Core.

Чтобы вернуться к списку фрагментов журнала аудита, щелкните ссылку **Содержание** в левой верхней части окна.

8 По окончании просмотра записей нажмите кнопку **Закрыть**.

Очистка журнала

Если вы получили все записи журнала аудита ViPNet SIES Core за истекший период эксплуатации, вы можете очистить журнал, освободив место в памяти ViPNet SIES Core для новых записей.

При очистке журнала аудита на ViPNet SIES Core сохраняются записи:

- не выгружавшиеся в ViPNet SIES MC;
- внесенные в журнал в течение последних трех суток.

Чтобы очистить журнал аудита SIES-узла:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Очистить журнал на SIES-узле**.

6 Нажмите кнопку **Да**.

Создание архива записей

Вы можете создать архив записей журнала аудита ViPNet SIES Core, например, чтобы исследовать события, произошедшие на ViPNet SIES Core за истекший период. В архив помещаются все записи фрагментов, не проходивших архивацию ранее.

Для каждого SIES-узла вы можете создать один архив записей. Чтобы создать новый архив взамен существующего, предварительно выгрузите (на стр. 77) существующий архив записей из ViPNet SIES MC, а затем удалите архив (на стр. 78).

Чтобы создать архив записей журнала аудита ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Создать архив**.

Запустится процесс создания архива записей журнала аудита выбранного ViPNet SIES Core.

Примечание. По завершении архивирования помещенные в архив фрагменты журнала аудита получат пометку **Да** в графе **В архиве** при выборе фрагментов для просмотра (на стр. 75).

6 Чтобы просмотреть сведения о созданном архиве, на панели дополнительных сведений нажмите **Журнал аудита** > **Информация об архиве**.

Созданный архив записей журнала аудита выбранного ViPNet SIES Core вы можете выгрузить из ViPNet SIES MC для обработки на рабочем месте.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Выгрузка архива записей

Вы можете выгрузить архив с записями журнала аудита ViPNet SIES Core из ViPNet SIES MC, например, чтобы работать с архивом на своем рабочем месте.

Чтобы выгрузить архив записей журнала аудита ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Выгрузить архив**.

6 Задайте пароль длиной не менее 8 символов для защиты файла с архивом журнала аудита.

Нажмите кнопку **OK**.

7 Укажите место сохранения архива.

8 Подтвердите успешную выгрузку архива во всплывающем окне, нажав кнопку **Подтвердить**.

В результате архив записей журнала аудита выбранного ViPNet SIES Core будет сохранен в файл с именем `audit_sies_mod_XXXXXXXXXXXX_ГГГГММДДТЧЧММССZ_суффикс.tar.gz`. Здесь:

- `XXXXXXXXXXXX` — 12-значный серийный номер ViPNet SIES Core;
- `ГГГГММДДТЧЧММСС` — дата выгрузки архива в UTC-кодировке;
- `T` — разделитель даты и времени;
- `Z` — флаг UTC-кодировки метки времени;
- `суффикс` — не более 16 символов признака уникальности архива в случае создания нескольких архивов одновременно (признак может отсутствовать).

Также вы можете выгрузить архивы журналов аудита для нескольких ViPNet SIES Core одновременно, воспользовавшись соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59). Архивы журналов аудита выбранных ViPNet SIES Core будут вложены в единый архив с именем файла `audit_sies_mod_archives_ГГГГММДДТЧЧММССZ_суффикс.tar.gz`.

Информацию о событиях аудита из загруженного файла вы можете исследовать с помощью дополнительного ПО.

Удаление архива записей

Вы можете удалить устаревший архив записей журнала аудита ViPNet SIES Core, например, чтобы создать новый архив.

Перед удалением архив следует выгрузить из ViPNet SIES MC и подтвердить успешное завершение выгрузки (на стр. 77).

Чтобы удалить архив записей журнала аудита SIES-узла:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Журнал аудита** > **Удалить архив**.

6 Нажмите кнопку **Да**.

Управление служебным журналом

В ходе эксплуатации ViPNet SIES Core ведутся служебные журналы, которые вы можете использовать для диагностики работы SIES-узла.

С помощью ViPNet SIES MC вы можете выгружать служебные журналы с ViPNet SIES Core, зарегистрированных в ViPNet SIES MC.

Получение записей

Записи служебных журналов хранятся на ViPNet SIES Core. Чтобы просмотреть служебные журналы, записи следует предварительно загрузить в ViPNet SIES MC.

Чтобы загрузить в ViPNet SIES MC записи служебных журналов с ViPNet SIES Core:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** .
3. Выберите ViPNet SIES Core.
4. На панели дополнительных сведений перейдите на вкладку **Журналы**.
5. Нажмите **Служебный журнал** > **Выгрузить журнал с SIES-узла**.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

По завершении загрузки записей служебных журналов вы можете выгрузить архив записей на свой компьютер (на стр. 80) для последующего просмотра и анализа.

Очистка журнала

Если вы получили все записи служебных журналов ViPNet SIES Core за истекший период эксплуатации, вы можете очистить журнал, чтобы облегчить контроль за записями журнала.

Чтобы очистить служебные журналы SIES-узла:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Служебный журнал** > **Очистить журнал на SIES-узле**.

6 Нажмите кнопку **Да**.

Выгрузка архива записей

Вы можете выгрузить архив с записями служебных журналов ViPNet SIES Core из ViPNet SIES MC, например, чтобы работать с записями на своем рабочем месте.

Совет. Предварительно загрузите в ViPNet SIES MC актуальные записи служебных журналов SIES-узла (на стр. 79).

Чтобы выгрузить архив записей служебных журналов ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Служебный журнал** > **Выгрузить архив**.

Записи о событиях из загруженного файла вы можете исследовать с помощью дополнительного ПО.

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Изменение уровня журналирования

Вы можете изменить уровень детализации записей служебного журнала, например, чтобы точнее локализовать возможную неполадку в работе ViPNet SIES Core.

Помимо изменения уровня детализации служебного журнала в целом, вы можете задать уровень детализации записей о работе отдельных модулей ViPNet SIES Core с помощью текстовой строки, полученной от представителя компании ИнфоТеКС.

Чтобы изменить уровень журналирования:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Журналы**.

5 Нажмите **Служебный журнал** > **Изменить уровень журналирования**.

6 Выберите новый уровень журналирования из списка. Каждый последующий уровень повышает детализацию и включает детализацию всех предыдущих уровней.

Примечание. Уровень **6 – Все события** вы можете установить только на ViPNet SIES Core с отладочной версией ПО.

До первой установки из ViPNet SIES MC на ViPNet SIES Core используется уровень журналирования **Все ошибки**.

Если у вас есть текстовая строка с дополнительными параметрами, полученная от представителя компании ИнфоТеКС, установите флажок **Дополнительные правила журналирования** и введите строку в текстовое поле.

7 Нажмите кнопку **Задать**.

Установленный уровень журналирования сохранится при перезагрузке ViPNet SIES Core вплоть до установки нового значения уровня или до приведения ViPNet SIES Core к заводскому состоянию.

Управление обновлениями ПО

Программное обеспечение, встроенное в ViPNet SIES Core, предусматривает обновление по мере выпуска новых версий с расширенными функциональными возможностями.

Получив новую версию от компании ИнфоТеКС, вы можете обновить ПО ViPNet SIES Core с помощью ViPNet SIES MC. Также ViPNet SIES MC сохраняет архив версий ПО ViPNet SIES Core для возможного последующего применения и выполнения регламентного контроля целостности и версии ПО (на стр. 71).

Обновление ПО до версии 2.2.1: порядок действий

Обновлять ПО до версии 2.2.1 следует на всех ViPNet SIES Core. Одновременно следует обновить ПО на тех ViPNet SIES Core, защищаемые устройства которых участвуют в одних и тех же прикладных связях с назначениями:

- **Вычисление и проверка имитовставки**
- **Шифрование в режиме реального времени**

Если невозможно обновить ПО на всех ViPNet SIES Core в течение одного периода регламентного обслуживания, сгруппируйте ViPNet SIES Core по признаку участия в одной и той же прикладной связи: ПО всех SIES-узлов, участвующих в прикладной связи должно быть либо обновлено до версии 2.2.1, либо иметь версию 2.2 и ниже.

Для обновления ПО ViPNet SIES Core до версии 2.2.1 вам понадобится следующее:

- ПО ViPNet SIES MC версии 2.2.2;
- обновление ПО ViPNet SIES Core версии 2.2.1;

Чтобы обновить ПО ViPNet SIES Core при наступлении периода регламентного обслуживания защищаемого устройства, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 12. Порядок обновления ПО ViPNet SIES Core

	Действие	Ссылка
☐	Обновите ПО ViPNet SIES MC до версии 2.2.2.	См. документ «ViPNet SIES MC. Установка и обслуживание».
☐	Загрузите в ViPNet SIES MC версию ПО 2.2.1 ViPNet SIES Core.	Добавление обновления (на стр. 83).
☐	Обновите ПО ViPNet SIES Core до версии 2.2.1.	Обновление ПО ViPNet SIES Core (на стр. 84).

	Действие	Ссылка
☐	Синхронизируйте прикладные связи на ViPNet SIES Core, ПО на которых было обновлено до версии 2.2.1.	Синхронизация прикладных связей (на стр. 51) Операцию можно выполнить до завершения обновления ПО SIES-узлов.

Добавление обновления

Перед обновлением ПО ViPNet SIES Core предварительно загрузите в ViPNet SIES MC файлы обновлений. Также в качестве обновления вы можете загрузить ПО ViPNet SIES Core для выполнения контроля целостности и версии ПО.

Чтобы загрузить в ViPNet SIES MC обновление ПО ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Обновления** .

3 В разделе **Обновление SIES-узлов** просмотрите сведения об обновлениях, добавленных в ViPNet SIES MC.

   Список добавленных обновлений отображается, если ранее обновления добавлялись в ViPNet SIES MC.

Версия	Совместима с платформами	Контрольный код	Устройства	Дата загрузки	Администратор	Размер	
1.6.0.28	SIES Core v5	F0370010	0	24.05.2018 в 13:17	AutoTestSuperAdmin	1.36 Мб	
1.6.0.38	SIES Core v5	D03C0010	0	24.05.2018 в 13:14	AutoTestSuperAdmin	1.57 Мб	
1.6.0.39	SIES Core v5	D03C0010	0	24.05.2018 в 13:17	AutoTestSuperAdmin	1.57 Мб	

   Рисунок 15. Обновления ПО ViPNet SIES Core в ViPNet SIES MC

4 Нажмите кнопку **Загрузить обновление SIES-узла**, чтобы добавить очередное обновление.

5 Выберите файл `*.upd` с обновлением ПО.

После успешной загрузки и проверки целостности архива файл обновления ПО ViPNet SIES Core будет добавлен в ViPNet SIES MC. Информация об обновлении появится в списке.

Совет. Чтобы убедиться в подлинности обновления ПО ViPNet SIES Core, вы можете сверить значение графы **Контрольный код** со значением, приведенным в разделе «Контрольные суммы» документа «ViPNet SIES Core. Формуляр. ФРКЕ.466219.011ФО».

Каждое из обновлений ПО ViPNet SIES Core, загруженных в ViPNet SIES MC, вы можете применить к одной или нескольким целевым платформам ViPNet SIES Core (на стр. 149), перечисленным в графе **Совместима с платформами**.

Обозначение платформы ViPNet SIES Core, зарегистрированного в ViPNet SIES MC, вы можете посмотреть (на стр. 26) в разделе **SIES-узлы** , нажав кнопку на панели дополнительных свойств.

Обновление ПО

Вы можете обновить текущее ПО ViPNet SIES Core до версии ПО, выбранной из списка предварительно загруженных обновлений. После применения обновления ПО ViPNet SIES Core текущие настройки и ключевая информация ViPNet SIES Core сохраняются.

Вы можете вернуть на ViPNet SIES Core предыдущую версию ПО.

Обновление ПО ViPNet SIES Core следует проводить в ходе регламентного обслуживания защищаемого устройства, в которое встроен ViPNet SIES Core.

Внимание! Перед началом обновления ПО на ViPNet SIES Core обеспечьте гарантированное питание до завершения обновления. Отказ питания может привести к выходу ViPNet SIES Core из строя.

Чтобы обновить ПО ViPNet SIES Core:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.

2 Перейдите в раздел **SIES-узлы** .

3 Выберите ViPNet SIES Core.

4 На панели дополнительных сведений перейдите на вкладку **Общее**.

5 Нажмите **Управление** > **Сменить режим работы** > **Конфигурирование**.

6 Нажмите **Управление** > **Обновить ПО**.

Примечание. Если вы еще не загружали обновление в ViPNet SIES MC, откроется окно с приглашением загрузить обновление ПО ViPNet SIES Core. После загрузки обновления в ViPNet SIES MC вы сможете обновить ПО ViPNet SIES Core.

7 Выберите обновление ViPNet SIES Core и нажмите кнопку **Применить**.

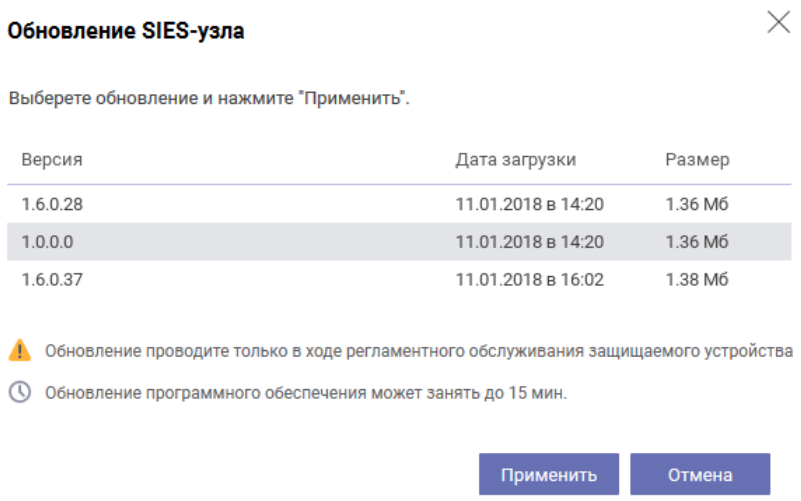

Рисунок 16. Выбор обновления

8 Проверьте версию выбранного обновления и подтвердите решение обновить ПО ViPNet SIES Core, нажав кнопку **Применить**.

После выполнения команд вы можете проверить номер установленной версии ПО на панели дополнительных сведений на вкладке **Задачи** или выбрав на панели навигации раздел **Журнал событий** .

Совет. Чтобы выполнить эту операцию для множества SIES-узлов, воспользуйтесь соответствующей возможностью одновременного управления несколькими SIES-узлами (на стр. 59).

Удаление обновления

Вы можете удалить обновление ПО ViPNet SIES Core из ViPNet SIES MC, если обновление не применялось ни на одном из ViPNet SIES Core, зарегистрированных в ViPNet SIES MC.

Файлы обновлений используются в ViPNet SIES MC при контроле целостности ПО ViPNet SIES Core. Поэтому обновления, примененные хотя бы на одном из ViPNet SIES Core, нельзя удалить из ViPNet SIES MC.

Чтобы удалить обновление ПО ViPNet SIES Core из ViPNet SIES MC:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Обновления** .

3 В разделе **Обновление SIES-узлов** просмотрите сведения об обновлениях, имеющихся в ViPNet SIES MC.

4 Справа от удаляемого обновления нажмите кнопку .

5 Нажмите кнопку **Да**.

3

Управление ViPNet SIES Unit

Ручная инициализация ViPNet SIES Unit: порядок действий 88

Ручная инициализация ViPNet SIES Unit: порядок действий

Настройте служебную ключевую подсистему ViPNet SIES Unit (см. глоссарий, стр. 159) для последующего управления SIES-узлом из ViPNet SIES MC.

Внимание! Перед повторной инициализацией ViPNet SIES Unit удалите существующий SIES-узел (на стр. 68) из ViPNet SIES MC.

Чтобы вручную настроить служебную ключевую подсистему ViPNet SIES Unit, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 13. Порядок инициализации ViPNet SIES Unit

	Действие	Ссылка
☐	От администратора ViPNet SIES Unit получите USB-носитель с запросом на служебный сертификат ViPNet SIES Unit.	
☐	Подключите USB-носитель с запросом на служебный сертификат ViPNet SIES Unit к рабочему месту супер-администратора, администратора MC или администратора группы.	
☐	Добавьте ViPNet SIES Unit в ViPNet SIES MC.	Добавление ViPNet SIES Unit по запросу на служебный сертификат (на стр. 19).
☐	Подтвердите завершение инициализации ViPNet SIES Unit и экспортируйте инициализирующий архив с защищенными конвертами ViPNet SIES MC на USB-носитель.	• Завершение инициализации SIES-узла (на стр. 23). • Одновременное управление несколькими SIES-узлами (на стр. 59).
☐	Доверенным способом (см. глоссарий, стр. 160) передайте USB-носитель с инициализирующим архивом администратору ViPNet SIES Unit для последующего импорта в ViPNet SIES Unit.	
☐	Получив от администратора ViPNet SIES Unit подтверждение о завершении инициализации ViPNet SIES Unit, обновите состояние ViPNet SIES Unit.	• Просмотр сведений о SIES-узле (на стр. 26). • Одновременное управление несколькими SIES-узлами (на стр. 59).

4

Управление SIES-узлами другого типа

Ручная инициализация другого SIES-узла 90

Ручная инициализация другого SIES-узла: порядок действий

Внимание! Перед повторной инициализацией удалите существующий SIES-узел (на стр. 68) из ViPNet SIES MC.

Чтобы настроить служебную ключевую подсистему другого SIES-узла, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 14. Порядок инициализации другого SIES-узла

	Действие	Ссылка
☐	От администратора другого SIES-узла получите USB-носитель с запросом на служебный сертификат SIES-узла.	
☐	Подключите USB-носитель с запросом на служебный сертификат SIES-узла к рабочему месту супер-администратора, администратора MC или администратора группы.	
☐	Добавьте другой SIES-узел в ViPNet SIES MC.	Добавление другого SIES-узла (на стр. 21).
☐	Добавьте в ViPNet SIES MC запрос на служебный сертификат другого SIES-узла.	Импорт запроса на сертификат (на стр. 46).
☐	На внешний USB-носитель выгрузите из ViPNet SIES MC следующие сертификаты: • служебный сертификат ViPNet SIES MC; • служебный сертификат другого SIES-узла, изданный ViPNet SIES MC.	Экспорт сертификата (на стр. 47).
☐	Доверенным способом передайте USB-носитель с сертификатами администратору другого SIES-узла для последующего импорта на SIES-узел.	
☐	Подтвердите завершение инициализации другого SIES-узла.	Завершение инициализации SIES-узла (на стр. 23).
☐	Если у SIES-узла с поддержкой управления из ViPNet SIES MC нет своего источника инициализирующей последовательности для датчика случайных чисел, обновите первичную ключевую информацию другого SIES-узла.	Обновление инициализирующей последовательности SIES-узла (на стр. 48).

5

Управление защищаемыми устройствами

Об управлении защищаемыми устройствами 92

Добавление защищаемого устройства 93

Просмотр сведений о защищаемом устройстве 96

Изменение параметров защищаемого устройства 97

Назначение SIES-узла на защищаемое устройство 98

Отмена назначения SIES-узла на защищаемое устройство 99

Одновременное управление несколькими защищаемыми устройствами 100

Регистрация резервных защищаемых устройств: порядок действий 101

Удаление защищаемого устройства 103

Управление прикладными связями защищаемого устройства 104

Об управлении защищаемыми устройствами

Каждое защищаемое устройство представляет в ViPNet SIES MC индустриальное устройство или устройство операторского уровня индустриальной системы, взаимодействующее с SIES-узлом.

Для реализации сценариев защиты данных и удаленного управления из ViPNet SIES MC каждый SIES-узел, зарегистрированный в ViPNet SIES MC, должен быть назначен на защищаемое устройство.

Добавление защищаемого устройства

Перед реализацией сценариев защиты данных индустриальной системы в ViPNet SIES MC следует добавить все защищаемые устройства.

Вы можете добавлять защищаемые устройства в ViPNet SIES MC независимо от добавления SIES-узлов, с которыми взаимодействуют защищаемые устройства.

Чтобы добавить защищаемое устройство в ViPNet SIES MC:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Щелкните ссылку **Добавить** > **Защищаемое устройство**.

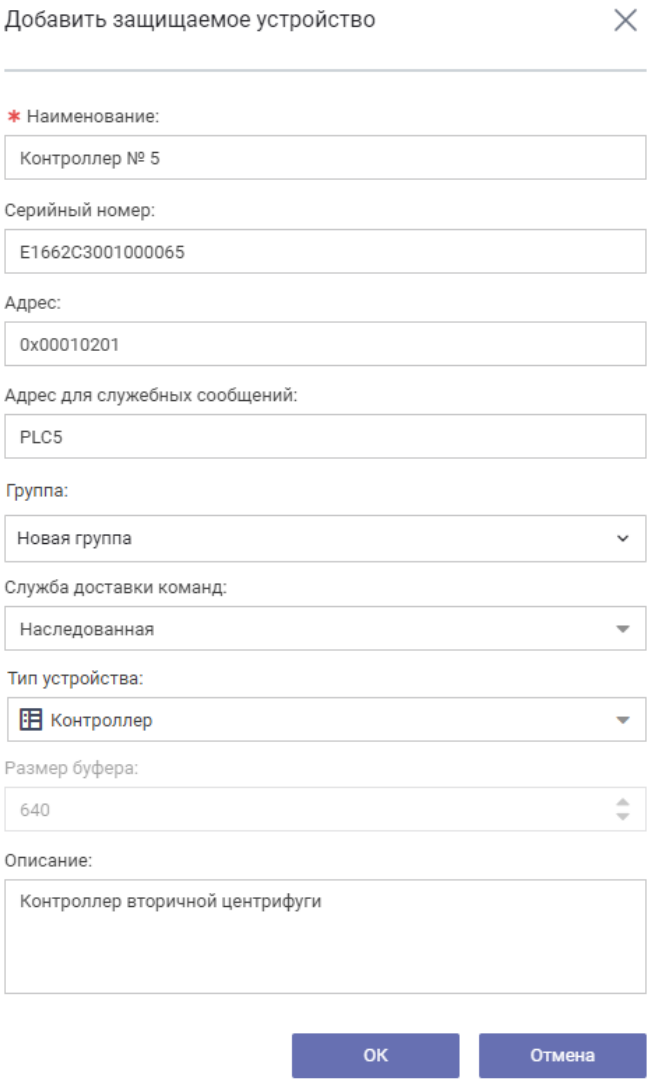

Рисунок 17. Задание параметров защищаемого устройства

4 Задайте следующие параметры добавляемого защищаемого устройства:

- **Наименование** — уникальное обозначение защищаемого устройства в ViPNet SIES MC. Длина значения — до 128 символов.

  Параметр обязательный для задания. Вы можете использовать любое наименование, которое облегчит вам идентификацию защищаемого устройства в топологии развернутого комплекса ViPNet SIES.

- **Серийный номер** (см. глоссарий, стр. 164) — уникальное обозначение защищаемого устройства (серийный, инвентарный номер или идентификатор). Длина значения — до 128 символов: буквы русского и латинского алфавита, специальные символы «_», «-», «(», «)», «\», «|», «/», «:», «.» и цифры.

  Серийный номер защищаемого устройства заносится в память ViPNet SIES Core, когда задается связь ViPNet SIES Core с защищаемым устройством (на стр. 70).

Совет. Если защищаемое устройство состоит из нескольких частей, каждая из которых взаимодействует с отдельным SIES-узлом, вам следует добавить каждую из составных частей в виде отдельного защищаемого устройства, задав для всех частей одинаковый серийный номер.

- **Адрес** (см. глоссарий, стр. 160) — уникальное обозначение защищаемого устройства в индустриальной системе, с помощью которого другие защищаемые устройства взаимодействуют с данным защищаемым устройством. Длина значения — до 128 символов: буквы русского и латинского алфавита, специальные символы «_», «–», «(», «)», «\», «|», «/», «:», «.» и цифры.

  Адрес должен быть уникальным для всего пространства значений, включающим в себя:

  - все адреса защищаемых устройств;
  - все мультивещательные адреса (см. глоссарий, стр. 163).

- **Адрес для служебных сообщений** (см. глоссарий, стр. 160) — адрес защищаемого устройства в индустриальной системе, на который ViPNet SIES MC будет отправлять команды управления и мониторинга для SIES-узла через службу доставки защищенных конвертов. Длина значения — до 128 символов.

  Задайте адрес, если вы планируете удаленно управлять SIES-узлами с помощью ViPNet SIES MC. Подробнее см. документ «ViPNet SIES MC. Руководство разработчика».

- **Группа** — выберите группу, в которую хотите добавить защищаемое устройство, если группа отличается от текущей группы ViPNet SIES MC.

- **Служба доставки команд** — выберите службу доставки защищенных конвертов, если для добавляемого защищаемого устройства нужно задать службу, не наследуемую от родительской группы. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».

- **Тип устройства** — выберите тип добавляемого индустриального устройства из предложенных в списке.

- **Размер буфера** — размер в килобайтах буфера защищаемого устройства, выделенного для временного хранения данных при обмене с ViPNet SIES MC.

  ViPNet SIES MC использует 640 Кбайт в качестве фиксированного значения размера буфера. Размер защищенных конвертов ViPNet SIES MC в адрес SIES-узла не превышает 640 Кбайт. Вы не можете изменить заданное значение.

- **Описание** — добавьте любую дополнительную информацию о защищаемом устройстве. Заполнять поле не обязательно.

Нажмите кнопку **OK**.

Вы можете назначить SIES-узел (на стр. 98) на добавленное защищаемое устройство.

Просмотр сведений о защищаемом устройстве

Вы можете просматривать сведения о защищаемом устройстве, зарегистрированном в ViPNet SIES MC, например, чтобы узнать, какой из SIES-узлов назначен на защищаемое устройство.

Чтобы просмотреть сведения о защищаемом устройстве:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство.
4. На панели дополнительных сведений просмотрите параметры выбранного защищаемого устройства.

Изменение параметров защищаемого устройства

В ходе эксплуатации SIES-узла параметры защищаемого устройства следует поддерживать в актуальном состоянии.

Чтобы изменить параметры защищаемого устройства SIES-узла:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство.
4. На панели дополнительных сведений нажмите кнопку .
5. Укажите новые параметры защищаемого устройства.
6. Нажмите кнопку **OK**.

Внимание! После изменения серийного номера защищаемого устройства, в которое встроен ViPNet SIES Core, задайте связь ViPNet SIES Core с защищаемым устройством (на стр. 70).

Назначение SIES-узла на защищаемое устройство

Чтобы ассоциировать SIES-узел с индустриальным устройством и управлять SIES-узлом из ViPNet SIES MC, назначьте SIES-узел на защищаемое устройство.

Внимание! SIES-узел будет помещен в ту группу ViPNet SIES MC, в которой расположено защищаемое устройство, на которое назначен SIES-узел.

Чтобы назначить SIES-узел на защищаемое устройство:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство.
4. На панели дополнительных сведений нажмите кнопку **Назначить SIES-узел**.
5. Выберите SIES-узел и нажмите кнопку **OK**.
6. Если защищаемое устройство и SIES-узел расположены в разных группах, появится окно с запросом подтверждения на перенос SIES-узла в группу защищаемого устройства. Нажмите кнопку **Да**.

Список всех SIES-узлов, назначенных на защищаемое устройство, вы можете просмотреть на панели дополнительных сведений в разделе **Назначенные SIES-узлы**.

Совет. Аналогичную операцию вы можете выполнить на вкладке **Общее** панели дополнительных сведений о SIES-узле (на стр. 26) в разделе **Защищаемое устройство**, нажав кнопку и выбрав **Назначить SIES-узел**.

Отмена назначения SIES-узла на защищаемое устройство

Вам может потребоваться отменить назначение SIES-узла на защищаемое устройство, например, перед заменой индустриального устройства, представленного защищаемым устройством в ViPNet SIES MC. Предварительно удалите прикладные связи защищаемого устройства (на стр. 125), на которое назначен SIES-узел.

Чтобы отменить назначение SIES-узла на защищаемое устройство:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство.
4. На панели дополнительных сведений в разделе **Назначенные SIES-узлы** щелкните по наименованию SIES-узла, который нужно снять с защищаемого устройства.
5. В раскрывшемся разделе нажмите кнопку .
6. Нажмите кнопку **Да**.

Совет. Аналогичную операцию вы можете выполнить на вкладке **Общее** панели дополнительных сведений о SIES-узле (на стр. 26) в разделе **Защищаемое устройство**, нажав кнопку и выбрав **Отменить назначение SIES-узла**.

Одновременное управление несколькими защищаемыми устройствами

Для экономии времени на однотипных операциях, вы можете выполнить операции одновременно для нескольких защищаемых устройств или их групп.

С выбранными защищаемыми устройствами вы можете выполнять следующие операции:

- перемещение между группами (на стр. 134);
- добавление парной прикладной связи (на стр. 107) между всеми выбранными защищаемыми устройствами;
- добавление парной прикладной связи (на стр. 109) между выбранными защищаемыми устройствами и защищаемыми устройствами, выбор которых будет предложен;
- добавление мультивещательной связи (на стр. 115);
- добавление резервирования парной связи (на стр. 111);
- удаление (на стр. 103).

Чтобы применить операции к нескольким защищаемым устройствам:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемые устройства.

4 Установите флажки слева от наименований тех защищаемых устройств или их групп, с которыми вы планируете выполнить намеченные операции управления. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Наименование**.

Совет. Чтобы снять флажок выделения со всех выбранных защищаемых устройств, нажмите кнопку и в меню выберите **Снять все выделения**.

---

5 На панели дополнительных сведений нажмите кнопку с нужной операцией управления.

6 Следуйте дальнейшим указаниям ViPNet SIES MC в зависимости от выбранной операции управления.

Регистрация резервных защищаемых устройств: порядок действий

Если в индустриальной системе применяется резервирование защищаемых устройств, вы можете использовать функции SIES-узлов по криптографической обработке данных на резервных защищаемых устройствах.

Чтобы использовать функции SIES-узлов по криптографической обработке данных с применением резервных защищаемых устройств, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 15. Регистрация резервных защищаемых устройств

	Действие	Ссылка
☐	Добавьте основное и резервные защищаемые устройства.	Добавление защищаемого устройства (на стр. 93). Если основное и резервные защищаемые устройства имеют один и тот же адрес, задайте этот адрес для всех добавляемых защищаемых устройств. Для удобства идентификации и поиска рекомендуется в **Наименование** защищаемого устройства добавить признак, характеризующий защищаемое устройство как резервное. Также можно использовать поле **Описание**.
☐	Добавьте SIES-узлы основного и резервных защищаемых устройств.	Добавление SIES-узла в ViPNet SIES MC (на стр. 16). Для удобства идентификации и поиска рекомендуется в **Наименование** SIES-узла добавить признак, характеризующий принадлежность SIES-узла к резервному защищаемому устройству. Также можно использовать поле **Описание**.
☐	Назначьте SIES-узлы на основное и резервные защищаемые устройства.	Назначение SIES-узла на защищаемое устройство (на стр. 98).
☐	Добавьте резервированную парную связь, указав в числе участников связи: • основное и резервные защищаемые устройства (на стр. 164) одной стороны взаимодействия; • защищаемое устройство второй стороны взаимодействия без поддержки резервирования или также основное и резервные защищаемые устройства.	Добавление резервированной парной связи (на стр. 111). Назначения связи задайте в соответствии с выбранным сценарием защиты данных. См. ViPNet SIES. Сценарии работы.

	Действие	Ссылка
☐	Синхронизируйте связи.	Синхронизация прикладных связей (на стр. 51).

Указанные действия выполните для всех групп основных и резервных защищаемых устройств, используемых в индустриальной системе.

Удаление защищаемого устройства

Удаление SIES-узла из ViPNet SIES MC может потребоваться вам, например, при изменении топологии информационных потоков индустриальной системы с выводом из эксплуатации индустриального устройства.

Если у защищаемого устройства есть прикладные связи, то сначала удалите связи (на стр. 125), а затем защищаемое устройство. Если на защищаемое устройство назначен SIES-узел, то отмените назначение SIES-узла (на стр. 99).

Чтобы удалить защищаемое устройство из ViPNet SIES MC:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите удаляемое защищаемое устройство.
4. На панели дополнительных сведений нажмите кнопку и в меню выберите **Удалить**.
5. Подтвердите удаление защищаемого устройства.

Управление прикладными связями защищаемого устройства

Для организации защищенного обмена данными между защищаемыми устройствами в реализуемых сценариях защиты информации добавьте прикладные связи между защищаемыми устройствами. Подробнее о сценариях защиты данных индустриальной системы, реализуемых с помощью комплекса ViPNet SIES, см. документ «ViPNet SIES. Сценарии работы».

В ViPNet SIES реализована поддержка прикладных связей следующих видов:

- парная связь (см. глоссарий, стр. 163);
- мультивещательная связь (см. глоссарий, стр. 163);
- резервированная парная связь (см. глоссарий, стр. 163).

Если на защищаемое устройство назначен SIES-узел, при добавлении или изменении связи ViPNet SIES MC проверяет возможность передачи информации о связи в зависимости от типа SIES-узла. Также эта операция выполняется при назначении SIES-узла (на стр. 98) на защищаемое устройство.

Таблица 16. Назначения прикладных связей, поддерживаемые SIES-узлами

Назначение	ViPNet SIES Core ViPNet SIES Unit Другой SIES-узел при поддержке удаленного управления SIES-узлом из ViPNet SIES MC	Другой SIES-узел без поддержки удаленного управления SIES-узлом из ViPNet SIES MC	Пользователь
Вычисление и проверка имитовставки	+	—	—
Шифрование в режиме реального времени	+	—	—
Шифрование и проверка электронной подписи	+	+	+
Вычисление и проверка хэш-суммы	+	—	+

Связи между защищаемыми устройствами имеют срок действия — период, в течение которого возможно выполнение криптографических операций SIES-узлами, между защищаемыми устройствами которых добавлена связь. В зависимости от вида связи срок действия связи соответствует сроку действия прикладной ключевой информации, используемой для криптографической обработки данных. Подробнее о сроках действия ключевой информации см. документ «ViPNet SIES MC. Общее описание».

Парные связи между защищаемыми устройствами идентифицируются в ViPNet SIES MC по наименованию защищаемого устройства, с которым задана связь. Задать наименование защищаемого устройства вы можете при добавлении защищаемого устройства (на стр. 93) или изменив параметры (на стр. 97) защищаемого устройства, зарегистрированного в ViPNet SIES MC.

Мультивещательные связи идентифицируются по уникальному наименованию.

Для выполнения сценариев защиты данных между защищаемыми устройствами, назначения связей и ключевую информацию следует поддерживать в синхронизированном состоянии с помощью ViPNet SIES MC.

Синхронизация заключается в загрузке актуальной ключевой информации и параметров связи на взаимодействующие SIES-узлы. После синхронизации связанные защищаемые устройства могут взаимодействовать друг с другом защищенным образом в реализованных сценариях защиты данных индустриальной системы.

Таблица 17. Сроки синхронизации связей

Назначение связи	Срок синхронизации
Вычисление и проверка имитовставки	Очередная синхронизация — за 45 суток до окончания действия текущего прикладного мастер-ключа ViPNet SIES.
Шифрование в режиме реального времени	Очередная синхронизация — за 45 суток до окончания действия текущего прикладного мастер-ключа ViPNet SIES.
Шифрование и проверка электронной подписи	В течение 45 суток с момента создания прикладного сертификата SIES-узла.
Вычисление и проверка хэш-суммы	В течение 45 суток с момента создания прикладного сертификата SIES-узла.

Перед синхронизацией связей с назначениями **Вычисление и проверка имитовставки** и **Шифрование в режиме реального времени**, выполняемой администратором группы, требуется предварительно создать прикладной мастер-ключ ViPNet SIES. Подробнее см. документ «ViPNet SIES MC. Установка и обслуживание».

Срок действия текущего прикладного мастер-ключа ViPNet SIES вы можете узнать, выбрав на панели навигации раздел **Сертификаты и ключи** .

Управление парными связями

Добавление парной связи для защищаемого устройства

Вы можете организовать обмен защищенными данными между защищаемыми устройствами, добавив парную прикладную связь, информация о которой будет храниться на SIES-узлах взаимодействующих защищаемых устройств. Перед добавлением связи выберите сценарий защиты данных индустриальной системы. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Рисунок 18. Парная связь между защищаемыми устройствами

Внимание! Перед добавлением прикладной парной связи с назначением **Шифрование и проверка электронной подписи** настройте прикладную ключевую подсистему SIES-узла для использования сертификатов (на стр. 36).

Чтобы добавить парную связь между защищаемыми устройствами:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Нажмите **Добавить** > **Парная связь**.

6 В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации логических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

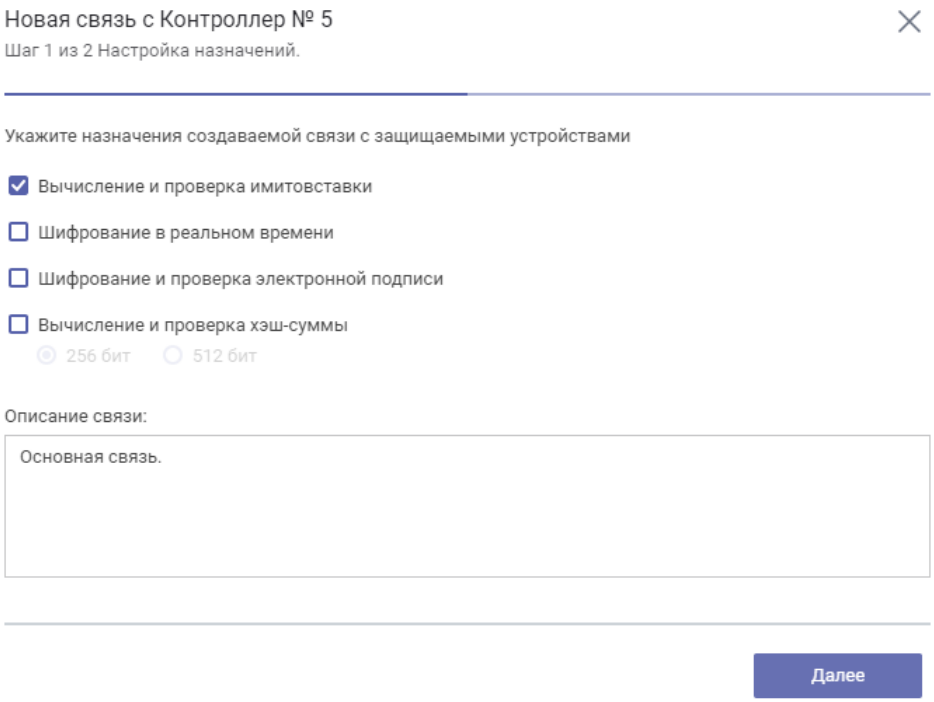

Рисунок 19. Задание атрибутов связи

Нажмите кнопку **Далее**.

7 Установите флажки слева от наименований тех защищаемых устройств или их групп, связи с которыми вы добавляете. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Примечание. Если защищаемое устройство, для которого вы добавляете связь, входит в группу, выбранную вами в качестве взаимодействующей стороны, то связь «самого с собой» для защищаемого устройства добавлена не будет. Для добавления связи защищаемого устройства «самого с собой» отдельно выберите то же защищаемое устройство в качестве взаимодействующей стороны.

Нажмите кнопку **Готово**.

Совет. Чтобы добавить связи между несколькими защищаемыми устройствами, зарегистрированными в ViPNet SIES MC, воспользуйтесь соответствующей возможностью одновременного управления несколькими защищаемыми устройствами (на стр. 100).

Добавление парной связи для группы защищаемых устройств

Вы можете организовать обмен защищенными данными между выбранными защищаемыми устройствами или их группами и другими защищаемыми устройствами, добавив между ними парные прикладные связи. Перед добавлением связей выберите сценарий защиты данных индустриальной системы. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Рисунок 20. Добавление парных связей для выбранных защищаемых устройств

Внимание! Перед добавлением прикладной парной связи с назначением **Шифрование и проверка электронной подписи** настройте прикладную ключевую подсистему SIES-узла для использования сертификатов (на стр. 36).

Чтобы добавить парную связь для группы защищаемых устройств:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемые устройства или их группы, установив флажок слева от наименования каждого защищаемого устройства или группы.

4 На панели дополнительных сведений нажмите кнопку **Добавить парные связи для каждого защищаемого устройства**.

5 В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации физических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

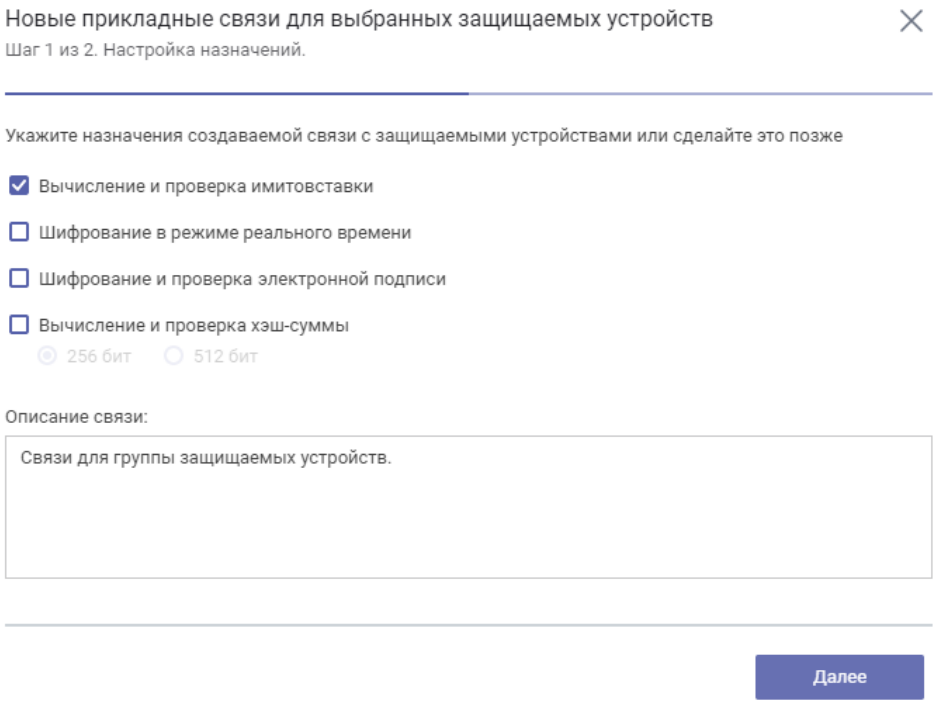

Рисунок 21. Задание атрибутов связи

Нажмите кнопку **Далее**.

6 Установите флажки слева от наименований тех защищаемых устройств или их групп, связи с которыми вы добавляете. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Примечание. Если защищаемое устройство, для которого вы добавляете связь, входит в группу, выбранную вами в качестве другой взаимодействующей стороны, то связь «самого с собой» для защищаемого устройства добавлена не будет. Для добавления связи защищаемого устройства «самого с собой» отдельно выберите то же защищаемое устройство в качестве взаимодействующей стороны.

Нажмите кнопку **Готово**.

Добавление парных связей между выбранными защищаемыми устройствами

Вы можете организовать обмен защищенными данными между выбранными защищаемыми устройствами или защищаемыми устройствами, помещенными в выбранную группу, добавив между ними парные прикладные связи. Перед добавлением связей выберите сценарий защиты данных индустриальной системы. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Рисунок 22. Добавление парных связей между выбранными защищаемыми устройствами

Внимание! Перед добавлением прикладной парной связи с назначением **Шифрование и проверка электронной подписи** настройте прикладную ключевую подсистему SIES-узла для использования сертификатов (на стр. 36).

Чтобы добавить парную связь для группы защищаемых устройств:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемые устройства или их группы, установив флажок слева от наименования каждого защищаемого устройства или группы.

4 На панели дополнительных сведений нажмите кнопку **Добавить парные связи между всеми выбранными устройствами**.

5 В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации физических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

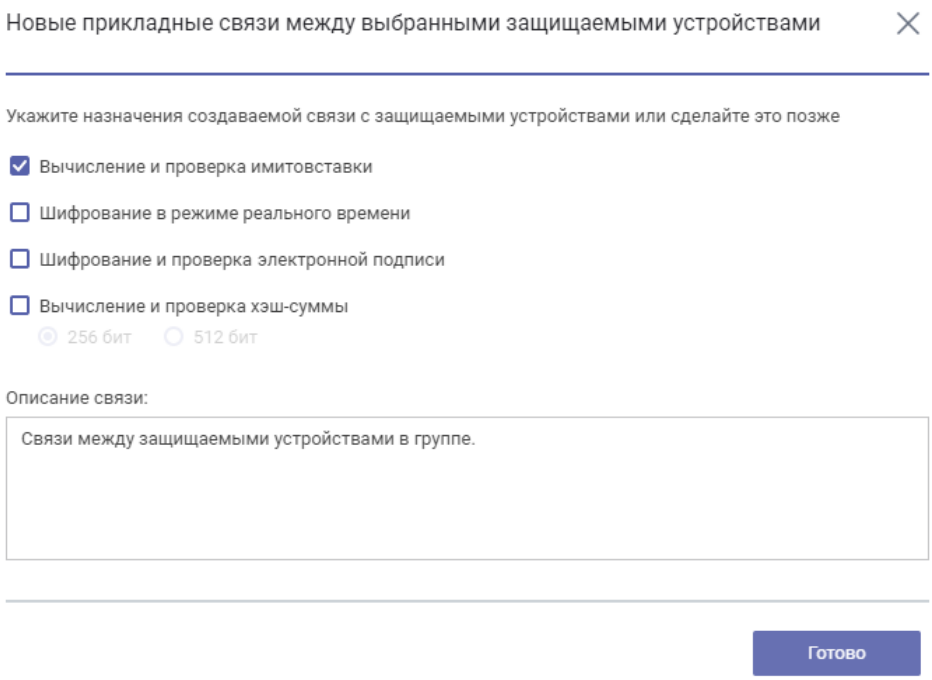

Рисунок 23. Задание атрибутов связи

Нажмите кнопку **Готово**.

Управление резервированными парными связями

Криптографическая обработка данных на резервных защищаемых устройствах реализована с помощью резервированных парных прикладных связей. Резервированные парные связи добавляются с помощью ViPNet SIES MC между взаимодействующими защищаемыми устройствами по аналогии с парными связями.

В отличие от парных связей, по которым взаимодействует по одному защищаемому устройству с каждой стороны, по резервированным парным связям с каждой стороны могут взаимодействовать основные и резервные защищаемые устройства, входящие в резервированные группы.

Количество резервированных групп, взаимодействующих в одной резервированной парной связи, не может быть больше двух. Между защищаемыми устройствами, входящими в резервированные группы, не должно быть парных связей.

Добавление резервированной парной связи

Если в индустриальной системе применяется резервирование защищаемых устройств, вы можете использовать функции SIES-узлов по криптографической обработке данных на резервных защищаемых устройствах.

Чтобы организовать криптографическую обработку данных между двумя защищаемыми устройствами, хотя бы одно из которых входит в резервированную группу, добавьте в ViPNet SIES MC резервированную парную связь. При добавлении резервированной парной связи в состав участников связи следует включить все защищаемые устройства, входящие в резервированные группы на обеих взаимодействующих сторонах.

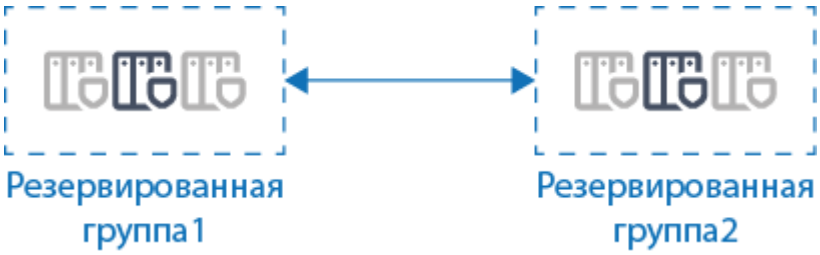

Рисунок 24. Резервированная парная связь между защищаемыми устройствами

Внимание! Для каждого защищаемого устройства вы можете использовать до двух резервных защищаемых устройств с интегрированными ViPNet SIES Core или с установленными ViPNet SIES Unit.

Между защищаемыми устройствами нельзя добавить резервированную парную связь, если между ними уже есть парная связь и наоборот.

Перед добавлением резервированной парной связи зарегистрируйте резервные защищаемые устройства (на стр. 101).

Чтобы добавить резервированную парную связь между защищаемыми устройствами:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Нажмите **Добавить** > **Резервированная парная связь**.

6 В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации физических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

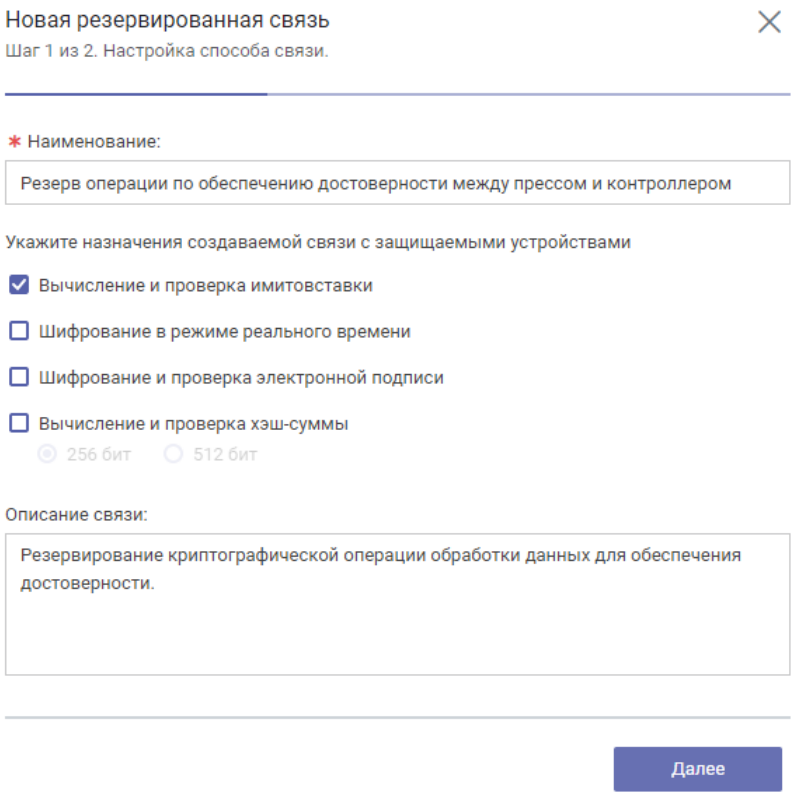

Рисунок 25. Задание атрибутов связи

Нажмите кнопку **Далее**.

7 Установите флажки слева от наименований тех защищаемых устройств или их групп, связи с которыми вы добавляете. Вам следует выбрать основное и резервные защищаемые устройства. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Нажмите кнопку **Далее**.

8 Ознакомьтесь со списком защищаемых устройств, взаимодействующих в резервированной парной связи.

Нажмите кнопку **Готово**.

Добавление защищаемого устройства в резервированную парную связь

Вы можете добавить защищаемое устройство в существующую резервированную парную связь, например, если к основному добавилось новое резервное защищаемое устройство.

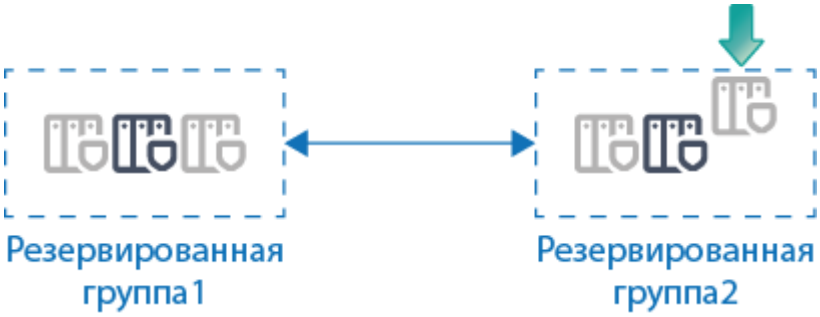

Рисунок 26. Добавление защищаемого устройства в резервированную парную связь

Чтобы добавить защищаемое устройство в резервированную парную связь:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство, участвующее в нужной резервированной парной связи.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Переключите текущее представление списка связей на отображение резервированных парных связей, нажав кнопку .

6 Щелкните по резервированной парной связи, в состав которой нужно добавить нового участника.

7 На раскрывшейся панели нажмите кнопку **Свойства связи**.

8 Перейдите на вкладку **Защищаемые устройства**.

9 Нажмите кнопку **Добавить**.

10 Установите флажки слева от наименований тех защищаемых устройств или их групп, которые нужно включить в состав резервированной парной связи. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Нажмите кнопку **Далее**.

11 Ознакомьтесь со списком добавляемых защищаемых устройств и нажмите кнопку **Готово**.

12 Закройте окно **Свойства резервированной связи**.

Исключение защищаемого устройства из резервированной парной связи

Вы можете исключить защищаемое устройство из существующей резервированной парной связи, например, если защищаемое устройство исключено из числа резервных.

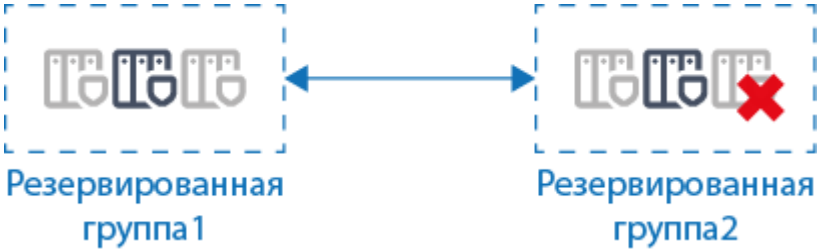

Рисунок 27. Исключение защищаемого устройства из резервированной парной связи

Чтобы исключить участника из резервированной парной связи:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство, участвующее в нужной резервированной парной связи.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Переключите текущее представление списка связей на отображение резервированных парных связей, нажав кнопку .

6 Щелкните по резервированной парной связи, из состава которой нужно удалить участника.

7 На раскрывшейся панели нажмите кнопку **Свойства связи**.

8 Перейдите на вкладку **Защищаемые устройства**.

9 Установите флажки слева от наименований тех защищаемых устройств или их групп, которые нужно исключить из состава резервированной парной связи. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

10 Нажмите кнопку .

11 Нажмите кнопку **Да**.

12 Закройте окно **Свойства резервированной связи**.

Управление мультивещательными связями

Добавление мультивещательной связи для защищаемого устройства

Вы можете организовать обмен защищенными данными между определенным множеством защищаемых устройств, добавив мультивещательную прикладную связь, информация о которой будет храниться на SIES-узлах взаимодействующих защищаемых устройств. Перед добавлением связи выберите сценарий защиты данных индустриальной системы. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Рисунок 28. Мультивещательная связь между защищаемыми устройствами

Чтобы добавить мультивещательную связь между защищаемыми устройствами:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Нажмите **Добавить** > **Мультивещательная связь**.

6 Задайте **Мультивещательный адрес**, на который защищаемые устройства — участники мультивещательной связи будут публиковать защищенные сообщения.

   Мультивещательный адрес должен быть уникальным для всего пространства адресов, используемых в прикладных связях. Длина значения — до 128 символов: буквы русского и латинского алфавита, специальные символы «_», «–», «(», «)», «\», «|», «/», «:», «.» и цифры.

   Наименование добавляемой связи по умолчанию совпадает с мультивещательным адресом, но вы можете изменить значение по своему усмотрению.

Новая мультивещательная связь с Контроллер № 5

Шаг 1 из 3. Настройка способа связи.

* Мультивещательный адрес:

1234-5678

* Наименование:

Обеспечение целостности

Укажите назначения создаваемой связи с защищаемыми устройствами

☑ Вычисление и проверка имитовставки

☐ Шифрование в режиме реального времени

Описание связи:

Основная связь.

Далее

Рисунок 29. Задание атрибутов связи

В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации физических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

Нажмите кнопку **Далее**.

7 Установите флажки слева от наименований тех защищаемых устройств или их групп, связи с которыми вы добавляете. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Примечание. Если состав участников мультивещательной связи неизвестен, вы можете пропустить этот шаг.

Нажмите кнопку **Далее**.

8 Установите флажки слева от наименований тех защищаемых устройств, которые смогут отправлять сообщения другим участникам мультивещательной связи.

Нажмите кнопку **Готово**.

Добавление мультивещательной связи для группы защищаемых устройств

Вы можете организовать обмен защищенными данными между выбранными защищаемыми устройствами или их группами, добавив мультивещательную прикладную связь. Перед добавлением связи выберите сценарий защиты данных индустриальной системы. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Чтобы добавить мультивещательную связь для группы защищаемых устройств:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите группу защищаемых устройств.
4. Для добавления мультивещательной связи между защищаемыми устройствами в выбранных группах на панели дополнительных сведений нажмите кнопку **Добавить мультивещательную связь**.
5. Задайте **Мультивещательный адрес**, на который защищаемые устройства — участники мультивещательной связи будут публиковать защищенные сообщения.

   Мультивещательный адрес должен быть уникальным для всего пространства адресов, используемых в прикладных связях. Длина значения — до 128 символов: буквы русского и латинского алфавита, специальные символы «_», «–», «(», «)», «\», «|», «/», «:», «.» и цифры.

   Наименование добавляемой связи по умолчанию совпадает с мультивещательным адресом, но вы можете изменить значение по своему усмотрению.

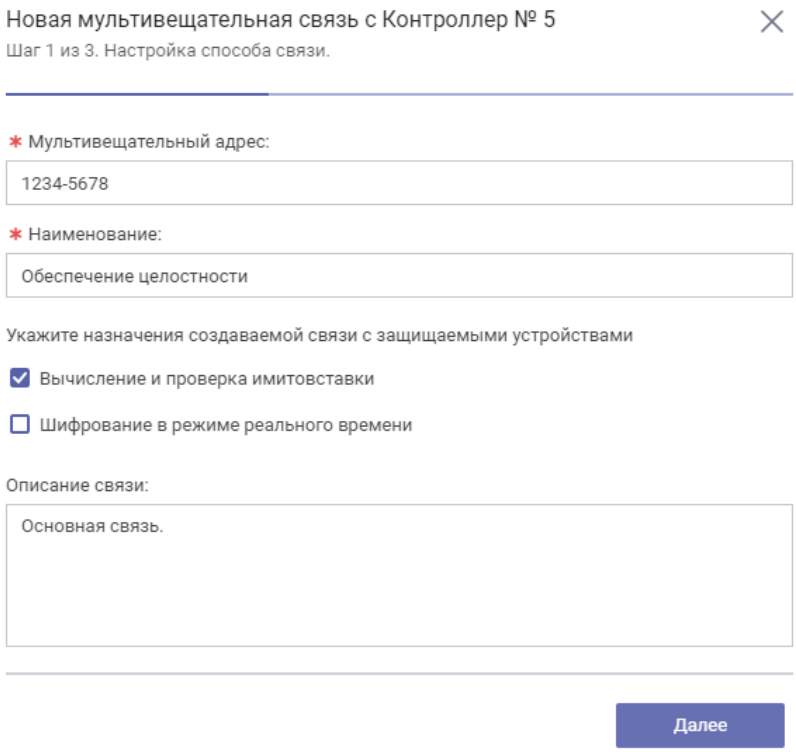

Рисунок 30. Задание атрибутов связи

В зависимости от потребностей в криптографической обработке данных задайте назначения добавляемой связи, установив флажки, соответствующие выбранным назначениям.

Примечание. Назначения добавленной связи можно задать позже, если связь добавляется для регистрации физических связей между защищаемыми устройствами.

В поле **Описание связи** вы можете ввести необязательный комментарий, характеризующий добавляемую прикладную связь.

Нажмите кнопку **Далее**.

6 Установите флажки слева от наименований тех защищаемых устройств, которые смогут отправлять сообщения другим участникам мультивещательной связи. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

7 Нажмите кнопку **Готово**.

Добавление участника мультивещательной связи

Вы можете добавить участника в существующую мультивещательную связь, например, если в сценарии защиты данных участвует новое защищаемое устройство.

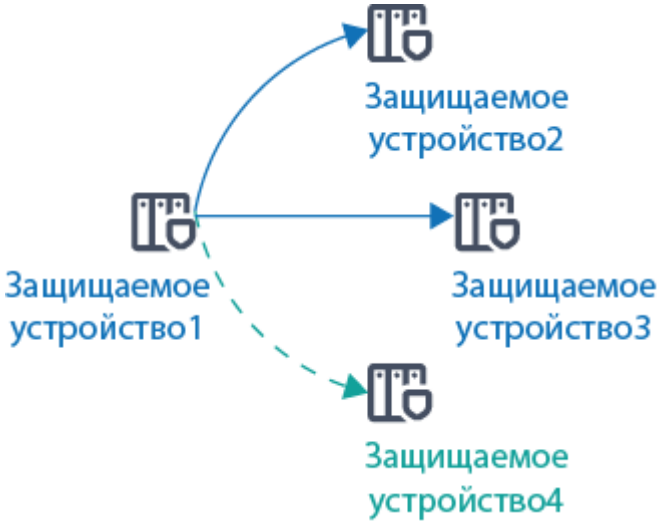

Рисунок 31. Добавление участника мультивещательной связи

Чтобы добавить участника в мультивещательную связь:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство, участвующее в нужной мультивещательной связи, или предварительно воспользуйтесь поиском на панели инструментов страницы.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Переключите текущее представление списка связей на отображение мультивещательных связей, нажав кнопку .

6 Щелкните по мультивещательной связи, в состав которой нужно добавить нового участника.

7 На раскрывшейся панели нажмите кнопку **Свойства связи**.

8 Перейдите на вкладку **Защищаемые устройства**.

9 Нажмите кнопку **Добавить**.

10 Установите флажки слева от наименований тех защищаемых устройств или их групп, которые нужно включить в состав участников мультивещательной связи. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.

Нажмите кнопку **Далее**.

11 Если выбранное защищаемое устройство должно иметь возможность отправки данных другим участникам мультивещательной связи, установите флажок слева от наименования защищаемого устройства.

Нажмите кнопку **Готово**.

12 Закройте окно **Свойства мультивещательной связи**.

Исключение участника мультивещательной связи

Вы можете исключить участника из существующей мультивещательной связи, например, если защищаемое устройство исключено из сценария защиты данных.

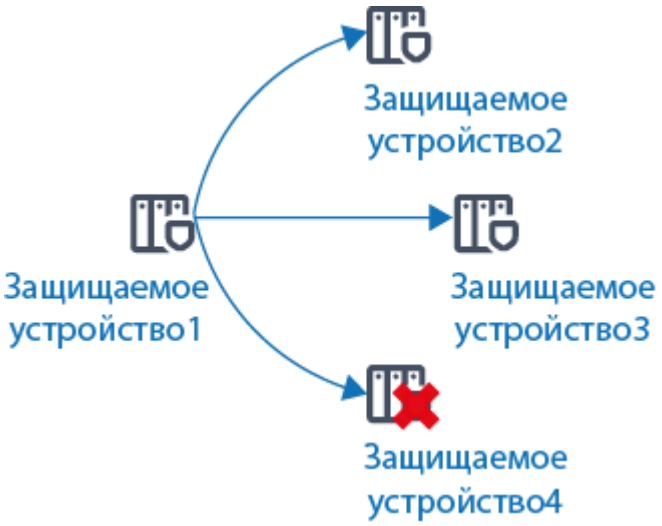

Рисунок 32. Исключение участника из мультивещательной связи

Чтобы исключить участника из мультивещательной связи:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство, участвующее в нужной мультивещательной связи, или предварительно воспользуйтесь поиском на панели инструментов страницы.
4. На панели дополнительных сведений перейдите на вкладку **Связи**.
5. Переключите текущее представление списка связей на отображение мультивещательных связей, нажав кнопку .
6. Щелкните по мультивещательной связи, из состава которой нужно удалить участника.
7. На раскрывшейся панели нажмите кнопку **Свойства связи**.
8. Перейдите на вкладку **Защищаемые устройства**.
9. Установите флажки слева от наименований тех защищаемых устройств или их групп, которые нужно исключить из состава участников мультивещательной связи. Чтобы выбрать все защищаемые устройства или их группы, установите флажок слева от заголовка **Защищаемое устройство**.
10. Нажмите кнопку .
11. Нажмите кнопку **Да**.
12. Закройте окно **Свойства мультивещательной связи**.

Изменение списка отправителей в мультивещательной связи

Вы можете изменить состав участников, обладающих правом отправки данных другим участникам существующей мультивещательной связи, например, при изменении сценария защиты данных в индустриальной системе.

Чтобы изменить состав отправителей мультивещательной связи:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Защищаемые устройства** .
3. Выберите защищаемое устройство, участвующее в нужной мультивещательной связи, или предварительно воспользуйтесь поиском на панели инструментов страницы.
4. На панели дополнительных сведений перейдите на вкладку **Связи**.
5. Переключите текущее представление списка связей на отображение мультивещательных связей, нажав кнопку .
6. Щелкните по мультивещательной связи, состав отправителей которой нужно изменить.
7. На раскрывшейся панели нажмите кнопку **Свойства связи**.
8. Перейдите на вкладку **Защищаемые устройства**.
9. В графе **Отправка данных записи** установите переключатели защищаемых устройств:
   - для запрещения отправлять данные другим участникам мультивещательной связи — в положение **Запретить**;

   Внимание! В составе связи должен быть хотя бы один участник с правом отправки сообщений.

   - для разрешения отправлять данные другим участникам мультивещательной связи — в положение **Разрешить**.

   Нажмите кнопку **Сохранить**.
10. Нажмите кнопку **Да**.

Просмотр связей

Вы можете просматривать связи защищаемого устройства, например, чтобы проверить состояние синхронизации связей.

Чтобы просмотреть связи, добавленные для защищаемого устройства:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

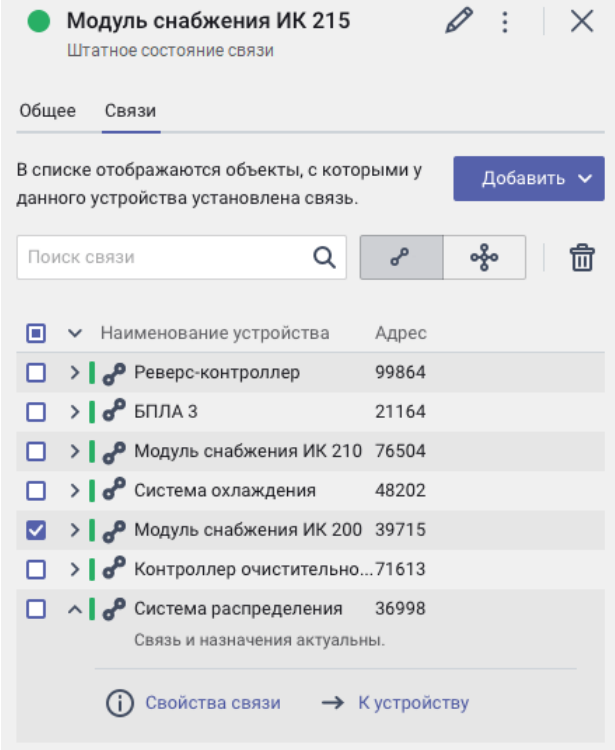

Рисунок 33. Заданные связи защищаемого устройства

5 Просмотрите прикладные связи, добавленные для защищаемого устройства.

С помощью кнопок вы можете переключать текущее представление списка связей между отображением парных или мультивещательных и резервированных парных связей.

Общие состояния связей помечаются следующими цветами:

— все назначения связи в нормальном состоянии;

— хотя бы у одного назначения связи есть проблемы (например, изменилось назначение связи): следует выполнить синхронизацию связи для восстановления криптографической обработки данных на защищаемых устройствах);

— хотя бы одно назначение связи в критическом состоянии (например, истек срок действия связи): следует выполнить синхронизацию связи для восстановления криптографической обработки данных на защищаемых устройствах;

— состояние назначений связи не контролируется.

Чтобы просмотреть подробности текущего состояния связи, в списке связей щелкните:

- для парной связи — наименование защищаемого устройства, для взаимодействия с которым добавлена связь;
- для мультивещательной связи — наименование связи с определенным множеством защищаемых устройств.

Также в списке связей отображается:

- для парной связи — идентификатор SIES-узла, назначенного на защищаемое устройство, для взаимодействия с которым добавлена связь;
- для мультивещательной связи — мультивещательный адрес определенного множества защищаемых устройств, для взаимодействия с которыми добавлена связь

Совет. При наличии связей с состоянием, отличным от нормального, убедитесь в том, что связи синхронизированы. Если в назначениях связей выбрано **Шифрование и проверка электронной подписи**, перед синхронизацией связей убедитесь в наличии в ViPNet SIES MC действительных прикладных сертификатов SIES-узлов.

6 На раскрывшейся панели свойств прикладной связи вы можете:

- просмотреть текущее состояние связи;
- просмотреть и изменить назначения связи, щелкнув **Свойства связи**;
- перейти к параметрам удаленного защищаемого устройства или назначенного на него SIES-узла, нажав кнопку **К объекту**.

Совет. Информацию о связях вы также можете просмотреть на вкладке **Связи** панели дополнительных сведений о SIES-узле (на стр. 49).

Изменение назначений связи

В ходе эксплуатации вам может потребоваться настроить связь между защищаемыми устройствами, изменив заданные назначения, например, при изменении сценария защиты данных индустриальной системы.

Чтобы изменить назначения связи между защищаемыми устройствами:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 В списке связей щелкните по наименованию защищаемого устройства, связь с которым вам нужно настроить.

6 На раскрывшейся панели свойств прикладной связи щелкните **Свойства связи**.

7 С помощью флажков измените назначения и параметры связи.

8 Нажмите кнопку **Сохранить**.

Удаление связи

Вы можете прекратить обмен защищенными данными между защищаемыми устройствами, удалив прикладную связь.

Удаление всех связей защищаемого устройства

Чтобы удалить все связи защищаемого устройства:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 Чтобы выбрать все связи, в списке связей установите флажок слева от заголовка **Наименование связи**.

6 Нажмите кнопку .

7 Нажмите кнопку **Да**.

8 Переключите представление списка связей защищаемого устройства для отображения мультивещательных связей, нажав кнопку .

9 Повторите действия 6–7.

10 Синхронизируйте связи (на стр. 51).

В результате все связи выбранного защищаемого устройства будут расформированы.

Выборочное удаление связей защищаемого устройства

Чтобы удалить связь защищаемого устройства:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **Защищаемые устройства** .

3 Выберите защищаемое устройство.

4 На панели дополнительных сведений перейдите на вкладку **Связи**.

5 С помощью кнопок выберите нужное представление списка связей с отображением парных или мультивещательных связей.

6 Установите флажки слева от наименований удаляемых связей.

Чтобы ускорить выбор нужной связи из большого числа связей, предварительно воспользуйтесь поиском на панели инструментов.

7 Нажмите кнопку .

8 Нажмите кнопку **Да**.

9 Синхронизируйте связи (на стр. 51).

6

Управление группами защищаемых устройств и SIES-узлов

О группах 128

Создание группы 131

Просмотр группы 133

Перемещение элемента в группу 134

Изменение параметров группы 136

Удаление элемента из группы 137

Удаление группы 138

О группах

Группы позволяют облегчить управление большим количеством SIES-узлов и защищаемых устройств. Выделение SIES-узлов и защищаемых устройств в отдельные группы дает следующие преимущества:

- упрощение поиска и выбора нужного SIES-узла или защищаемого устройства;
- применение однотипных операций управления одновременно ко всем однотипным элементам группы.

Вы можете объединить в группы защищаемые устройства и назначенные на них SIES-узлы. Например, вы можете сгруппировать защищаемые устройства и SIES-узлы по следующим признакам:

- размещение на одном и том же индустриальном объекте или технологическом участке;
- управление единым технологическим процессом;
- отношение к единому сегменту индустриальной системы;
- проведение регламентного обслуживания в один и тот же срок;
- управление единым администратором группы.

Каждая группа может содержать следующие элементы:

- SIES-узлы;
- защищаемые устройства;
- подгруппы, содержащие вышеперечисленные элементы.

С помощью групп формируется иерархическое представление всех SIES-узлов и защищаемых устройств, зарегистрированных в ViPNet SIES MC.

Примечание. Элементы, помещенные в группу, нельзя одновременно поместить в другую группу.

В отсутствие групп все SIES-узлы и защищаемые устройства, добавляемые в ViPNet SIES MC, помещаются в группу **Нераспределенные элементы** в представлении **Все элементы**. Также в представление **Все элементы** помещаются все группы, создаваемые в ViPNet SIES MC. Представление **Все элементы** и группу **Нераспределенные элементы** удалить нельзя.

Супер-администратор или администратор MC может создать группу в ViPNet SIES MC и поместить в новую группу SIES-узлы и защищаемые устройства из группы **Нераспределенные элементы**. Для удобства управления в новой группе можно создавать подгруппы.

Представление **Все элементы** позволяет администратору просмотреть список всех SIES-узлов и защищаемых устройств, полномочие на управление которыми делегировано администратору. Представление включает в себя следующие элементы:

- нераспределенные;
- помещенные в группы.

Каждой группой может управлять администратор группы. Полномочие управлять группой делегируется супер-администратором или администратором безопасности тому администратору группы, которому назначена данная группа. Полномочие управления группой распространяется на все элементы делегированной группы, включая подгруппы. Администратор группы может менять иерархию подчинения подгрупп только в рамках той группы наивысшего уровня, полномочие управления которой делегировано администратору группы.

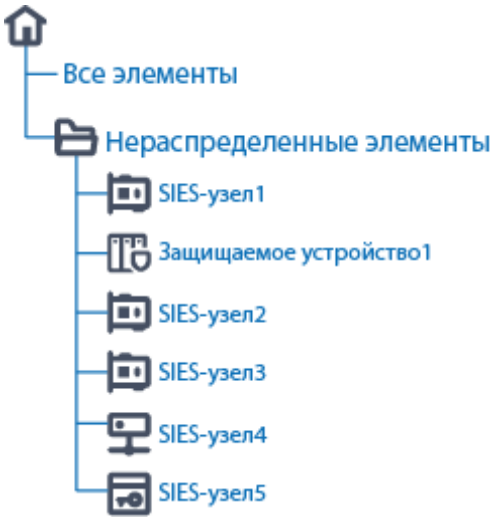

Рисунок 34. Представление элементов для всех администраторов до создания группы и делегирования полномочий управления

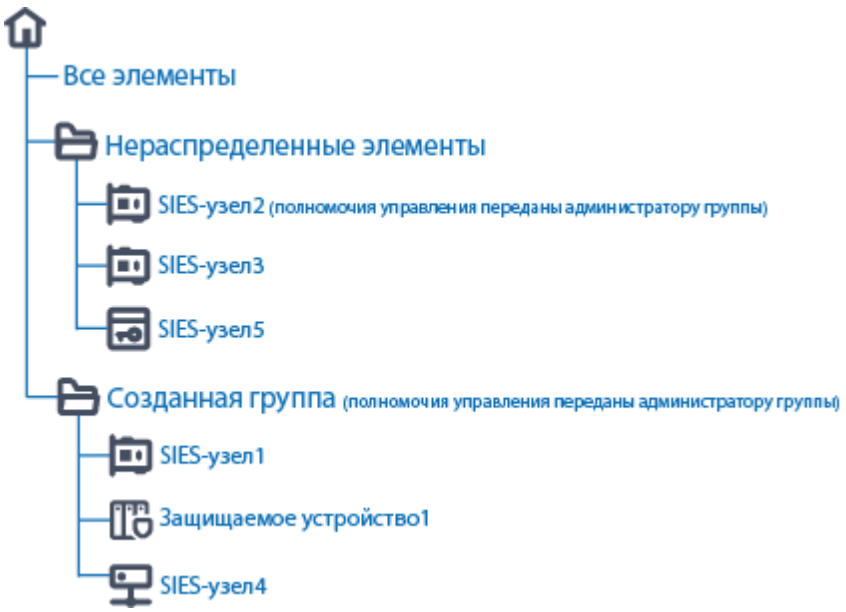

Рисунок 35. Представление элементов для супер-администраторов после создания группы и делегирования полномочий управления администратору группы

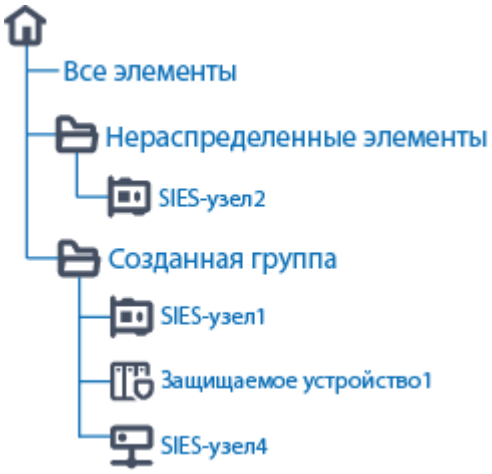

Рисунок 36. Представление элементов для администратора группы после создания группы и делегирования полномочий управления

Если сотрудник совмещает функции администратора группы с функциями оператора ViPNet SIES Workstation, то после инициализации ViPNet SIES Core администратор группы автоматически получит полномочие управлять данным ViPNet SIES Core. Новый SIES-узел будет помещен в группу **Нераспределенные элементы** для данного администратора группы, если SIES-узел предварительно не был добавлен в определенную группу ViPNet SIES MC.

Для добавления прикладных связей между защищаемыми устройствами в разных группах администратор должен обладать полномочиями управления данными группами.

Отдельные операции управления можно выполнять одновременно с несколькими группами защищаемых устройств и SIES-узлов.

Создание группы

Перед распределением SIES-узлов и защищаемых устройств по группам создайте в ViPNet SIES MC нужные группы.

Чтобы создать группу:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** или **Защищаемые устройства**.

3 Щелкните **Добавить** > **Группу**.

4 Появится окно **Создание группы**.

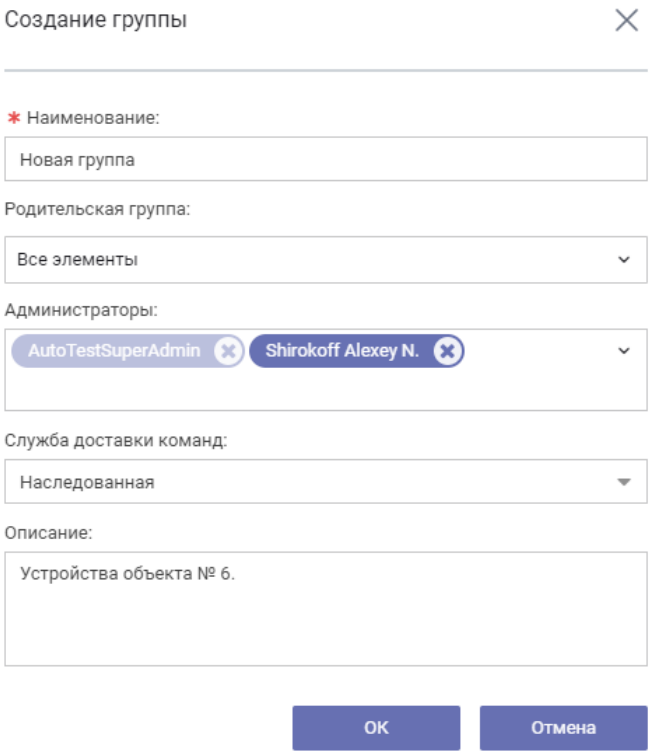

Рисунок 37. Атрибуты создаваемой группы

- В поле **Наименование** задайте имя добавляемой группы.
- Если создаваемую группу нужно сделать подгруппой не текущей группы ViPNet SIES MC, в списке **Родительская группа** выберите нужную группу.
- Если вы подключились к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, то в списке **Администраторы** вы можете выбрать администраторов групп, которым делегируете полномочия управления создаваемой группой.

- Настройки службы доставки защищенных конвертов ViPNet SIES MC для создаваемой группы наследуются от родительской группы. Если для элементов группы нужно задать другую службу доставки защищенных конвертов ViPNet SIES MC, выберите службу доставки в списке **Служба доставки команд**. Подробнее о настройке службы доставки см. документ «ViPNet SIES MC. Установка и обслуживание».
- В поле **Описание** вы можете задать любое наименование, которое облегчит вам идентификацию созданной группы.

5 Нажмите кнопку **OK**.

Просмотр группы

Чтобы просмотреть состав группы:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC, администратора группы или аудитора.

2 Перейдите в раздел **SIES-узлы** или **Защищаемые устройства**.

3 Перейдите в группу одним из следующих способов:

- нажмите кнопку и в открывшемся списке щелкните по нужной группе;
- щелкая по наименованиям групп на странице, перейдите по структуре к нужной группе.

Примечание. Щелчок по строке группы на странице открывает свойства выбранной группы на панели дополнительной информации. Двойной щелчок по строке группы открывает состав группы также, как щелчок по наименованию группы.

4 Просмотрите состав выбранной группы.

С помощью кнопок вы можете переключать текущее представление элементов на странице между отображением в виде сквозного списка или в виде структуры групп.

В зависимости от выбранного раздела одновременно в группах вы можете просматривать только SIES-узлы или защищаемые устройства.

Чтобы просмотреть все элементы в выбранной и подчиненных группах, полномочия управления которыми вам делегированы, воспользуйтесь представлением в виде сквозного списка элементов.

Совет. Для быстрого перехода в другую группу, расположенную на одном из вышестоящих уровней иерархии, вы можете использовать кнопки в строке навигации по группам.

Перемещение элемента в группу

В каждую группу вы можете поместить следующие элементы:

- SIES-узлы;
- защищаемые устройства;
- другие группы (вкладывать группы друг в друга можно на глубину до десяти уровней).

Внимание! Перемещение групп может повлиять на доступность групп для других администраторов, которым делегированы полномочия управления ими наравне с вами.

Чтобы поместить элементы в группу:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** или **Защищаемые устройства**.

3 Выберите элемент.

Примечание. Следует по отдельности перемещать элементы, расположенные на разных уровнях иерархии (например, вложенные группы).

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

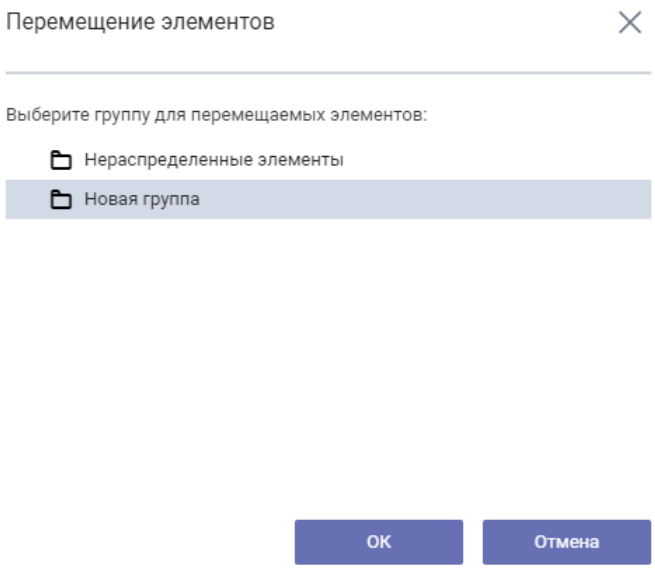

Рисунок 38. Выбор целевой группы

Примечание. Если SIES-узел назначен на защищаемое устройство, то при перемещении в выбранную группу будет перемещен как SIES-узел, так и защищаемое устройство.

5 Выберите целевую группу для перемещаемого элемента и нажмите кнопку **OK**.

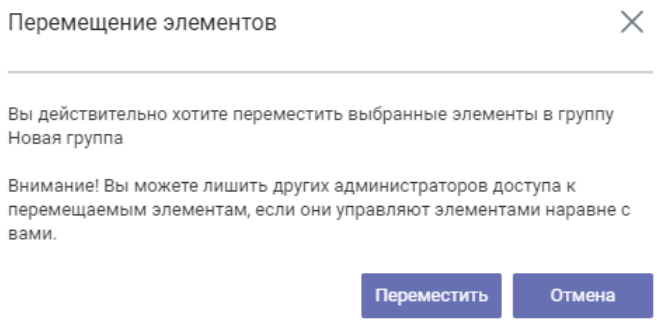

Рисунок 39. Предупреждение о нарушении полномочий управления

6 Ознакомьтесь с информацией и нажмите кнопку **Переместить**.

Совет. Вы можете поместить в группу несколько элементов одновременно. Установите флажки слева от наименований элементов. Чтобы выбрать все элементы, установите флажок слева от заголовка **Наименование**. Затем нажмите кнопку **Переместить** на панели дополнительных сведений.

Изменение параметров группы

Вы можете изменить параметры группы, например, если полномочия управления группой нужно делегировать другому администратору.

Чтобы изменить параметры группы:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **SIES-узлы** или **Защищаемые устройства**.
3. Одним из следующих способов перейдите в вышестоящую группу той группы, параметры которой нужно изменить:
   - нажмите кнопку и в открывшемся списке щелкните по нужной вышестоящей группе;
   - щелкая по наименованиям групп на странице, перейдите по структуре к нужной вышестоящей группе.
4. Щелкните по группе, параметры которой нужно изменить.
5. На панели дополнительных сведений нажмите кнопку .
6. Измените параметры группы и для сохранения изменений нажмите кнопку **OK**.

Удаление элемента из группы

При изменении структуры элементов ViPNet SIES MC вам может потребоваться удалить отдельные элементы из группы, не удаляя элементы из ViPNet SIES MC.

Чтобы сохранить возможность управления неиспользуемыми элементами, переместите (на стр. 134) выбранные элементы в другую группу, например, в группу **Нераспределенные элементы**.

Удаление группы

При изменении структуры элементов ViPNet SIES MC вы можете удалить ненужные группы.

Чтобы удалить группу:

1 Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.

2 Перейдите в раздел **SIES-узлы** или **Защищаемые устройства**.

3 Выберите группу.

Примечание. Следует по отдельности удалять элементы, расположенные на разных уровнях иерархии (например, вложенные группы).

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

Примечание. Вне зависимости от выбранного раздела будут удалены только SIES-узлы, исключенные из управления ViPNet SIES MC.

5 Подтвердите удаление, нажав кнопку **Да**.

Совет. Вы можете удалить несколько групп одновременно. Установите флажки слева от наименований удаляемых групп. Чтобы выбрать все группы, установите флажок слева от заголовка **Наименование**. Для удаления щелкните **Удалить** на панели дополнительных сведений.

7

Визуальное отображение SIES-узлов и прикладных связей

О структурной схеме индустриальной системы 140

Просмотр состояния SIES-узла 141

Просмотр состояния прикладной связи защищаемого устройства 142

О структурной схеме индустриальной системы

Структурная схема индустриальной системы в разделе **Инфраструктура** позволяет визуально следить за состоянием SIES-узлов и прикладных связей между защищаемыми устройствами, а также получать основные сведения об отображаемых элементах.

Структурная схема индустриальной системы показывает следующее:

- все защищаемые устройства, зарегистрированные в ViPNet SIES MC;
- SIES-узлы, назначенные на защищаемые устройства;
- текущее состояние SIES-узлов;
- прикладные связи между защищаемыми устройствами;
- текущее состояние прикладных связей между защищаемыми устройствами;
- основные сведения о каждом из вышеперечисленных элементов.

Защищаемые устройства и SIES-узлы отображаются на схеме в соответствии с полномочиями управления, делегированными администратору.

Текущее состояние SIES-узлов и прикладных связей отображается соответствующим цветом. Подробнее см. раздел Просмотр сведений о SIES-узле (на стр. 26) и Просмотр связей (на стр. 122).

Просмотр состояния SIES-узла

С помощью структурной схемы индустриальной системы вы можете следить за состоянием и просматривать свойства SIES-узлов.

Чтобы просмотреть состояние и свойства SIES-узла:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Инфраструктура** .
3. Для обновления схемы нажмите клавиши **Ctrl+R**.
4. На структурной схеме щелкните защищаемое устройство с назначенным SIES-узлом.

Совет. Наименование и адрес защищаемого устройства отображаются во всплывающей подсказке при наведении мыши на значок защищаемого устройства.

---

5. На панели дополнительных сведений ознакомьтесь со свойствами и состоянием SIES-узла.

   Для перехода к управлению SIES-узлом в разделе **Назначенные SIES-узлы** щелкните по идентификатору SIES-узла и на панели дополнительных сведений нажмите кнопку **К объекту**.

Просмотр состояния прикладной связи защищаемого устройства

С помощью структурной схемы индустриальной системы вы можете следить за состоянием прикладных связей между защищаемыми устройствами.

Чтобы просмотреть состояние прикладной связи между защищаемыми устройствами:

1. Подключитесь к веб-интерфейсу ViPNet SIES MC с полномочиями супер-администратора, администратора MC или администратора группы.
2. Перейдите в раздел **Инфраструктура** .
3. Для обновления схемы нажмите клавиши **Ctrl+R**.
4. На структурной схеме щелкните прикладную связь или защищаемое устройство, для которого добавлена искомая прикладная связь.
5. На панели дополнительных сведений ознакомьтесь со свойствами и состоянием прикладной связи.

A

Параметры SIES-узла

В разделе **SIES-узлы** отображаются основные параметры SIES-узлов, функционирующих в индустриальной системе и зарегистрированных в ViPNet SIES MC.

Дополнительные параметры SIES-узлов отображаются на вкладках панели дополнительной информации.

Основные параметры

В строке списка на странице **Зарегистрированные SIES-узлы** приводятся следующие параметры SIES-узла:

1 **Режим** — содержит текущий режим работы SIES-узла. ViPNet SIES MC отображает следующие режимы работы SIES-узла:

- **Инициализация** — режим активируется после приведения SIES-узла к заводскому состоянию (на стр. 66);
- **Конфигурирование** — режим используется для регламентного обслуживания SIES-узла, вы можете активировать этот режим (на стр. 30);
- **Штатный** — режим используется для выполнения криптографических операций с данными защищаемого устройства, вы можете активировать этот режим (на стр. 30);
- **Блокировка** — режим используется для запрещения выполнения криптографических операций с данными защищаемого устройства, вы можете активировать этот режим (на стр. 30).

2 **Управление** — содержит текущий режим управления SIES-узлом из ViPNet SIES MC. В ViPNet SIES MC предусмотрены следующие режимы управления SIES-узлом:

- **Не инициализирован** — режим устанавливается для всех SIES-узлов, добавленных (на стр. 16) в ViPNet SIES MC, но не прошедших инициализацию.
- **Удаленное** — режим устанавливается для SIES-узлов, эксплуатируемых в составе защищаемых устройств. Управление SIES-узлами выполняется из ViPNet SIES MC по каналам связи индустриальной системы.

  Вы можете активировать удаленное управление SIES-узлом (на стр. 32).
- **Локальное** — режим устанавливается для SIES-узлов, недоступных по каналам связи индустриальной системы. Управление SIES-узлами выполняется путем передачи команд ViPNet SIES MC через ViPNet SIES Workstation.

  Вы можете активировать локальное управление SIES-узлом (на стр. 32).
- **Ручное** — режим устанавливается для SIES-узлов типа **Пользователь** или **Другой** без поддержки на защищаемом устройстве управления SIES-узлом из ViPNet SIES MC.
- **Исключен из управления** — режим устанавливается для SIES-узлов, временно выведенных из управления ViPNet SIES MC для изменения топологии информационных потоков индустриальной системы или для извлечения SIES-узла из защищаемого устройства и удаления из ViPNet SIES MC. ViPNet SIES MC прекращает регистрацию любых событий SIES-узла, исключенного из управления.

  Вы можете исключить SIES-узел из управления ViPNet SIES MC (на стр. 61).

Вкладка Общее

Вкладка **Общее** панели дополнительной информации содержит параметры SIES-узла. Дополнительно отображаются параметры защищаемого устройства, на которое назначен (на стр. 98) SIES-узел.

Для просмотра дополнительных сведений о SIES-узле, нажмите кнопку . Откроется панель, содержащая следующее:

- **Версия платформы** — обозначение аппаратной платформы (на стр. 149) SIES-узла. Идентификатор аппаратной платформы используется при обновлении ПО ViPNet SIES Core (на стр. 84);
- **Версия ПО**, загруженного на SIES-узел;
- **Дата обновления ПО**.

Параметр **Контроль ДНСД** содержит состояние датчика контроля доступа к SIES-узлу, если SIES-узел оборудован датчиком.

Примечание. Работу с датчиком контроля доступа поддерживают только SIES-узлы типа **ViPNet SIES Core**.

В ViPNet SIES MC используются следующие состояния датчика контроля доступа к SIES-узлу:

- **Неизвестно** — состояние датчика контроля доступа к SIES-узлу не определено, поскольку SIES-узел не вернул информацию о состоянии в ViPNet SIES MC, — вы можете обновить состояние SIES-узла (на стр. 26);
- **Включен** — датчик контроля доступа к SIES-узлу включен по команде из ViPNet SIES MC (на стр. 72);
- **Отключен** — датчик контроля доступа к SIES-узлу отключен по команде из ViPNet SIES MC (на стр. 73).

Параметр **Контрольный код** содержит контрольный код ПО SIES-узла по результатам выполнения контроля целостности ПО.

Набор параметров **Защищаемое устройство** для ViPNet SIES Core содержит состояние связи с защищаемым устройством.

Связь с защищаемым устройством определяет принадлежность ViPNet SIES Core к конкретному защищаемому устройству индустриальной системы.

В ViPNet SIES MC используются следующие состояния связи с защищаемым устройством:

- **Связь задана** — в памяти ViPNet SIES Core сохранен серийный номер защищаемого устройства, определяющий принадлежность ViPNet SIES Core к защищаемому устройству.

- **Связь не задана** — связь ViPNet SIES Core с защищаемым устройством не задавалась или задание связи выполнить не удалось. Начальное значение, устанавливаемое ViPNet SIES MC по умолчанию для всех ViPNet SIES Core.
- **Связь задается** — команда ViPNet SIES MC по заданию связи ViPNet SIES Core с защищаемым устройством поставлена в очередь и ожидается ответ ViPNet SIES Core на команду.
- **Связь обновляется** — связь ViPNet SIES Core с защищаемым устройством задана, но поставлена в очередь новая команда ViPNet SIES MC по заданию связи ViPNet SIES Core с защищаемым устройством.

Остальные параметры защищаемого устройства вы можете задать (на стр. 97), щелкнув по наименованию защищаемого устройства.

Раздел параметров **Состояние ключевой подсистемы** отображает общее состояние служебной и прикладной ключевых подсистем SIES-узла.

В ViPNet SIES MC используются следующие состояния ключевых подсистем SIES-узла:

- **Нормальное** — ключевая подсистема SIES-узла настроена и действительна.
- **Есть проблемы** — немедленного вмешательства не требуется.

  Служебная ключевая подсистема — осталось менее 90 дней до истечения срока действия по крайней мере одного из сертификатов SIES-узла, используемого в защищенном взаимодействии с ViPNet SIES MC.

  Прикладная ключевая подсистема — осталось менее 90 дней до истечения срока действия по крайней мере одного из сертификатов SIES-узла, используемого в криптографической обработке данных защищаемого устройства, или по крайней мере одна прикладная связь не синхронизирована.
- **Критическое** — требуется немедленное вмешательство.

  Служебная ключевая подсистема — на SIES-узле отсутствуют действительные сертификаты, используемые в защищенном взаимодействии с ViPNet SIES MC.

  Прикладная ключевая подсистема — на SIES-узле отсутствуют действительные сертификаты, используемые в криптографической обработке данных защищаемого устройства, или истек срок действия по крайней мере одной прикладной связи.
- **Не контролируется** — SIES-узел исключен из управления администратором ViPNet SIES MC.
- **Не настроена** — состояние устанавливается для всех SIES-узлов, добавленных в ViPNet SIES MC.

  Для служебной ключевой подсистемы ViPNet SIES Core, ViPNet SIES Unit и другого SIES-узла состояние устанавливается для SIES-узлов перечисленных типов, добавленных в ViPNet SIES MC, но не прошедших инициализацию.

  Для прикладной ключевой подсистемы ViPNet SIES Core, ViPNet SIES Unit и другого SIES-узла состояние устанавливается для SIES-узлов перечисленных типов, которые не прошли инициализацию или не имеющих прикладных связей.

Более детально состояние ключевой системы SIES-узла вы можете оценить на вкладке **Сертификаты и ключи**, выбрав и просмотрев сведения об отдельных сертификатах служебной или прикладной ключевой подсистемы SIES-узла (на стр. 39).

Также здесь вы можете узнать о состоянии первичной ключевой информации ViPNet SIES Core.

Вкладка Задачи

Вкладка **Задачи** панели дополнительной информации содержит очередь задач, поставленных SIES-узлу администратором ViPNet SIES MC или автоматически ViPNet SIES MC.

Каждая задача состоит из команд управления и мониторинга, инициированных в адрес SIES-узла. Задача может включать как одну, так и несколько команд, последовательно выполняемых SIES-узлом.

Таблица 18. Состояние задачи на разных этапах обработки

Наименование состояния	Цветовое обозначение	Описание
Ожидает выполнения		Задача была создана, но еще не выполнялась.
Задача выполняется	Нет	Задача выполняется в текущий момент. Чтобы отменить задачу: 1 На вкладке **Задачи** щелкните выполняемую задачу. 2 Нажмите кнопку **Отменить задачу**.
Задача выполнена		Выполнение задачи успешно завершилось.
Ошибка выполнения		В ходе выполнения задачи возникла ошибка. Чтобы просмотреть сообщение об ошибке, на вкладке **Задачи** щелкните задачу с ошибкой выполнения.
Задача отменена		Выполнение задачи отменено администратором.

B

Аппаратные платформы ViPNet SIES Core

Соответствие аппаратной платформы и версии ViPNet SIES Core приведено в таблице ниже.

Таблица 19. Аппаратные платформы ViPNet SIES Core

Версия ViPNet SIES Core	Обозначение аппаратной платформы
1.0	ICM v4
1.5	ICM v4
1.6 и выше	SIES Core v5

C

Уровни критичности событий

В ViPNet SIES MC регистрируются все события, происходящие в ходе эксплуатации ViPNet SIES MC.

События разделяются по уровням критичности. По уровню критичности событий можно оценить 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.

D

Возможные неполадки и способы их устранения

Длительное выполнение команды

На вкладке **Задачи** панели дополнительных свойств состояние команды, отправленной на SIES-узел, длительное время отображается как **Выполняется**.

Возможная причина № 1

Задан адрес защищаемого устройства (на стр. 97), не соответствующий фактическому адресу защищаемого устройства в индустриальной системе.

Способ устранения

Задайте корректный адрес защищаемого устройства в ViPNet SIES MC и повторите команду.

Возможная причина № 2

В ViPNet SIES MC не получен ответ на команду, отправленную SIES-узлу.

Способ устранения

Проверьте корректность адреса защищаемого устройства в ViPNet SIES MC и повторите команду.

Команды не выполняются на SIES-узле

Команды ViPNet SIES MC не выполняются на SIES-узле в режиме удаленного управления.

Возможная причина

Нет связи с SIES-узлом по каналам индустриальной системы.

Способ устранения

Воспользуйтесь возможностью ручной доставки на SIES-узел команд управления ViPNet SIES MC через защищаемое устройство. Для этого выполните следующие действия:

1. Выгрузите из ViPNet SIES MC защищенный конверт с командой для SIES-узла (на стр. 56).
2. Загрузите защищенный конверт с командой на защищаемое устройство для дальнейшей трансляции защищенного конверта SIES-узлу.
3. Дождитесь окончания обработки защищенного конверта SIES-узлом.
4. С защищаемого устройства выгрузите защищенный конверт с ответом SIES-узла.
5. Загрузите защищенный конверт с ответом SIES-узла в ViPNet SIES MC (на стр. 58).

Не выполняются криптографические операции в адрес другого SIES-узла

На ViPNet SIES Core, встроенном в защищаемое устройство, не удается выполнить криптографические операции, связанные с обработкой данных в криптографических контекстах (см. глоссарий, стр. 162) в адрес SIES-узла, связь с которым задана в ViPNet SIES MC.

Подробнее о функциях, реализующих криптографические операции ViPNet SIES Core, см. документ «ViPNet SIES Core SDK. Общее описание».

Возможная причина

Не синхронизирована связь между взаимодействующими SIES-узлами.

Способ устранения

Синхронизируйте связь между SIES-узлами на обеих сторонах взаимодействия.

Не синхронизируется прикладная связь

Не удается синхронизировать связь с назначением **Шифрование и проверка электронной подписи**.

Возможная причина

На взаимодействующих SIES-узлах отсутствуют действительные прикладные сертификаты.

Способ устранения

1. Проверьте сроки действия прикладных сертификатов на SIES-узлах (на стр. 39).
2. Выпустите новые прикладные сертификаты.
3. Загрузите новые прикладные сертификаты на SIES-узлы (на стр. 42).
4. Повторите синхронизацию прикладной связи (на стр. 51).

Не полностью синхронизируются прикладные связи на ViPNet SIES Core

В результате выполнения задачи по синхронизации прикладных связей на ViPNet SIES Core выдается сообщение **Частичный успех, добавлены не все записи**.

Возможная причина

Хранилище прикладных связей ViPNet SIES Core фрагментировано. Требуется принудительная дефрагментация с помощью перезагрузки ViPNet SIES Core.

Способ устранения

1. Сообщите администратору ViPNet SIES Core о необходимости перезагрузить ViPNet SIES Core или защищаемое устройство.
2. После перезагрузки ViPNet SIES Core повторите синхронизацию прикладных связей (на стр. 51).

Ошибка выполнения задачи синхронизации прикладных связей

В ходе синхронизации прикладных связей для некоторых SIES-узлов выполнение задачи завершается с ошибкой **Отсутствуют активированные мастер-ключи**.

Возможная причина

Отсутствует прикладной симметричный мастер-ключ.

Способ устранения

Повторите синхронизацию прикладных связей (на стр. 51) для тех SIES-узлов, выполнение задачи для которых завершилось с ошибкой.

Не удается создать и загрузить сертификат на ViPNet SIES Core

При попытке создать и загрузить сертификат на ViPNet SIES Core выдается ошибка.

Возможная причина

Хранилище прикладных связей ViPNet SIES Core фрагментировано. Требуется принудительная дефрагментация с помощью перезагрузки ViPNet SIES Core.

Способ устранения

1. Сообщите администратору ViPNet SIES Core о необходимости перезагрузить ViPNet SIES Core или защищаемое устройство.
2. После перезагрузки ViPNet SIES Core повторно создайте и загрузите сертификат (на стр. 41).

E

Глоссарий

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.

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 Unit

Компонент комплекса ViPNet SIES. Программно-аппаратный или программный комплекс, размещенный на операторском уровне индустриальной системы. Интегрируется с устройствами операторского уровня индустриальной системы (SCADA, OPC и другими) и выполняет функции SIES-узла.

ViPNet SIES Workstation

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

Адрес защищаемого устройства

Уникальное обозначение защищаемого устройства в индустриальной системе, с помощью которого другие защищаемые устройства взаимодействуют с данным защищаемым устройством. Используется в парных и резервированных парных прикладных связях.

Адрес защищаемого устройства для служебных сообщений

Идентификатор защищаемого устройства, по которому ViPNet SIES MC может отправить защищенный конверт защищаемому устройству в адрес SIES-узла по каналам связи индустриальной системы.

Аутентификация

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

Датчик случайных чисел (ДСЧ)

Программный датчик, вырабатывающий псевдослучайную последовательность путем детерминированного преобразования инициализирующей последовательности (исходной ключевой информации).

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.

Идентификатор SIES-узла

Уникальное обозначение SIES-узла, позволяющее однозначно идентифицировать SIES-узел в индустриальной системе. Для ViPNet SIES Core используется 12-значный серийный номер программно-аппаратного комплекса, присвоенный изготовителем. Для ViPNet SIES Unit используется 12-значный идентификатор, присвоенный ViPNet SIES MC.

Имитовставка

Специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения контроля целостности сообщения и аутентификации источника данных сообщения.

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.

Инициализирующая последовательность

Инициализирующая последовательность (исходная ключевая информация) — совокупность данных, используемая датчиком случайных чисел для выработки псевдослучайной последовательности.

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.

Ключевая информация

Специальным образом организованная совокупность криптографических ключей, предназначенная для криптографической защиты информации в течение определенного срока времени.

Команда мониторинга

Запрос ViPNet SIES MC, направляемый SIES-узлу для получения данных о параметрах или текущем режиме работы SIES-узла.

Команда управления

Запрос ViPNet SIES MC, направляемый SIES-узлу для изменения параметров или текущего режима работы SIES-узла.

Компрометация ключей

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

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 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.

Криптографический контекст

Долговременная информация многократного использования, позволяющая выполнять криптографическую обработку данных с параметрами, определяемыми прикладными связями между взаимодействующими защищаемыми устройствами.

Мультивещательная прикладная связь

Прикладная связь для криптографической обработки данных во взаимодействии между несколькими защищаемыми устройствами.

Мультивещательный адрес

Уникальное обозначение мультивещательной прикладной связи между защищаемыми устройствами, на которое участники связи публикуют и с которого прочитывают защищенные сообщения.

Парная прикладная связь

Прикладная связь для криптографической обработки данных во взаимодействии между двумя защищаемыми устройствами.

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.

Программное обеспечение (ПО)

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

Резервированная группа

Совокупность основного и резервных защищаемых устройств, соответствующих основному.

Резервированная парная прикладная связь

Прикладная связь для криптографической обработки данных во взаимодействии защищаемых устройств в индустриальных системах с применением резервирования.

Резервное защищаемое устройство

Защищаемое устройство, предназначенное для замещения основного защищаемого устройства в случае отказа или вывода из эксплуатации.

Серийный номер защищаемого устройства

Идентификатор защищаемого устройства в системе учета объектов индустриальной системы, уникальный в рамках индустриального объекта, на котором применяется комплекс ViPNet SIES.

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.

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.

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.

Хэширование

Преобразование массива данных произвольной длины в битовую строку фиксированной длины, выполняемое определенным алгоритмом. Результат применения хэш-функции (хэш-код или хэш-сумма) однозначно определяется первоначальным массивом данных. Повторное применение хэш-функции к массиву данных и сравнение повторного хэш-кода с первоначальным хэш-кодом позволяет проверить целостность массива данных.

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.