ViPNet SIES Unit для Windows

Руководство администратора

infotecs

ФРКЕ.00237-01 32 01

Версия продукта 2.3

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

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.

Для кого предназначен документ

Документ предназначен для администраторов безопасности устройств операторского уровня индустриальной системы, использующих ViPNet SIES Unit для защиты данных.

Предполагается, что администратор обладает базовым представлением о криптографической защите данных, а также об устройстве компьютерных и индустриальных систем, опытом администрирования Windows.

Связанные документы

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

Таблица 1. Связанные документы

Документ	Содержание
ViPNet SIES Unit. Руководство разработчика	Информация по использованию ViPNet SIES Unit RESTful API для криптографической обработки данных устройства верхнего уровня индустриальной системы
ViPNet SIES Unit SDK. Общее описание	Состав комплекта средств разработки ПО ViPNet SIES Unit SDK (Software Development Kit), описание выполняемых функций и методика применения ViPNet SIES Unit SDK
ViPNet SIES. Сценарии работы	Основные сценарии работы комплекса ViPNet SIES в индустриальной системе
ViPNet SIES. Сценарии эксплуатации	Описание основных задач, возникающих в ходе эксплуатации комплекса ViPNet SIES в индустриальной системе. Каждая задача сопровождается методикой ее решения

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.
`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 ИнфоТеКС:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +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 компании ИнфоТеКС регулируется политикой ответственного разглашения.

Новые возможности версии 2.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet SIES Unit версии 2.3 по сравнению с версией 2.0.

- **Автоматическая инициализация без использования ViPNet SIES Workstation**

  Если между защищаемым устройством и ViPNet SIES MC есть канал связи TCP/IP, инициализацию ViPNet SIES Unit можно провести с использованием сертификата оператора WS, но без помощи ViPNet SIES Workstation.

  Дополнительно потребуется компьютер с развернутым рабочим местом оператора WS, если рабочее место нельзя организовать на защищаемом устройстве. Подробнее об операторе WS см. документ «ViPNet SIES MC. Общее описание».

- **Установка на отдельную аппаратную платформу**

  Если ресурсы, архитектура или операционная система защищаемого устройства не позволяют установить ПО или использовать функции установленного ViPNet SIES Unit, можно использовать отдельную аппаратную платформу для установки ViPNet SIES Unit. Защищаемое устройство будет вызывать функции ViPNet SIES Unit дистанционно через сеть TCP/IP.

- **Загрузка защищенного конверта ViPNet SIES MC через утилиту локального управления**

  В отсутствие связи между ViPNet SIES MC и ViPNet SIES Unit можно вручную загрузить защищенный конверт ViPNet SIES MC в ViPNet SIES Unit для обработки. Защищенный конверт с результатом обработки для передачи администратору ViPNet SIES MC также выгружается через утилиту локального управления.

- **Создание и обработка CRISP-сообщений в потоке**

  Для криптографических преобразований больших массивов данных в ViPNet SIES Unit реализована возможность создания и обработки CRISP-сообщений в потоке.

  Подробнее см. документы «ViPNet SIES Unit. Руководство разработчика» и «ViPNet SIES Unit SDK. Общее описание».

- **Вызов функций ViPNet SIES Unit SDK в блокирующем и неблокирующем режимах**

  Теперь функции ViPNet SIES Unit можно вызывать в блокирующем (синхронном) и неблокирующем (асинхронном) режимах с помощью нового ViPNet SIES Unit SDK. Неблокирующий режим позволяет параллельно вызывать несколько функций ViPNet SIES Unit. Реализация асинхронного режима работы потребовала изменения интерфейса вызова функций ViPNet SIES Unit SDK.

  Подробнее см. документ «ViPNet SIES Unit SDK. Общее описание».

- **Получение списка сертификатов ViPNet SIES Unit из ViPNet SIES MC**

  Администратор ViPNet SIES MC может синхронизировать информацию о хранимых сертификатах между ViPNet SIES Unit и ViPNet SIES MC.

- **Исправлены дефекты**

  В ViPNet SIES Unit версии 2.3 устранены дефекты, выявленные в предыдущей версии.

О ViPNet SIES Unit

ViPNet SIES Unit — прикладная служба для криптографических операций с данными, обрабатываемыми на устройствах верхнего уровня индустриальных (см. глоссарий, стр. 54) и IIoT–систем (см. глоссарий, стр. 52):

- SCADA-серверы (см. глоссарий, стр. 53);
- автоматизированные рабочие места операторов;
- автоматизированные рабочие места инженеров;
- серверы сбора и обработки информации IIoT–систем.

Использование ViPNet SIES Unit позволяет реализовать сценарии безопасности серверов и рабочих станций при взаимодействии с:

- индустриальными устройствами среднего и нижнего уровней со встроенными ViPNet SIES Core (см. глоссарий, стр. 53), подробнее см. документ «ViPNet SIES Core. Общее описание»;
- серверами и рабочими станциями верхнего уровня с установленными ViPNet SIES Unit;
- индустриальными устройствами, интегрированными с другими SIES-узлами (см. глоссарий, стр. 53).

Устройство, интегрированное с ViPNet SIES Unit, становится защищаемым устройством (см. глоссарий, стр. 54). По запросам защищаемого устройства ViPNet SIES Unit выполняет следующие криптографические операции:

- зашифрование и расшифрование данных по алгоритму «Магма» ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) в режиме гаммирования по ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) (подраздел 5.2) в CRISP-сообщении (см. глоссарий, стр. 52);
- вычисление значения имитовставки (см. глоссарий, стр. 54) для данных и проверка значения имитовставки по алгоритму «Магма» ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) в режиме выработки имитовставки по ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) в CRISP-сообщении;
- зашифрование и расшифрование данных в CMS-контейнере (см. глоссарий, стр. 52) с использованием сертификатов (см. глоссарий, стр. 55) X.509 по алгоритму ГОСТ 28147-89 в соответствии с методическими рекомендациями 26.2.002-2013;
- вычисление значения хэш-кода (см. глоссарий, стр. 55) и проверка значения хэш-кода по алгоритму ГОСТ Р 34.11-2012;
- создание и проверка усиленной неквалифицированной электронной подписи (см. глоссарий, стр. 55) данных в CMS-контейнере по алгоритму ГОСТ Р 34.10-2012.

С помощью криптографических операций ViPNet SIES Unit обеспечивает реализацию сценариев защиты данных в зависимости от модели угроз и нарушителя информационной безопасности, разработанной для индустриальной системы, например:

- обеспечение целостности (см. глоссарий, стр. 55) при передаче данных по существующим каналам связи;

- обеспечение конфиденциальности (см. глоссарий, стр. 55) при передаче данных по существующим каналам связи;
- защита от навязывания индустриальной системе ложных данных;
- защита от повторов и навязывания индустриальной системе устаревших данных;
- доверенное хранение данных о функционировании защищаемого устройства.

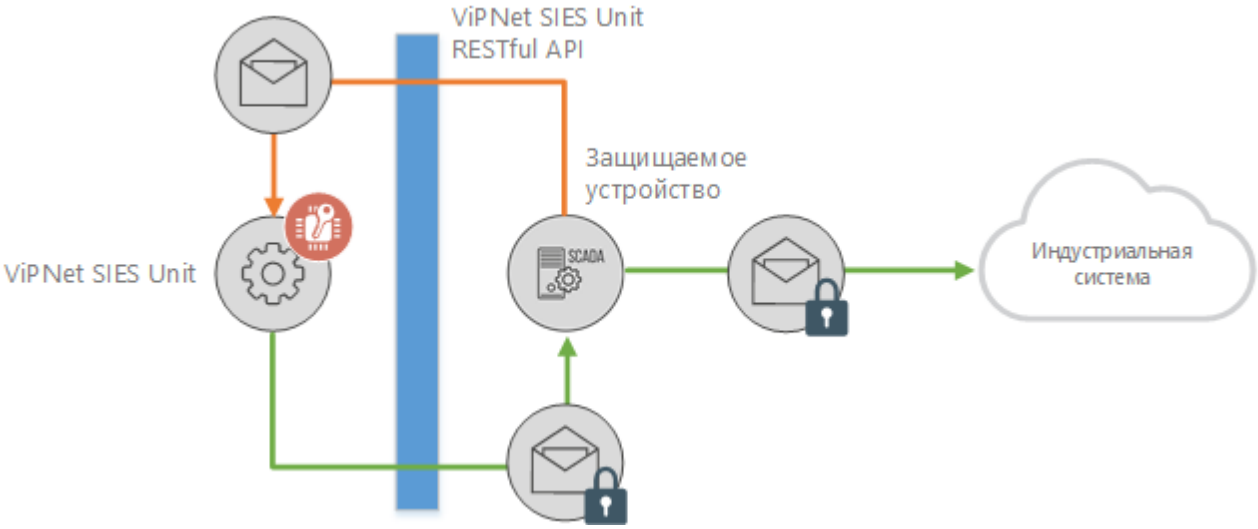

Рисунок 1. Пример взаимодействия SCADA-сервера и ViPNet SIES Unit

Для использования защищаемым устройством функций криптографической обработки данных ViPNet SIES Unit следует организовать взаимодействие прикладного ПО защищаемого устройства и ViPNet SIES Unit через RESTful API (см. глоссарий, стр. 53) или ViPNet SIES Unit SDK (см. глоссарий, стр. 53). Подробнее см. документ «ViPNet SIES Unit. Руководство разработчика» или «ViPNet SIES Unit SDK. Общее описание». Сценарии использования ViPNet SIES Unit см. в документе «ViPNet SIES. Сценарии работы».

Управлять ViPNet SIES Unit с помощью ViPNet SIES MC (см. глоссарий, стр. 53) можно:

- по каналам связи индустриальной системы;
- транслируя на ViPNet SIES Unit защищенные конверты (см. глоссарий, стр. 54) ViPNet SIES MC с помощью:
  - ViPNet SIES Workstation (см. глоссарий, стр. 53);
  - через утилиту локального управления.

Работой ViPNet SIES Unit может управлять администратор с помощью утилиты локального управления ViPNet SIES Unit Administrator.

Комплект поставки

В комплект поставки ViPNet SIES Unit для Windows входят следующие компоненты:

1. Программа установки ПО ViPNet SIES Unit.
2. Утилита формирования и проверки контрольной суммы ViPNet HashCalc.
3. Документация в формате PDF:
   - ViPNet SIES Unit Windows. Руководство администратора (данный документ).
   - ViPNet SIES Unit. Руководство разработчика.
   - ViPNet SIES Unit SDK. Общее описание.
   - ViPNet SIES Unit. Лицензионные соглашения на компоненты сторонних производителей.
   - ViPNet HashCalc. Руководство пользователя.

Системные требования

Требования к устройству для использования ViPNet SIES Unit:

1. Электропитание — от источника бесперебойного питания, позволяющего ОС корректно завершить работу ViPNet SIES Unit при внезапном отключении электропитания.
2. Порт USB — не менее 1 шт.
3. USB-носитель, поддерживаемый устройством — 1 шт.
4. Операционная система (работа с другими версиями не гарантируется):
   - Windows 8.1 (32-разрядная или 64-разрядная);
   - Windows 10 (32-разрядная или 64-разрядная);
   - Windows Server 2012 (64-разрядная);
   - Windows Server 2012 R2 (64-разрядная);
   - Windows Server 2016 (64-разрядная).

Примечание. По вопросам использования ViPNet SIES Unit в других версиях Windows обращайтесь в ИнфоТеКС.

5. Пользователю LocalService в операционной системе требуется доступ к сетевому порту RESTful API (по умолчанию 9876) и к сетевому порту подключения ViPNet SIES Workstation (по умолчанию 2345). Вы можете изменить указанные значения с помощью утилиты локального управления после установки ViPNet SIES Unit.
6. Установленные последние пакеты обновлений операционной системы.

Внимание! Не рекомендуется одновременно устанавливать ПО ViPNet PKI Client и ViPNet SIES Unit.

Для установки и настройки ViPNet SIES Unit вы должны обладать полномочиями администратора ОС на устройстве.

1

Установка ViPNet SIES Unit

Подготовка к работе

ViPNet SIES Unit можно использовать:

- на защищаемом устройстве;
- отдельной аппаратной платформе, к которой защищаемое устройство может подключаться по сети (если ресурсы защищаемого устройства не позволяют установить ПО или использовать функции ViPNet SIES Unit).

К обоих случаях к платформе, на которой устанавливается ViPNet SIES Unit, предъявляются одинаковые системные требования.

Подготовка к работе на защищаемом устройстве

Чтобы подготовить ViPNet SIES Unit к работе на защищаемом устройстве, выполните действия из таблицы ниже в предложенном порядке.

Таблица 4. Порядок подготовки к работе ViPNet SIES Unit

	Действие	Ссылка
☐	На защищаемом устройстве установите дату и время согласно всемирному координированному времени (UTC) и локальному часовому поясу с погрешностью не более 1 минуты	
☐	На защищаемое устройство установите ViPNet SIES Unit	Установка ПО (на стр. 19)
☐	Настройте источник бесперебойного питания так, чтобы при внезапном отключении электропитания корректно завершалась работа службы **ViPNet SIES Unit**	
☐	Разместите хранилище CRISP на SSD-диске (не обязательно). Это повысит скорость выполнения криптографических операций в сценариях защиты данных с использованием прикладных связей с назначениями **Вычисление и проверка имитовставки** и **Шифрование в режиме реального времени**	Смена пути к хранилищу CRISP (на стр. 38)

	Действие	Ссылка
☐	Если инициализация ViPNet SIES Unit будет проводиться с помощью ViPNet SIES Workstation и на защищаемом устройстве сетевой порт с номером 2345 занят, задайте другой номер сетевого порта ViPNet SIES Unit	Настройка сетевого порта подключения ViPNet SIES Workstation (на стр. 40)
☐	Если на защищаемом устройстве сетевой порт с номером 9876 занят, задайте другой номер сетевого порта ViPNet SIES Unit	Настройка сетевого порта RESTful API (на стр. 39)
☐	Убедитесь в том, что служба **ViPNet SIES Unit** запущена	
☐	Проведите инициализацию ViPNet SIES Unit	• Автоматическая инициализация с помощью ViPNet SIES Workstation (на стр. 21) • Автоматическая инициализация без использования ViPNet SIES Workstation (на стр. 21) • Ручная инициализация (на стр. 23)
☐	Смените PIN-код ViPNet SIES Unit	Смена PIN-кода (на стр. 41)
☐	Переведите ViPNet SIES Unit в режим работы **Штатный**	Перевод в режим выполнения криптографических операций (на стр. 31)

Теперь ViPNet SIES Unit готов к реализации сценариев защиты данных. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Подготовка к работе на отдельной аппаратной платформе

Если ресурсы, архитектура или операционная система защищаемого устройства не позволяют установить ПО или использовать функции установленного ViPNet SIES Unit, можно использовать отдельную аппаратную платформу для установки ViPNet SIES Unit. Защищаемое устройство будет вызывать функции ViPNet SIES Unit дистанционно.

Аппаратная платформа с установленным ViPNet SIES Unit и защищаемое устройство, использующее функции ViPNet SIES Unit, должны:

- располагаться в единой контролируемой зоне;
- взаимодействовать по сети TCP/IP.

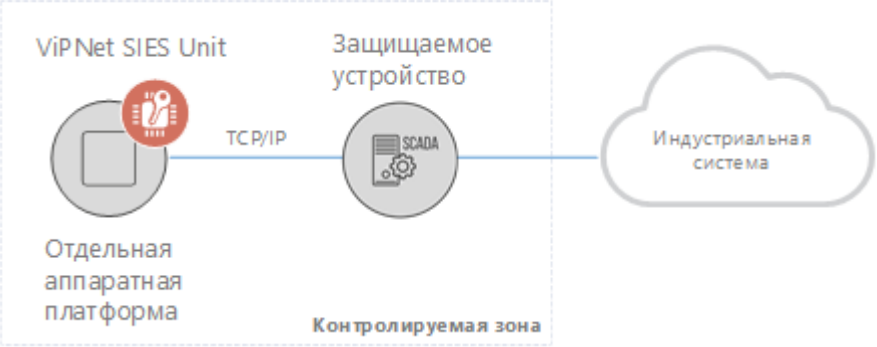

Рисунок 2. Размещение ViPNet SIES Unit на отдельной аппаратной платформе

Таблица 5. Порядок подготовки к работе ViPNet SIES Unit

	Действие	Ссылка
☐	На аппаратной платформе установите дату и время согласно всемирному координированному времени (UTC) и локальному часовому поясу с погрешностью не более 1 минуты	
☐	На аппаратную платформу установите ViPNet SIES Unit	Установка ПО (на стр. 19)
☐	Настройте источник бесперебойного питания так, чтобы при внезапном отключении электропитания корректно завершалась работа службы **ViPNet SIES Unit**	
☐	Разместите хранилище CRISP на SSD-диске (не обязательно). Это повысит скорость выполнения криптографических операций в сценариях защиты данных с использованием прикладных связей с назначениями **Вычисление и проверка имитовставки** и **Шифрование в режиме реального времени**	Смена пути к хранилищу CRISP (на стр. 38)
☐	Если инициализация ViPNet SIES Unit будет проводиться с помощью ViPNet SIES Workstation и на аппаратной платформе сетевой порт с номером 2345 занят, задайте другой номер сетевого порта ViPNet SIES Unit	Настройка сетевого порта подключения ViPNet SIES Workstation (на стр. 40)
☐	Если на аппаратной платформе сетевой порт с номером 9876 занят, задайте другой номер сетевого порта ViPNet SIES Unit	Настройка сетевого порта RESTful API (на стр. 39)
☐	Задайте IP-адрес ViPNet SIES Unit для подключения защищаемого устройства	Задание IP-адреса для подключения защищаемого устройства (на стр. 42)

	Действие	Ссылка
☐	В сетевых настройках аппаратной платформы разрешите подключение только защищаемого устройства по заданным: • IP-адресу; • сетевому порту RESTful API	
☐	Делегируйте пользователю LocalService полномочия доступа к сетевому порту для подключения защищаемого устройства	На аппаратной платформе запустите командную строку Windows от имени администратора и выполните команду: `netsh http add urlacl url="http://<IP-адрес>:<порт RESTful API>/api/v2" user="NT AUTHORITY\LocalService"` Здесь: • `<IP-адрес>` — IP-адрес ViPNet SIES Unit для подключения защищаемого устройства; • `<порт RESTful API>` — значение 9876 или другое значение, заданное выше
☐	Убедитесь в том, что служба **ViPNet SIES Unit** запущена	
☐	Проведите инициализацию ViPNet SIES Unit	• Автоматическая инициализация с помощью ViPNet SIES Workstation (на стр. 21) • Автоматическая инициализация без использования ViPNet SIES Workstation (на стр. 21) • Ручная инициализация (на стр. 23)
☐	Смените PIN-код ViPNet SIES Unit	Смена PIN-кода (на стр. 41)
☐	Переведите ViPNet SIES Unit в режим работы **Штатный**	Перевод в режим выполнения криптографических операций (на стр. 31)

Теперь ViPNet SIES Unit готов к реализации сценариев защиты данных. Подробнее см. документ «ViPNet SIES. Сценарии работы».

Установка ПО

Перед установкой ViPNet SIES Unit убедитесь в целостности программы установки:

1. С помощью утилиты ViPNet HashCalc вычислите контрольную сумму программы установки по алгоритму ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.
2. Сравните вычисленное значение контрольной суммы со значением из раздела «Контрольные суммы» документа «ViPNet SIES Unit. Формуляр» ФРКЕ.466219.017ФО.

Если значения контрольных сумм не совпали, не выполняя установку ViPNet SIES Unit, обратитесь к представителю ИнфоТеКСа.

Чтобы установить ViPNet SIES Unit:

1. Запустите программу установки ViPNet SIES Unit.
2. Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок.

   Для установки ViPNet SIES Unit с параметрами по умолчанию, нажмите кнопку **Установить**.

   Если вы хотите настроить путь к каталогу установки программы:

   2.1 Нажмите кнопку **Компоненты и параметры**.

   2.2 В поле **Путь установки** задайте новый путь к каталогу установки программы.

   Каталог установки программы по умолчанию:

   - `C:\Program Files\InfoTeCS\ViPNet SIES Unit` — для 32-разрядных ОС;
   - `C:\Program Files (x86)\InfoTeCS\ViPNet SIES Unit` — для 64-разрядных ОС.

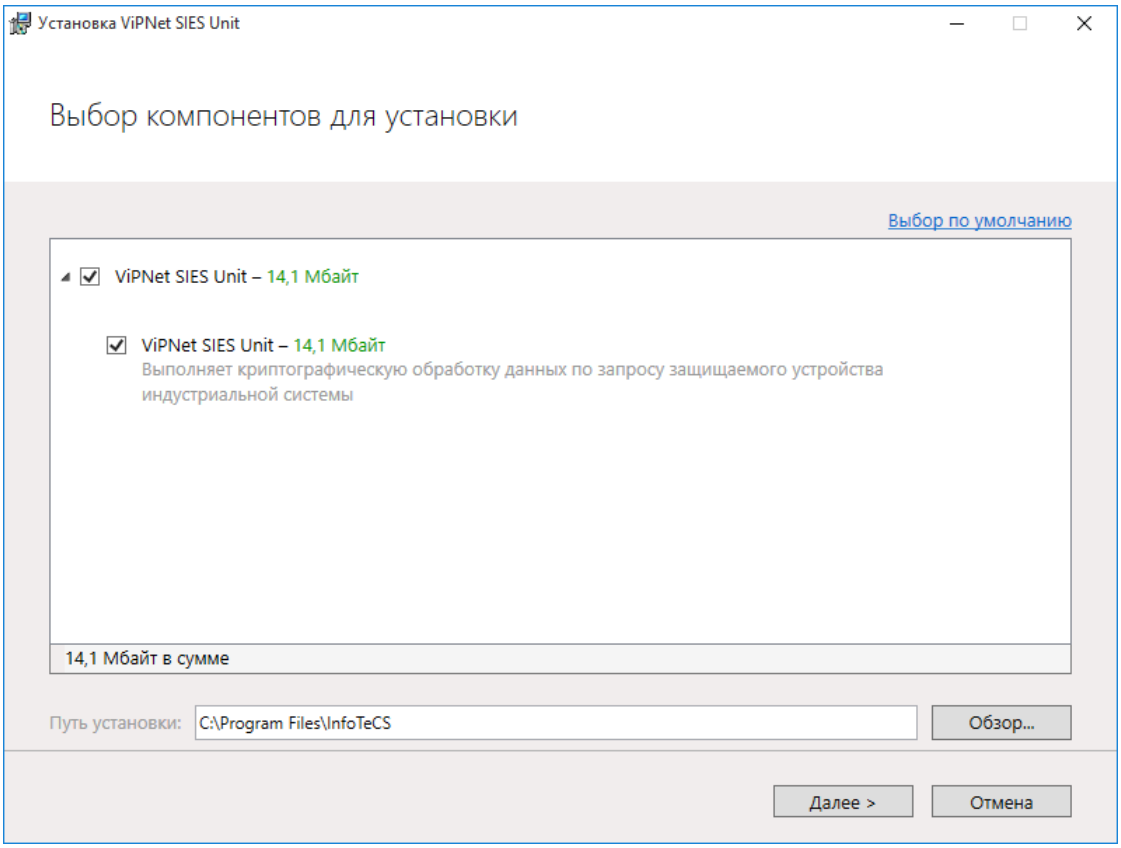

Рисунок 3. Компоненты и параметры установки ViPNet SIES Unit

2.3 Нажмите кнопку **Далее**.

2.4 На следующей странице мастера при необходимости задайте параметры установки и нажмите кнопку **Установить**.

3 По завершении установки нажмите кнопку **Готово** в окне мастера.

Инициализация

Перед началом использования проведите инициализацию (см. глоссарий, стр. 54) ViPNet SIES Unit для последующего защищенного управления из ViPNet SIES MC. Вы можете выполнить инициализацию ViPNet SIES Unit:

- с помощью ViPNet SIES Workstation;
- с помощью сертификата оператора ViPNet SIES Workstation без использования ViPNet SIES Workstation;
- вручную, если ViPNet SIES Workstation недоступен.

По завершении инициализации смените PIN-код ViPNet SIES Unit (на стр. 36).

Автоматическая инициализация с помощью ViPNet SIES Workstation

О проведении инициализации ViPNet SIES Unit с помощью ViPNet SIES Workstation см. в документе «ViPNet SIES Workstation. Руководство по эксплуатации».

Перед инициализацией ViPNet SIES Unit на устройстве разрешите входящие TCP-соединения на сетевой порт подключения ViPNet SIES Workstation, заданный в настройках ViPNet SIES Unit (на стр. 36).

Автоматическая инициализация без использования ViPNet SIES Workstation

Если между устройством с установленным ViPNet SIES Unit и ViPNet SIES MC есть канал связи TCP/IP, вы можете провести инициализацию ViPNet SIES Unit с использованием сертификата оператора WS. Подробнее об операторе WS см. документ «ViPNet SIES MC. Общее описание».

Перед проведением инициализации у администратора ViPNet SIES MC получите:

- IP-адрес или доменное имя ViPNet SIES MC;
- HTTPS-порт подключения администраторов;

Чтобы провести инициализацию:

1. Получите ключи электронной подписи оператора WS одним из способов:
   - на существующем рабочем месте оператора WS экспортируйте ключи электронной подписи в файл `*.pfx`;

- подготовьтесь к инициализации (на стр. 22) и экспортируйте ключи электронной подписи в файл `*.pfx`.

Подробнее об экспорте ключей см. документацию на используемый криптопровайдер.

2 Запустите командную строку Windows от имени администратора.

3 Перейдите в каталог установки ViPNet SIES Unit (по умолчанию `C:\Program Files\InfoTeCS\ViPNet SIES Unit` в 32-разрядных версиях Windows или `C:\Program Files (x86)\InfoTeCS\ViPNet SIES Unit` в 64-разрядных).

4 Выполните команду `siesunit_init -s <адрес> -p <порт> -f <контейнер>`, где:

- `<адрес>` — IP-адрес или доменное имя ViPNet SIES MC;
- `<порт>` — HTTPS-порт подключения администраторов (если используется номер порта 443, то параметр `-p` можно опустить);
- `<контейнер>` — полный путь к файлу `*.pfx` с ключами электронной подписи оператора WS.

5 Поводите курсором в пределах появившегося окна **Электронная рулетка** (см. глоссарий, стр. 56).

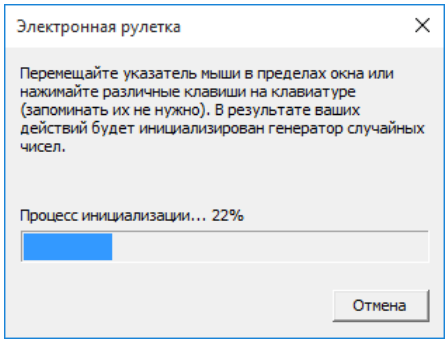

Рисунок 4. Биологический датчик случайных чисел (электронная рулетка)

6 На запрос **Enter the password of the private key** введите пароль к файлу `*.pfx`, заданный при экспорте ключей, и нажмите клавишу **Enter**.

7 Дождитесь сообщения **ViPNet SIES Unit initialization has been completed**.

Подготовка к автоматической инициализации без использования ViPNet SIES Workstation: порядок действий

Чтобы подготовиться к автоматической инициализации без использования ViPNet SIES Workstation, выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 6. Порядок подготовки

Действие	Ссылка

	Действие	Ссылка
☐	На компьютере, защищаемом устройстве или отдельной аппаратной платформе установите криптопровайдер любого производителя, поддерживающий создание и проверку электронной подписи по ГОСТ Р 34.10-2012	Например: • ViPNet CSP; • ViPNet PKI Client См. документацию на используемый криптопровайдер
☐	С помощью криптопровайдера создайте запрос на сертификат	• См. документацию на используемый криптопровайдер • См. ViPNet SIES MC. Общее описание > Ключевая информация и сертификаты > Требования к сертификатам пользовательской ключевой подсистемы
☐	Доверенным способом передайте запрос на сертификат администратору удостоверяющего центра для издания сертификата	
☐	У администратора удостоверяющего центра получите и на компьютере, защищаемом устройстве или отдельной аппаратной платформе с криптопровайдером установите: • корневой сертификат удостоверяющего центра; • список аннулированных сертификатов удостоверяющего центра; • изданный сертификат	См. документацию на используемый криптопровайдер
☐	Передайте изданный сертификат администратору ViPNet SIES MC для добавления в ViPNet SIES MC с ролью оператора WS	

Ручная инициализация

Если у вас нет возможности использовать ViPNet SIES Workstation (например, нельзя подключиться к устройству из локальной сети), проведите ручную инициализацию ViPNet SIES Unit.

Чтобы вручную инициализировать ViPNet SIES Unit:

1. Подключите USB-носитель к устройству с установленным ViPNet SIES Unit.
2. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
3. В списке действий выберите **Generate service key pair**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
4. Поводите курсором в пределах появившегося окна **Электронная рулетка** (см. глоссарий, стр. 56).

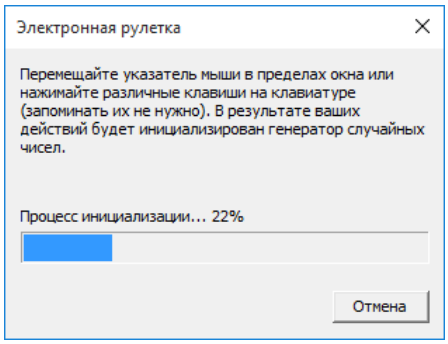

Рисунок 5. Биологический датчик случайных чисел (электронная рулетка)

По окончании выработки ключевой информации будет выдано сообщение **Certificate request file has been generated at** и указан путь к файлу `*.p10` с запросом (см. глоссарий, стр. 54) на служебный сертификат ViPNet SIES Unit (см. глоссарий, стр. 55).

5 На подключенный USB-носитель скопируйте файл `*.p10` из указанного каталога.

6 Отключите и доверенным способом передайте USB-носитель администратору ViPNet SIES MC для издания служебного сертификата ViPNet SIES Unit.

7 У администратора ViPNet SIES MC получите инициализирующий архив для завершения инициализации ViPNet SIES Unit.

8 К устройству с установленным ViPNet SIES Unit подключите USB-носитель с инициализирующим архивом.

9 В списке действий утилиты локального управления выберите **Complete ViPNet SIES Unit initialization**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

10 На запрос **Put archive from ViPNet SIES MC into** скопируйте инициализирующий архив с USB-носителя в указанный каталог. Затем введите символ `y` и нажмите клавишу **Enter**.

11 При наличии в каталоге нескольких инициализирующих архивов выберите нужный, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

12 Запустится обработка инициализирующего архива, по окончании которой будет выдано сообщение **ViPNet SIES Unit initialization has been completed**.

13 Отключите USB-носитель от устройства.

Вы можете закрыть окно утилиты локального управления.

Обновление ПО

Перед обновлением ViPNet SIES Unit убедитесь в целостности программы установки новой версии ViPNet SIES Unit:

1. С помощью утилиты ViPNet HashCalc вычислите контрольную сумму программы установки по алгоритму ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.
2. Сравните вычисленное значение контрольной суммы со значением из раздела «Контрольные суммы» документа «ViPNet SIES Unit. Формуляр» ФРКЕ.466219.017ФО.

Если значения контрольных сумм не совпали, не выполняя установку ViPNet SIES Unit, обратитесь к представителю ИнфоТеКСа.

Чтобы обновить ПО ViPNet SIES Unit:

1. Закройте утилиту локального управления.
2. Запустите программу установки ViPNet SIES Unit.
3. Нажмите кнопку **Обновить**.
4. По завершении обновления компонентов ViPNet SIES Unit нажмите кнопку **Готово** в окне мастера.

Возврат ПО к предыдущей версии

Перед установкой предыдущей версии ПО ViPNet SIES Unit убедитесь в целостности программы установки предыдущей версии:

1. С помощью утилиты ViPNet HashCalc вычислите контрольную сумму программы установки по алгоритму ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.
2. Сравните вычисленное значение контрольной суммы со значением из раздела «Контрольные суммы» документа «ViPNet SIES Unit. Формуляр» ФРКЕ.466219.017ФО.

Если значения контрольных сумм не совпали, не выполняя установку ViPNet SIES Unit, обратитесь к представителю ИнфоТеКСа.

Чтобы вернуться к использованию предыдущей версии ПО ViPNet SIES Unit:

1. Запустите программу установки, выбрав **Пуск** > **ViPNet** > **Настройка компонентов ViPNet SIES Unit**.
2. Выберите **Удалить** и нажмите кнопку **Далее**.
3. Установите флажок **Сохранить пользовательские данные**.

   Установите флажок **Автоматически перезагрузить компьютер при необходимости**.

   Нажмите кнопку **Удалить все компоненты**.
4. Установите ПО (на стр. 19) предыдущей версии ViPNet SIES Unit.

Удаление ПО

Перед выводом из эксплуатации удалите ПО ViPNet SIES Unit с устройства:

1. Приведите ViPNet SIES Unit к заводскому состоянию (на стр. 44).
2. Запустите программу установки, выбрав **Пуск** > **ViPNet** > **Настройка компонентов ViPNet SIES Unit**.
3. Выберите **Удалить** и нажмите кнопку **Далее**.
4. Снимите флажок **Сохранить пользовательские данные**.

   Установите флажок **Автоматически перезагрузить компьютер при необходимости**.

   Нажмите кнопку **Удалить все компоненты**.

2

Управление ViPNet SIES Unit

Получение информации о текущем состоянии

Вы можете получить информацию о текущем состоянии и режиме работы ViPNet SIES Unit:

1. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
2. В списке действий выберите **ViPNet SIES Unit details**, введя цифру `0`.
3. Если служба **ViPNet SIES Unit** запущена, на экран будет выведен список параметров текущего состояния ViPNet SIES Unit:
   - `ID` — идентификатор SIES-узла. До завершения инициализации выдается значение `000000000000`.
   - `Type` — тип SIES-узла. Для ViPNet SIES Unit выдается значение `5`.
   - `Version` — версия ПО ViPNet SIES Unit.
   - `Mode` — текущий режим работы ViPNet SIES Unit (на стр. 30):
     - `Initialization` — режим **Инициализация**;
     - `Regular` — режим **Штатный**;
     - `Configuration` — режим **Конфигурирование**;
     - `Cleaning` — режим **Очистка**.

Смена режима работы

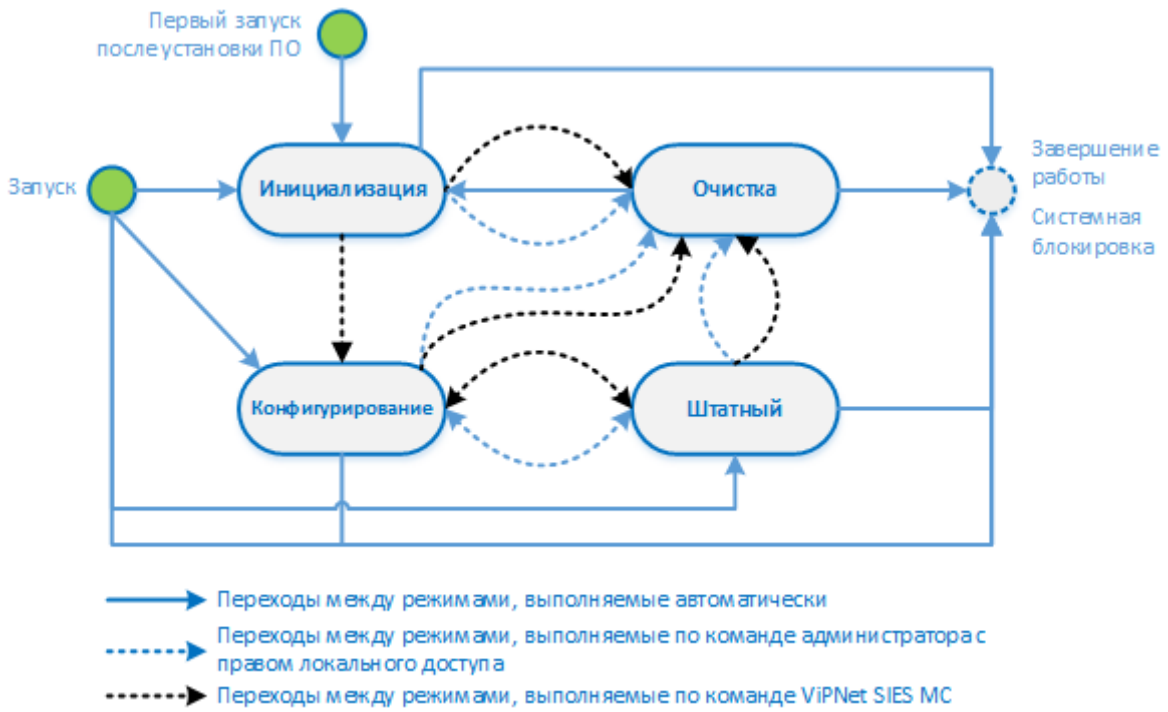

Рисунок 6. Режимы работы ViPNet SIES Unit

В ходе эксплуатации ViPNet SIES Unit работает в одном из следующих режимов:

- **Инициализация** — предназначен для ввода ViPNet SIES Unit в эксплуатацию по командам администратора безопасности устройства с установленным ViPNet SIES Unit. Также в данном режиме ViPNet SIES Unit обрабатывает защищенные конверты ViPNet SIES MC.

  В данный режим ViPNet SIES Unit переходит:

  - автоматически после запуска, если ViPNet SIES Unit находился в данном режиме перед завершением работы;
  - при первом запуске после установки ПО ViPNet SIES Unit;
  - после приведения к заводскому состоянию.

- **Штатный** — основной режим работы ViPNet SIES Unit. Предназначен для выполнения криптографических операций по запросам защищаемого устройства и обработки защищенных конвертов ViPNet SIES MC.

  В данный режим ViPNet SIES Unit переходит:

  - автоматически после запуска, если ViPNet SIES Unit находился в данном режиме перед завершением работы;
  - по команде администратора ViPNet SIES MC;
  - по команде администратора безопасности устройства с установленным ViPNet SIES Unit.

Выход из режима возможен по команде администратора ViPNet SIES MC или по команде администратора безопасности устройства с установленным ViPNet SIES Unit.

- **Конфигурирование** — в этом режиме администратор ViPNet SIES MC может удаленно управлять работой ViPNet SIES Unit. Криптографические операции по запросам защищаемого устройства в этом режиме не выполняются.

  В данный режим ViPNet SIES Unit переходит:

  - автоматически после запуска, если ViPNet SIES Unit находился в данном режиме перед завершением работы;
  - по команде администратора ViPNet SIES MC;
  - по команде администратора безопасности устройства с установленным ViPNet SIES Unit.

  Выход из режима возможен по команде администратора ViPNet SIES MC или по команде администратора безопасности устройства с установленным ViPNet SIES Unit.

- **Очистка** — предназначен для приведения ViPNet SIES Unit к заводскому состоянию. В этом режиме ViPNet SIES Unit не обрабатывает защищенные конверты ViPNet SIES MC и не выполняет криптографические операции по запросам защищаемого устройства. Администратор безопасности устройства с установленным ViPNet SIES Unit может получить информацию о текущем состоянии ViPNet SIES Unit.

- **Системная блокировка** — в данном режиме ViPNet SIES Unit не отвечает на запросы защищаемого устройства и не обрабатывает защищенные конверты ViPNet SIES MC. Переход ViPNet SIES Unit в данный режим равносилен отсутствию ViPNet SIES Unit на устройстве. В данный режим ViPNet SIES Unit переходит автоматически в следующих случаях:

  - обнаружение нарушения целостности программного обеспечения ViPNet SIES Unit во время стартового, периодического или регламентного контроля целостности программных компонентов;
  - обнаружение ошибок во время контроля работоспособности программных модулей ViPNet SIES Unit;
  - завершение работы ViPNet SIES Unit.

  ViPNet SIES Unit остается в данном режиме до устранения причины блокировки и последующего запуска ViPNet SIES Unit.

Перевод в режим выполнения криптографических операций

Криптографические операции с данными защищаемого устройства на ViPNet SIES Unit выполняются в режиме **Штатный**. Вы можете перевести ViPNet SIES Unit в режим **Штатный** только из режима **Конфигурирование**.

Чтобы перевести ViPNet SIES Unit в режим работы **Штатный**:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Switch to Regular mode**, введя соответствующую цифру.

3 На запрос **Are you sure you want to switch ViNet SIES Unit to Regular mode** введите символ `y` и нажмите клавишу **Enter**.

   ViPNet SIES Unit будет переведен в режим работы **Штатный**.

   После получения сообщения **ViPNet SIES Unit mode has been changed** вы можете выйти из утилиты локального управления.

Блокирование выполнения криптографических операций

Блокирование выполнения криптографических операций на ViPNet SIES Unit требуется перед регламентным обслуживанием устройства с установленным ViPNet SIES Unit путем перевода ViPNet SIES Unit в режим работы **Конфигурирование**. Вы можете перевести ViPNet SIES Unit в режим **Конфигурирование** только из режима **Штатный**.

Чтобы перевести ViPNet SIES Unit в режим работы **Конфигурирование**:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Switch to Configuration mode**, введя соответствующую цифру.

3 На запрос **Are you sure you want to switch ViNet SIES Unit to Configuration mode** введите символ `y` и нажмите клавишу **Enter**.

   ViPNet SIES Unit будет переведен в режим работы **Конфигурирование**.

4 После получения сообщения **ViPNet SIES Unit mode has been changed** вы можете выйти из утилиты локального управления.

Контроль целостности программных модулей

Целостность программных модулей ViPNet SIES Unit контролируется автоматически каждые 10 минут работы службы **ViPNet SIES Unit**.

В ходе эксплуатации проверяйте целостность программных модулей ViPNet SIES Unit, например, при регламентном обслуживании устройства с установленным ViPNet SIES Unit. Проверку следует проводить не реже, чем 1 раз в 12 месяцев.

Чтобы проверить целостность ПО ViPNet SIES Unit:

1. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
2. В списке действий выберите **Verify integrity**, введя соответствующую цифру.

   Начнется проверка целостности программных модулей ViPNet SIES Unit.
3. Если проверка не выявила нарушения целостности, на экране появится сообщение **ViPNet SIES Unit software integrity has been verified successfully**.

   Если проверка выявила нарушение целостности:

   - на экране появится сообщение **ViPNet SIES Unit software integrity is violated**;
   - ViPNet SIES Unit будет переведен в режим работы **Системная блокировка**.

   Вы можете выгрузить служебный журнал и обратиться в службу поддержки ИнфоТеКСа для диагностики проблемы.

Получение записей о событиях аудита

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

- события хранилища сертификатов и ключевой информации;
- события изменения режима работы ViPNet SIES Unit;
- события проверки целостности ПО ViPNet SIES Unit;
- системные события.

Записи о событиях аудита ViPNet SIES Unit хранятся в разделе **Журналы приложений и служб** > **ViPNet SIES Unit** > **Audit** журнала системных событий Windows.

Просмотреть и экспортировать записи вы можете из стандартной программы **Просмотр событий**.

Получение записей служебного журнала

Служебный журнал позволяет контролировать работу ViPNet SIES Unit. Служебный журнал хранится в разделе **Журналы приложений и служб** > **ViPNet SIES Unit** журнала системных событий Windows.

Записи служебного журнала заносятся в два раздела:

- **Admin** — записи о запуске и останове службы **ViPNet SIES Unit**:
  - код 8 — служба запущена;
  - код 9 — служба остановлена.
- **Log** — записи о событиях в работе службы **ViPNet SIES Unit** в зависимости от заданного уровня детализации (на стр. 36).

Просмотреть и экспортировать записи вы можете из стандартной программы **Просмотр событий**.

При возникновении неполадок в работе ViPNet SIES Unit доверенным способом передайте экспортированные записи представителю ИнфоТеКСа для выяснения причины неполадок.

Настройка

Изменение уровня журналирования

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

Чтобы изменить уровень детализации записей служебного журнала:

1. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
2. В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
3. В списке действий выберите **Log level**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
4. Задайте новый уровень детализации, введя соответствующую цифру.

   Детализация возрастает по мере увеличения номера уровня. Каждый последующий уровень повышает детализацию и включает детализацию всех предыдущих уровней:

   - **Fatal** — информация о критических ошибках в работе программных модулей;
   - **Critical** — информация об ошибках в работе программных модулей;
   - **Warning** — информация о событиях, которые могут привести к ошибкам в работе программных модулей (уровень установлен по умолчанию);
   - **Info** — информация о событиях, не приводящих к ошибкам в работе программных модулей;
   - **Debug** — подробное журналирование системной информации для последующего использования в отладке;
   - **Trace** — подробное журналирование системной информации с трассировкой вызовов для последующего использования в отладке.

   Нажмите клавишу **Enter**.
5. Перезапустите службу **ViPNet SIES Unit**.

Совет. В ходе эксплуатации ViPNet SIES Unit рекомендуем использовать уровень **Warning**. По завершении работ, связанных с изменением уровня журналирования (например, сбора отладочной информации для направления в ИнфоТеКС), вновь задайте уровень **Warning**.

Настройка коэффициентов производительности

Коэффициенты производительности выбираются автоматически при установке ViPNet SIES Unit исходя из следующих предположений:

- реализуются все сценарии защиты данных, предусмотренные для ViPNet SIES Unit (подробнее см. документ «ViPNet SIES. Сценарии работы»);
- преимущественно выполняется криптографическая обработка данных в режиме реального времени.

Установленные по умолчанию значения коэффициентов обеспечивают выполнение оптимального количества криптографических операций ViPNet SIES Unit в одну секунду.

С учетом особенностей технологического процесса и реализуемых сценариев защиты данных, вам может понадобится дополнительная настройка коэффициентов производительности:

- при ограниченных системных ресурсах устройства с установленным ViPNet SIES Unit;
- изменении системных характеристик устройства с момента установки ViPNet SIES Unit.

Вы можете задать три коэффициента производительности ViPNet SIES Unit:

- CRISP-операции для прикладных связей с назначениями:
  - **Вычисление и проверка имитовставки**;
  - **Шифрование в режиме реального времени**;
- CMS-операции для прикладных связей с назначением **Шифрование и проверка электронной подписи**;
- хэш-операции для прикладных связей с назначением **Вычисление и проверка хэш-суммы**.

Внимание! Выполняя настройку, учитывайте зависимость значений коэффициентов от количества ядер процессора устройства с установленным ViPNet SIES Unit. Иначе настройка может привести к снижению производительности ViPNet SIES Unit.

Для достижения оптимальной производительности ViPNet SIES Unit суммарное значение коэффициентов не должно превосходить величину 2 * CPU_cores, где CPU_cores — количество ядер процессора устройства с установленным ViPNet SIES Unit.

Исключение составляют одноядерные процессоры, для которых все коэффициенты устанавливаются равным 1. Вычисление и проверка хэш-кода не относится к приоритетным операциям, поэтому коэффициент хэш-операций следует устанавливать равным 1.

По умолчанию значения коэффициентов CRISP-операций и CMS-операций распределяется в соотношении:

- 60 % — CRISP-операции;
- 40 % — CMS-операции.

Таблица 7. Устанавливаемые по умолчанию коэффициенты производительности

Количество ядер	CRISP-операции	CMS-операции	Хэш-операции
1	1	1	1
2	2	1	1
4	5	2	1
8	10	5	1
16	19	12	1
32	38	25	1
64	77	50	1
128	154	101	1

Чтобы настроить коэффициенты производительности ViPNet SIES Unit:

1. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
2. В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
3. В списке действий выберите коэффициент, введя соответствующую цифру:
   - CRISP-операции — **CRISP workers**;
   - CMS-операции — **CMS workers**;
   - хэш-операции — **Hash workers**.

   Нажмите клавишу **Enter**.
4. Введите новое значение коэффициента производительности и нажмите клавишу **Enter**.
5. Настроив все коэффициенты, перезапустите службу **ViPNet SIES Unit**.

Смена пути к хранилищу CRISP

Если устройство с установленным ViPNet SIES Unit оборудовано SSD-диском, вы можете повысить скорость выполнения CRISP-операций, разместив хранилище CRISP на SSD-диске.

Чтобы перенести хранилище CRISP на SSD-диск:

1. Создайте любой каталог на SSD-диске.
2. Убедитесь в наличии у пользователя LocalService полномочия записи в созданный каталог.
3. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
4. В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

5 В списке действий выберите **CRISP storage path**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

6 На запрос **Do you want to change CRISP storage path** введите символ `y` и нажмите клавишу **Enter**.

7 На запрос **Specify new path to CRISP storage** введите путь к созданному каталогу SSD-диска. Путь следует вводить с учетом регистра символов.

8 Нажмите клавишу **Enter**.

9 Перезапустите службу **ViPNet SIES Unit**.

Управление отложенной записью данных

Для ускорения криптографической обработки в сценариях защиты данных с использованием прикладных связей с назначениями **Вычисление и проверка имитовставки** и **Шифрование в режиме реального времени**, вы можете перевести ViPNet SIES Unit в режим отложенной записи информации на жесткий диск. Режим позволяет сократить количество операций записи и чтения данных с жесткого диска устройства с установленным ViPNet SIES Unit, замедляющих криптографическую обработку.

Чтобы изменить режим отложенной записи:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

3 В списке действий выберите **CRISP pending**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

4 Задайте состояние режима, введя символ:

- `0` для отключения режима (задано по умолчанию);
- `1` для включения режима.

5 Нажмите клавишу **Enter**.

6 Перезапустите службу **ViPNet SIES Unit**.

Настройка сетевого порта RESTful API

По умолчанию ViPNet SIES Unit использует сетевой порт 9876 для RESTful API. Если порт 9876 занят другой службой, вы можете задать другой сетевой порт. Номер порта должен отличаться от заданного для подключения ViPNet SIES Workstation.

Чтобы задать другой сетевой порт для RESTful API:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

3 В списке действий выберите **Application port**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

4 Введите новый номер сетевого порта. Вводимое значение не должно совпадать с номером сетевого порта для подключения ViPNet SIES Workstation. Нажмите клавишу **Enter**.

5 Перезапустите службу **ViPNet SIES Unit**.

6 Убедитесь в том, что служба **ViPNet SIES Unit** запущена.

   Если служба не запустилась, проверьте наличие полномочия доступа пользователя LocalService к сетевому порту RESTful API.

   Если полномочие отсутствует, делегируйте полномочие самостоятельно (на стр. 48) или обратитесь к системному администратору для решения проблемы.

Настройка сетевого порта подключения ViPNet SIES Workstation

По умолчанию ViPNet SIES Unit использует сетевой порт 2345 для подключения ViPNet SIES Workstation. Если порт 2345 занят другой службой, вы можете задать другой сетевой порт. Номер порта должен отличаться от заданного для RESTful API.

Чтобы задать другой сетевой порт для подключения ViPNet SIES Workstation:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

3 В списке действий выберите **Service port**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

4 Введите новый номер сетевого порта. Вводимое значение не должно совпадать с номером сетевого порта RESTful API. Нажмите клавишу **Enter**.

5 Перезапустите службу **ViPNet SIES Unit**.

6 Убедитесь в том, что служба **ViPNet SIES Unit** запущена.

   Если служба не запустилась, проверьте наличие полномочия доступа пользователя LocalService к сетевому порту подключения ViPNet SIES Workstation.

   Если полномочие отсутствует, вы можете делегировать полномочие самостоятельно (на стр. 48) или обратиться к системному администратору для решения проблемы.

Смена PIN-кода

Перед запуском службы **ViPNet SIES Unit** предъявляется PIN-код. Его значение хранится на USB-носителе администратора устройства с установленным ViPNet SIES Unit, предназначенном для хранения PIN-кода.

PIN-код вам потребуется менять:

- после инициализации ViPNet SIES Unit;
- по истечении срока действия PIN-кода в ходе регламентного обслуживания устройства с установленным ViPNet SIES Unit — не реже, чем 1 раз каждые 12 месяцев.

Внимание! Вы должны самостоятельно следить за своевременной сменой PIN-кода.

Чтобы сменить PIN-код:

1. Подключите USB-носитель к устройству с установленным ViPNet SIES Unit и определите путь, по которому USB-носитель подключен.
2. Стандартными средствами Windows остановите службу **ViPNet SIES Unit**.
3. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
4. В списке действий выберите **Change PIN**, введя символ `1`. Затем нажмите клавишу **Enter**.
5. На запрос **Are you sure you want to change storage PIN** введите символ `y` и нажмите клавишу **Enter**.

   При первой смене PIN-кода после инициализации ViPNet SIES Unit на запрос **Specify path to create the storage PIN** введите путь к корневому каталогу USB-носителя. Путь следует вводить с учетом регистра символов, например:

   ```
   e:\
   ```

   Нажмите клавишу **Enter**.

   Дождитесь сообщения **New PIN has been set successfully** об успешной смене PIN-кода.
6. Запустите службу ViPNet SIES Unit (на стр. 43).

Изменение пути к файлу с PIN-кодом

Если в ходе эксплуатации ViPNet SIES Unit путь подключения USB-носителя с PIN-кодом стал отличаться от ранее заданного в настройках ViPNet SIES Unit (например, изменился каталог монтирования USB-носителя), для запуска службы **ViPNet SIES Unit** измените путь в настройках ViPNet SIES Unit.

Совет. Текущий путь к PIN-коду вы можете узнать в разделе **Settings** утилиты локального управления **ViPNet SIES Unit Administrator**.

Чтобы изменить путь к PIN-коду:

1 Стандартными средствами Windows остановите службу **ViPNet SIES Unit**.

2 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

3 В списке действий выберите **Set PIN media path**, введя символ `2`. Затем нажмите клавишу **Enter**.

4 На запрос **Do you want to set other path** введите символ `y` и нажмите клавишу **Enter**.

5 На запрос **Specify existing path to PIN** введите путь к корневому каталогу USB-носителя. Путь следует вводить с учетом регистра символов.

6 Нажмите клавишу **Enter**.

   Дождитесь сообщения **PIN media path has been set successfully** об успешной смене пути к PIN-коду в настройках ViPNet SIES Unit.

7 Запустите службу **ViPNet SIES Unit**.

Задание IP-адреса для подключения защищаемого устройства

Если ViPNet SIES Unit установлен на отдельной аппаратной платформе, к которой защищаемое устройство подключается по сети TCP/IP, задайте IP-адрес для подключения защищаемого устройства (по умолчанию задан IP-адрес 127.0.0.1).

Чтобы задать IP-адрес:

1 Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.

2 В списке действий выберите **Settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

3 В списке действий выберите **Application port's IP**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.

4 На запрос **Application port's IP** задайте IP-адрес аппаратной платформы с установленным ViPNet SIES Unit.

5 Нажмите клавишу **Enter**.

6 Перезапустите службу **ViPNet SIES Unit**.

Загрузка защищенного конверта ViPNet SIES MC

Если между ViPNet SIES MC и ViPNet SIES Unit нет связи, вы можете вручную загрузить в ViPNet SIES Unit для обработки защищенный конверт ViPNet SIES MC. Конверт можно загрузить только после инициализации ViPNet SIES Unit в режимах:

- **Штатный**;
- **Конфигурирование**.

Чтобы загрузить защищенный конверт:

1. У администратора ViPNet SIES MC получите USB-носитель с защищенным конвертом. Конверт из архива `*.tar.gz` распаковывать не нужно.

   USB-носитель может содержать конверты для других SIES-узлов. Будут обработаны только конверты, предназначенные для этого SIES-узла.
2. Подключите USB-носитель к устройству с установленным ViPNet SIES Unit.
3. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
4. В списке действий выберите **Processing commands from external media**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
5. На запрос **Are you sure you want to process commands from external media** введите символ `y` и нажмите клавишу **Enter**.
6. На запрос **Specify path to the external media** введите полный путь к каталогу USB-носителя с защищенным конвертом и нажмите клавишу **Enter**.
7. Запустится обработка защищенного конверта, по окончании которой появится сообщение **SUCCESS: Command from external media has been processed successfully**.
8. Отключите USB-носитель от устройства с установленным ViPNet SIES Unit.
9. Передайте USB-носитель администратору ViPNet SIES MC для загрузки в ViPNet SIES MC защищенного конверта с ответом ViPNet SIES Unit.

Запуск службы ViPNet SIES Unit

Чтобы запустить службу **ViPNet SIES Unit**:

1. К устройству с установленным ViPNet SIES Unit подключите USB-носитель с PIN-кодом.
2. Стандартными средствами Windows запустите службу **ViPNet SIES Unit**.

Приведение к заводскому состоянию

В ходе приведения к заводскому состоянию будет удалена прикладная и ключевая информация, после чего ViPNet SIES Unit будет переведен в режим **Инициализация**.

Чтобы привести ViPNet SIES Unit к заводскому состоянию:

1. Запустите утилиту локального управления, выбрав **Пуск** > **ViPNet** > **ViPNet SIES Unit Administrator**.
2. В списке действий выберите **Reset to factory settings**, введя соответствующую цифру. Затем нажмите клавишу **Enter**.
3. На запрос **Are you sure you want to reset to factory settings** введите символ `y` и нажмите клавишу **Enter**.
4. После получения сообщения **Factory settings have been restored** вы можете выйти из утилиты локального управления.
5. Любым способом уведомите администратора ViPNet SIES MC о приведении ViPNet SIES Unit к заводскому состоянию.

Для восстановления работоспособности ViPNet SIES Unit проведите инициализацию ViPNet SIES Unit (на стр. 21).

Компрометация ViPNet SIES Unit и восстановление после компрометации

Компрометация по инициативе администратора

При выявлении факта несанкционированного доступа к ViPNet SIES Unit данный SIES-узел считается скомпрометированным. Если вам стало известно о компрометации ViPNet SIES Unit:

1. Приведите ViPNet SIES Unit к заводскому состоянию (на стр. 44).
2. Оповестите администратора ViPNet SIES MC о компрометации ViPNet SIES Unit.

Восстановление работоспособности после компрометации

Если скомпрометированный ViPNet SIES Unit пригоден для дальнейшего использования, для восстановления работоспособности проведите инициализацию ViPNet SIES Unit (на стр. 21).

A

Возможные неполадки и способы их устранения

Не удается завершить ручную инициализацию ViPNet SIES Unit

После обработки команды **Complete ViPNet SIES Unit initialization** утилита локального управления выдает сообщение:

- **FAILURE**
- **Internal error**
- **Cannot unpack**

Диагностика

После обработки команды **Complete ViPNet SIES Unit initialization** утилита локального управления выдает сообщение **FAILURE: bad ViPNet SIES MC command <имя файла>** или **FAILURE: Cannot find archive for this node at <имя файла>**.

Возможная причина

Инициализирующий архив ViPNet SIES MC, обработанный утилитой локального управления, не соответствует запросу на служебный сертификат ViPNet SIES Unit.

Способ устранения

1. В утилите локального управления повторно выполните команду **Complete ViPNet SIES Unit initialization.**
2. Получив запрос **Put archive from ViPNet SIES MC into**, скопируйте корректный архив в указанный каталог.
3. Введите символ `y` и нажмите клавишу **Enter** для завершения инициализации ViPNet SIES Unit.

Диагностика

После обработки команды **Complete ViPNet SIES Unit initialization** утилита локального управления выдает сообщение **Internal error. Please reset to factory settings and retry initialization**.

Возможная причина

- Не был сформирован запрос на служебный сертификат ViPNet SIES Unit.
- Ранее утилитой локального управления был обработан некорректный инициализирующий архив ViPNet SIES MC. ViPNet SIES Unit не был приведен к заводскому состоянию перед повторной инициализацией.

Способ устранения

1. Приведите ViPNet SIES Unit к заводскому состоянию.
2. Повторите инициализацию.

Диагностика

После обработки команды **Complete ViPNet SIES Unit initialization** утилита локального управления выдает сообщение **Cannot unpack <путь к файлу с инициализирующим архивом>**.

Возможная причина

Инициализирующий архив ViPNet SIES MC поврежден.

Способ устранения

1. У администратора ViPNet SIES MC получите новый инициализирующий архив.
2. В утилите локального управления повторно выполните команду **Complete ViPNet SIES Unit initialization.**
3. Получив запрос **Put archive from ViPNet SIES MC into**, скопируйте архив в указанный каталог.
4. Введите символ `y` и нажмите клавишу **Enter** для завершения инициализации ViPNet SIES Unit.

Ошибка инициализации ViPNet SIES Unit с помощью сертификата оператора WS

При выполнении команды `siesunit_init` выдается сообщение **ViPNet SIES MC error code: -109**.

Способ устранения

1 Сообщите о проблеме администратору ViPNet SIES MC.

2 От администратора ViPNet SIES MC дождитесь сообщения об устранении проблемы.

3 Повторите инициализацию ViPNet SIES Unit.

Ошибка инициализации ViPNet SIES Unit

В ходе инициализации ViPNet SIES Unit возникла ошибка.

Способ устранения

1 Приведите ViPNet SIES Unit к заводскому состоянию (на стр. 44).

2 Повторите инициализацию (на стр. 21).

Служба ViPNet SIES Unit не запускается — отсутствуют полномочия доступа

Служба **ViPNet SIES Unit** не запускается. В журнале системных событий Windows в разделе **Журналы приложений и служб** > **ViPNet SIES Unit** > **Log** появляются записи об ошибках с сообщением **FATAL ERROR: Cannot start http listener**.

Возможная причина

Отсутствуют полномочия доступа пользователя LocalService к сетевому порту RESTful API или к сетевому порту подключения ViPNet SIES Workstation.

Способ устранения

1 Запустите командную строку Windows от имени администратора и выполните следующие команды:

- `netsh http add urlacl url="http://127.0.0.1:9876/api/v2" user="NT AUTHORITY\LocalService"`
- `netsh http add urlacl url="http://*:2345/api/v2" user="NT AUTHORITY\LocalService"`

Если вы задавали новые значения сетевого порта RESTful API (на стр. 39) и сетевого порта подключения ViPNet SIES Workstation (на стр. 40), в командах укажите актуальные номера сетевых портов.

2 Закройте командную строку Windows.

3 Запустите службу **ViPNet SIES Unit**.

Служба ViPNet SIES Unit не запускается — изменился путь к файлу с PIN-кодом хранилища

Служба **ViPNet SIES Unit** не запускается. В журнале системных событий Windows в разделе **Журналы приложений и служб** > **ViPNet SIES Unit** > **Log** появляются записи об ошибках с сообщением **FATAL: Empty pin code**.

Возможная причина

Файл с PIN-кодом хранилища не обнаружен по заданному пути.

Способ устранения

1 Убедитесь, что USB-носитель с PIN-кодом подключен к устройству с установленным ViPNet SIES Unit.

2 Запустите службу **ViPNet SIES Unit**.

3 Если служба **ViPNet SIES Unit** не запустилась:

3.1 Запустите утилиту **ViPNet SIES Unit Administrator**.

3.2 В списке действий выберите **Settings**, введя символ 3. Затем нажмите клавишу **Enter**.

3.3 Убедитесь, что значение пути в пункте **PIN media path** соответствует реальному на подключенном USB-носителе.

3.4 Если указанный путь не соответствует реальному, укажите актуальный путь (на стр. 41).

Не удается завершить работу службы ViPNet SIES Unit

Не удается запустить службу **ViPNet SIES Unit**. В журнале аудита имеется запись **Нарушена целостность счетчика CRISP**.

Способ устранения

1 Удалите ViPNet SIES Unit с устройства (на стр. 27).

2 Повторно подготовьте ViPNet SIES Unit к работе на устройстве (на стр. 15).

Служба ViPNet SIES Unit не запускается — ошибка чтения и записи файла пин-кода

Служба **ViPNet SIES Unit** не запускается. В журнале системных событий Windows в разделе **Журналы приложений и служб** > **ViPNet SIES Unit** > **Log** появляются записи об ошибках с сообщениями:

- **CRITICAL: Cannot open <путь>**
- **CRITICAL: Cannot read <путь>**

Возможная причина

Отсутствуют полномочия доступа пользователя LocalService к файлу пин-кода.

Способ устранения

1 Проверьте наличие файла по указанному пути. Если файла нет:
   - определите путь к существующему файлу с пин-кодом;
   - измените путь к файлу с пин-кодом (на стр. 41).

2 Пользователю LocalService делегируйте полномочия чтения и записи файла по указанному пути.

3 Запустите службу **ViPNet SIES Unit**.

Не удается обработать CRISP-сообщение

По неочевидным причинам ViPNet SIES Unit выдает сообщение об ошибке при запросе на обработку CRISP-сообщения (см. глоссарий, стр. 52).

Возможная причина

Работа ViPNet SIES Unit была непредвиденно завершена в одном из следующих случаев:

- умышленное нажатие на кнопку перезагрузки устройства с установленным ViPNet SIES Unit (например, в результате зависания ПО или действий злоумышленника);
- неумышленное нажатие на кнопку перезагрузки устройства с установленным ViPNet SIES Unit;
- критическая ошибка Windows («синий экран»);

- автоматическое обновление Windows или перезагрузка по расписанию.

Способ устранения

1 Приведите ViPNet SIES Unit к заводскому состоянию (на стр. 44).

2 Выполните повторную инициализацию ViPNet SIES Unit (на стр. 21).

B

Глоссарий

CMS-контейнер

Криптографическое сообщение, оформленное по стандарту CMS. Применение CMS-контейнеров в обмене криптографическими сообщениями рекомендовано Техническим комитетом Росстандарта (ТК 026: «Криптографическая защита информации»).

CRISP (Cryptographic Industrial Security Protocol)

Неинтерактивный протокол прикладного уровня для защищенной передачи данных в индустриальных системах. Обеспечивает конфиденциальность и целостность сообщений и защищает от навязывания повторных сообщений. Применяется в соответствии с утвержденными рекомендациями по стандартизации Р 1323565.1.029-2019 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем». Адресация, маршрутизация и доставка сообщения выполняются средствами индустриальной системы.

CRISP-сообщение

Блок данных, защищенный с помощью протокола CRISP. Создание и обработку CRISP-сообщений выполняют SIES-узлы.

IIoT-система

IoT-система отраслевого применения, объединяющая промышленные (производственные) объекты, оснащенные встроенными технологиями для взаимодействия друг с другом или с внешней средой и с возможностью удаленного контроля и управления в автоматическом режиме без участия человека. Строится по принципам индустриального интернета вещей (IIoT).

RESTful API

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

SCADA (Supervisory Control And Data Acquisition)

Программное средство для организации систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления в режиме реального времени.

SDK (Software Development Kit)

Комплект средств разработки, позволяющий специалистам по программному обеспечению встраивать в собственные разработки функции продукта через прикладной интерфейс, реализованный в продукте.

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 ИнфоТеКСа для защиты информации в индустриальных системах (Патент РФ № 2706176).

ViPNet SIES Core

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

ViPNet SIES MC

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

ViPNet SIES Workstation

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

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.

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.

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 несекретной 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.

Конфиденциальность

Свойство информации, предназначенной только определенному кругу лиц, которая должна храниться в тайне от всех остальных.

Операционная система (ОС)

Комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Программное обеспечение (ПО)

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

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.

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.

Целостность

Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.