ViPNet SIES

Описание комплекса

infotecs

© АО «ИнфоТеКС», 2021

ФРКЕ.00192-03 90 01

Версия продукта 2.3

Этот документ входит в комплект поставки ViPNet SIES, 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 АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

В продукте использовано изобретение, защищенное патентом РФ № 2706176.

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

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 ... **5**
О документе ... 6
Связанные документы ... 6
Соглашения документа ... 6
Обратная связь ... 8
Новые возможности версии 2.3 ... 9
Комплект документации ViPNet SIES ... 10

Глава 1. Описание комплекса продуктов ViPNet SIES ... **11**
Назначение комплекса ... 12
Состав комплекса ... 14
Компоненты комплекса ... 17
ViPNet SIES Core ... 17
ViPNet SIES Unit ... 18
ViPNet SIES MC ... 18
ViPNet SIES Workstation ... 20
Организация защиты данных индустриальной системы с применением ViPNet SIES ... 23
Достоинства комплекса продуктов ViPNet SIES ... 26

Глава 2. Защита критической информационной инфраструктуры ... **27**
Об использовании комплекса ViPNet SIES для защиты значимого объекта критической информационной инфраструктуры ... 28
Идентификация и аутентификация (ИАФ) ... 29
Управление доступом (УПД) ... 31
Ограничение программной среды (ОПС) ... 32
Аудит безопасности (АУД) ... 33
Обеспечение целостности (ОЦЛ) ... 34
Обеспечение доступности (ОДТ) ... 35
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) ... 37
Управление конфигурацией (УКФ) ... 39
Управление обновлениями программного обеспечения (ОПО) ... 40

Приложение А. История версий ... **41**
Версия 2.2 ... 41
Версия 2.1 ... 42
Версия 2.0 ... 43

Приложение В. Глоссарий 44

Введение

О документе 6

Обратная связь 8

Новые возможности версии 2.3 9

Комплект документации ViPNet SIES 10

О документе

Документ описывает комплекс продуктов ViPNet® Security for Industrial and Embedded Solutions (SIES), предназначенный для защиты информации в индустриальных (см. глоссарий, стр. 47) и IIoT–системах (см. глоссарий, стр. 45). Также документ содержит перечень мер обеспечения безопасности значимых объектов критической информационной инфраструктуры, реализация которых возможна с помощью компонентов комплекса ViPNet SIES.

Связанные документы

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

Таблица 1. Связанные документы

Документ	Содержание
ViPNet SIES Core. Общее описание	Описание, технические характеристики и методика 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	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
ViPNet SIES MC. Общее описание	Описание и методика применения центра ViPNet SIES Management Center (MC), управляющего компонентами комплекса ViPNet SIES в индустриальной системе. Документ входит в комплект поставки ViPNet SIES MC

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.

Обозначение	Описание
	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 версии 2.3 по сравнению с версией 2.2.

Информация об изменениях в предыдущих версиях ViPNet SIES приведена в приложении История версий (на стр. 43).

- **Повышена кратность резервирования для защищаемых устройств с ViPNet SIES Core**

  Теперь в резервированной парной связи с каждой стороны могут участвовать до 11 защищаемых устройств с ViPNet SIES Core.

- **Расширены сценарии эксплуатации**

  Добавлены регламенты по обновлению ключевой информации прикладной ключевой подсистемы ViPNet SIES при использовании внешнего удостоверяющего центра для выпуска сертификатов.

  Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».

- **Расширены рекомендации по защите индустриальных протоколов**

  Добавлены рекомендации по защите протоколов LoRaWAN RU и XNB с помощью комплекса ViPNet SIES.

  Документ предоставляется ИнфоТеКСом по запросу.

Комплект документации ViPNet SIES

Рекомендуем знакомиться с документами в указанном порядке.

Таблица 4. Состав документации

Документ	О документе
ViPNet SIES. Описание комплекса	Данный документ
ViPNet SIES. Сценарии работы	Содержит основные сценарии работы комплекса ViPNet SIES в индустриальной системе
ViPNet SIES. Защита индустриальных протоколов	Содержит методики по реализации защищенного обмена данными в промышленных протоколах, используемых в индустриальных сетях связи. Документ предоставляется ИнфоТеКСом по запросу
ViPNet SIES. Сценарии эксплуатации	Содержит описание основных задач, возникающих в ходе эксплуатации комплекса ViPNet SIES в индустриальной системе. Каждая задача сопровождается методикой ее решения
ViPNet SIES. Руководство разработчика	Содержит методики по интеграции в комплекс ViPNet SIES стороннего компонента для криптографической обработки данных защищаемого устройства и взаимодействия с другими защищаемыми устройствами, интегрированными с SIES-узлами. Документ предоставляется ИнфоТеКСом по запросу
ViPNet SIES. Практикум	Содержит пример внедрения комплекса ViPNet SIES в индустриальную систему, имитирующую управление участком технологического процесса пивоваренного производства
ViPNet SIES. Пример интеграции с MasterSCADA	Содержит описание примера использования функций ViPNet SIES Core и ViPNet SIES Unit в прикладном проекте пакета программ ИнСАТ MasterSCADA для защиты данных на устройствах индустриальной системы, поддерживающих SoftLogic. Также в документе приведена информация по организации обмена защищенными конвертами между ViPNet SIES MC и SIES-узлами из прикладного проекта SCADA
ViPNet SIES OPC UA Server. Пример реализации шлюзового компонента	Содержит пример реализации шлюзового компонента для обмена защищенными конвертами между ViPNet SIES MC и устройством операторского уровня индустриальной системы для доставки конвертов защищаемым устройствам по каналам связи индустриальной системы

1

Описание комплекса продуктов ViPNet SIES

Назначение комплекса 12

Состав комплекса 14

Компоненты комплекса 17

Организация защиты данных индустриальной системы с применением ViPNet SIES 23

Достоинства комплекса продуктов ViPNet SIES 26

Назначение комплекса

Комплекс продуктов ViPNet Security for Industrial and Embedded Solutions (SIES) — решение для криптографической защиты данных в индустриальных системах и системах промышленного интернета вещей (IIoT).

Индустриальная система как правило имеет многоуровневую иерархию, включающую в себя уровни:

- операторского или диспетчерского управления — верхний уровень;
- автоматического управления — средний уровень;
- ввода и вывода данных, исполнительных устройств — нижний уровень.

IIoT-система как правило включает в себя:

- приложения, использующие собранные данные;
- на верхнем уровне:
  - серверы сбора и хранения данных;
  - серверы анализа данных и средств управления;
- на среднем уровне — среда сбора данных:
  - IIoT-шлюзы;
- на нижнем уровне:
  - подключаемые устройства-датчики.

Комплекс ViPNet SIES (см. глоссарий, стр. 46) может применяться для защиты данных на всех уровнях индустриальной и IIoT-системы:

- на верхнем уровне:
  - SCADA-серверы (см. глоссарий, стр. 46);
  - автоматизированные рабочие места операторов;
  - автоматизированные рабочие места инженеров;
  - серверы сбора и обработки информации IIoT–систем;
- на среднем уровне:
  - программируемые логические контроллеры;
  - IIoT-шлюзы;
- на нижнем уровне:
  - датчики;
  - исполнительные механизмы;

- иные аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

Основные задачи комплекса ViPNet SIES:

- выполнение криптографических (см. глоссарий, стр. 48) операций для защиты данных:
  - зашифрование и расшифрование;
  - вычисление и проверка имитовставки (см. глоссарий, стр. 47);
  - вычисление и проверка хэш-кода (см. глоссарий, стр. 49);
  - создание и проверка электронной подписи (см. глоссарий, стр. 49);
- централизованное управление ключевой информацией для выполнения криптографических операций с данными индустриальной системы:
  - выработка, хранение и распространение ключей (см. глоссарий, стр. 48);
  - контроль за сроком действия ключей и сертификатов;
  - создание запросов на сертификаты (см. глоссарий, стр. 48);
  - издание, хранение и распространение сертификатов;
  - смена ключевой информации.

С помощью криптографических операций комплекс ViPNet SIES позволяет реализовать различные сценарии защиты данных в индустриальных и IIoT-системах. Типовые сценарии приведены в документе «ViPNet SIES. Сценарии работы».

Сценарии защиты данных с помощью комплекса ViPNet SIES можно реализовать в индустриальных и IIoT-системах с различными моделями распространения информации и в системах с применением резервирования индустриальных устройств.

Примечание. Далее индустриальную и IIoT-систему будем называть системой.

Состав комплекса

Комплекс продуктов ViPNet SIES включает в себя следующие компоненты:

- программно-аппаратный комплекс ViPNet SIES Core (см. глоссарий, стр. 46) — средство криптографической защиты информации, обрабатываемой устройствами нижнего и среднего уровней системы;
- прикладная служба ViPNet SIES Unit (см. глоссарий, стр. 47) — средство криптографической защиты информации, обрабатываемой устройствами верхнего уровня системы;
- программно-аппаратный комплекс ViPNet SIES MC — средство централизованного управления (см. глоссарий, стр. 46) компонентами комплекса ViPNet SIES, развернутыми в системе;
- автоматизированное рабочее место (АРМ) с программным обеспечением (ПО) ViPNet SIES Workstation (см. глоссарий, стр. 47) — средство ввода в эксплуатацию и обслуживания ViPNet SIES Core и ViPNet SIES Unit на индустриальных объектах (см. глоссарий, стр. 47).

Также в комплекс ViPNet SIES можно интегрировать сторонний компонент для криптографической обработки данных защищаемого устройства и взаимодействия с другими защищаемыми устройствами, интегрированными с SIES-узлами. Подробнее см. документ «ViPNet SIES. Руководство разработчика». Документ предоставляется ИнфоТеКСом по запросу.

Схема с примером решения ViPNet SIES, развернутого в индустриальной системе, приведена на рисунке ниже.

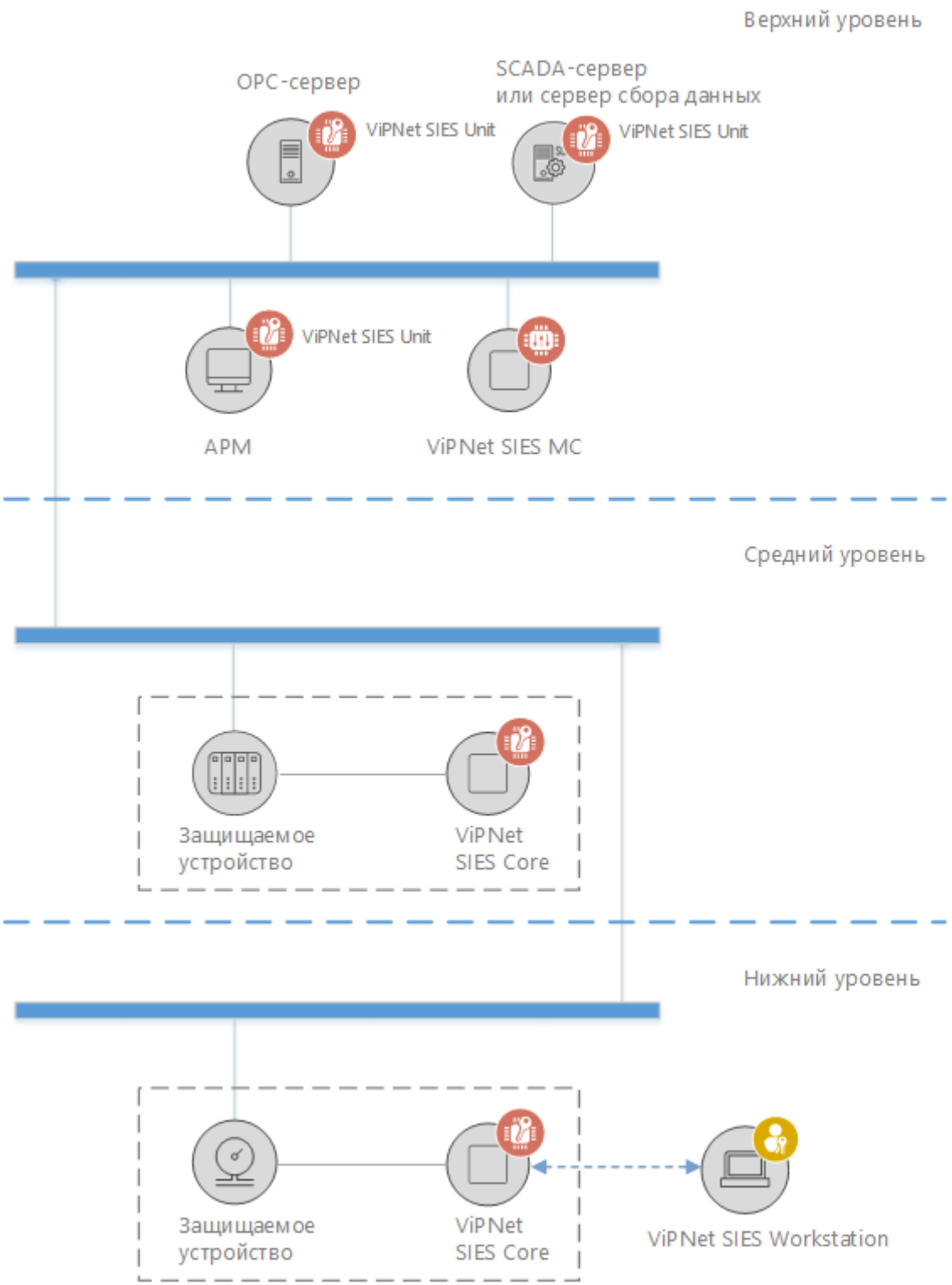

Рисунок 1. Пример решения ViPNet SIES, развернутого в индустриальной системе

Схема с примером решения ViPNet SIES, развернутого в IIoT-системе, приведена на рисунке ниже.

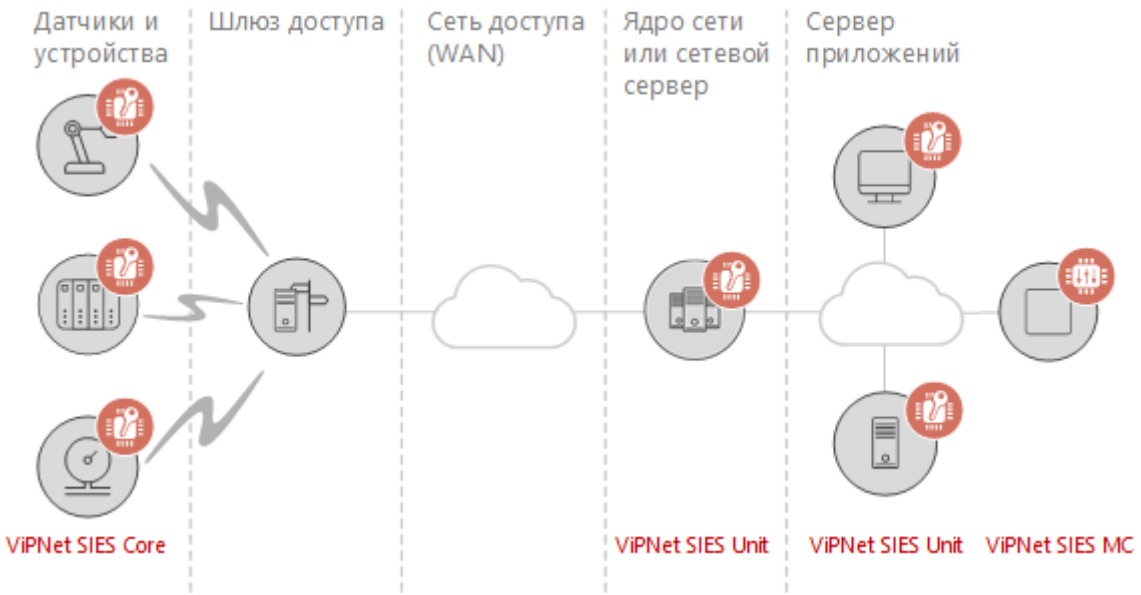

Рисунок 2. Пример решения ViPNet SIES, развернутого в IIoT-системе

Компоненты комплекса

ViPNet SIES Core

ViPNet SIES Core — программно-аппаратный комплекс в форме процессорного модуля (System On Module), предназначенный для интеграции с индустриальными устройствами, такими как:

- программируемые логические контроллеры (PLC);
- устройства сбора и передачи информации (RTU);
- промышленные контроллеры автоматизации (PAC);
- интеллектуальное оконечное оборудование (сенсоры, датчики, счетчики, различные исполнительные устройства);
- IIoT-шлюзы.

Рисунок 3. Внешний вид ViPNet SIES Core

ViPNet SIES Core интегрируются с защищаемым устройством (см. глоссарий, стр. 47) на аппаратном уровне через межплатные интерфейсы UART, USB или SPI. Прикладное ПО защищаемого устройства взаимодействует с ViPNet SIES Core с помощью функций ViPNet SIES Core SDK (см. глоссарий, стр. 46) или через стек протоколов. Подробнее см. документ «ViPNet SIES Core. Общее описание».

Основные функции ViPNet SIES Core:

- выполнение криптографических операций для защиты данных защищаемого устройства;
- поддержание жизненного цикла ключевой информации.

ViPNet SIES Unit

ViPNet SIES Unit — средство криптографической защиты информации, обрабатываемой устройствами верхнего уровня системы (например, SCADA, OPC, HMI).

ViPNet SIES Unit устанавливается на защищаемое устройство (отдельную аппаратную платформу) верхнего уровня или внутри виртуального модуля (см. глоссарий, стр. 46) облачной инфраструктуры IIoT-системы и работает как служба ОС.

Прикладное ПО защищаемого устройства взаимодействует с ViPNet SIES Unit через RESTful API (см. глоссарий, стр. 45) или ViPNet SIES Unit SDK. Подробнее см. документ «ViPNet SIES Unit. Руководство разработчика» или «ViPNet SIES Unit SDK. Общее описание».

Основные функции ViPNet SIES Unit:

- выполнение криптографических операций для защиты данных защищаемого устройства;
- поддержание жизненного цикла ключевой информации.

ViPNet SIES MC

ViPNet SIES MC — центр управления компонентами комплекса продуктов ViPNet SIES, установленными в системе. ViPNet SIES MC устанавливается на верхнем уровне системы.

ViPNet SIES MC взаимодействует с SIES-узлами (см. глоссарий, стр. 46) — компонентами ViPNet SIES Core и ViPNet SIES Unit, интегрированными с защищаемыми устройствами. ViPNet SIES MC контролирует состояние SIES-узлов, централизованно управляет ключевой информацией, а также режимами работы SIES-узлов.

Для удаленного управления SIES-узлами используются каналы связи системы и требуется разработка шлюзового компонента между ViPNet SIES MC и транспортным уровнем системы.

По запросу ИнфоТеКС может предоставить пример реализации шлюзового компонента ViPNet SIES OPC UA Server (см. глоссарий, стр. 46), который служит одним из возможных способов организации взаимодействия ViPNet SIES MC с SIES-узлами по каналам связи системы.

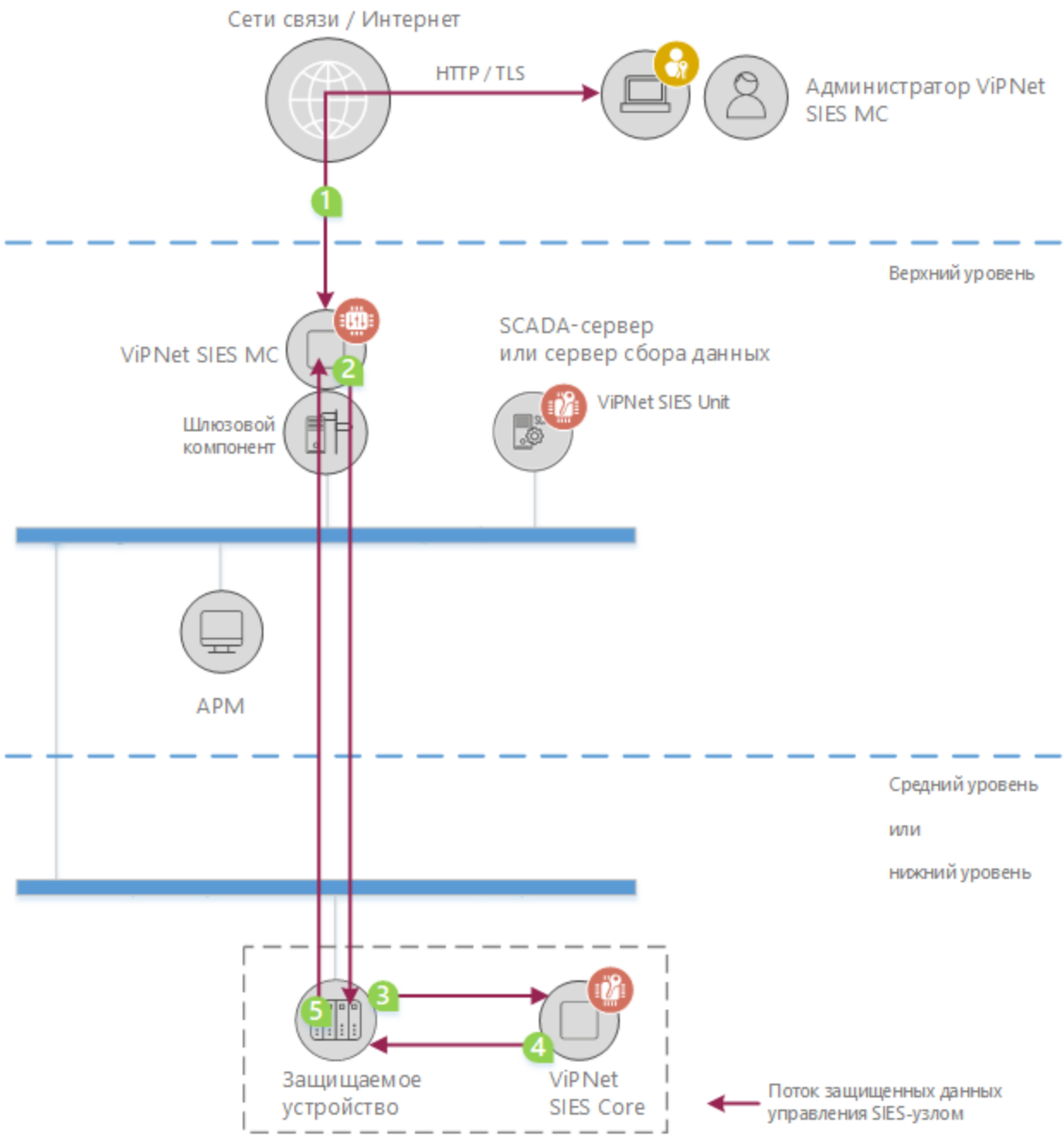

Рисунок 4. Удаленное управление SIES-узлом

Удаленное управление компонентами комплекса ViPNet SIES на примере ViPNet SIES Core происходит в следующей последовательности:

1 Администратор ViPNet SIES MC с рабочего места подключается к веб-интерфейсу ViPNet SIES MC по протоколу TLS и выполняет операцию управления SIES-узлом.

2 ViPNet SIES MC формирует команды управления и мониторинга, упаковывает команды в защищенные конверты в адрес SIES-узла. Шлюзовой компонент по каналам связи системы передает защищенные конверты защищаемому устройству, с которым интегрирован SIES-узел.

3 Получив защищенные конверты от ViPNet SIES MC, защищаемое устройство транслирует защищенные конверты SIES-узлу.

4. После исполнения команды управления ViPNet SIES Core возвращает результат защищаемому устройству в виде защищенного конверта.
5. В обратной последовательности защищаемое устройство отправляет ViPNet SIES MC защищенный конверт, который отображается администратору ViPNet SIES MC.

В зависимости от архитектуры в системе могут одновременно использоваться несколько шлюзовых компонентов.

Для локального управления ViPNet SIES Core подключается к USB-порту на АРМ (см. глоссарий, стр. 47) с установленным ПО ViPNet SIES Workstation, соединенному по защищенному TLS-каналу с ViPNet SIES MC. Для локального управления ViPNet SIES Unit АРМ с установленным ПО ViPNet SIES Workstation по сети подключается к защищаемому устройству с установленным ViPNet SIES Unit.

Подробнее о возможных вариантах организации управления см. документ «ViPNet SIES. Сценарии эксплуатации».

ViPNet SIES Workstation

ViPNet SIES Workstation — ПО для установки на АРМ локального обслуживания ViPNet SIES Core и ViPNet SIES Unit. Применяется совместно с ViPNet SIES MC.

Используется для инициализации (см. глоссарий, стр. 47) ViPNet SIES Core и ViPNet SIES Unit перед вводом в эксплуатацию, а также для локального обслуживания ViPNet SIES Core и ViPNet SIES Unit в ходе эксплуатации. ViPNet SIES Workstation позволяет транслировать команды ViPNet SIES MC на ViPNet SIES Core и ViPNet SIES Unit в отсутствие связи между этими компонентами и ViPNet SIES MC.

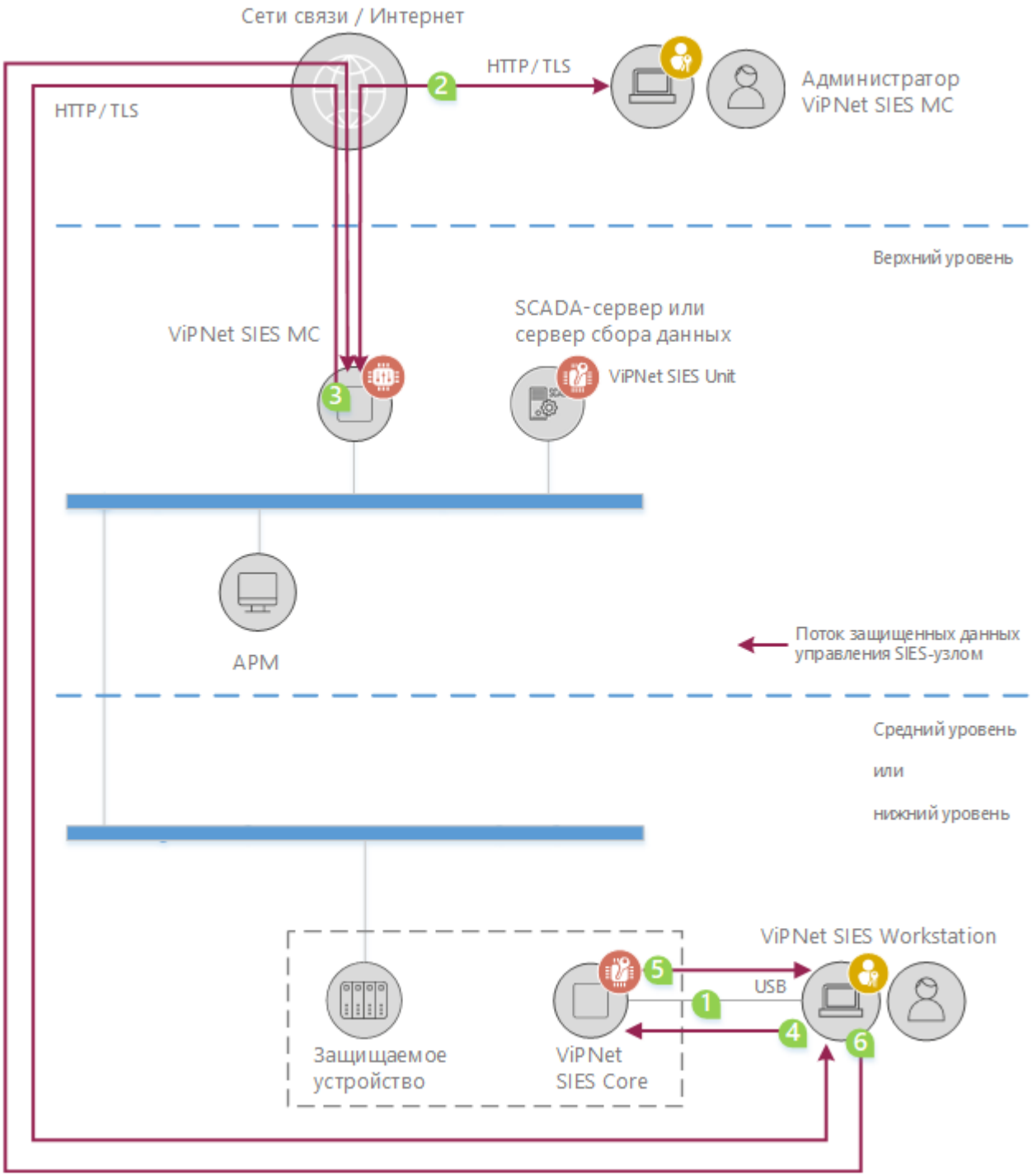

Рисунок 5. Локальное управление SIES-узлом

Управлять ViPNet SIES Core на индустриальных объектах без отправки команд по каналам связи системы можно в следующей последовательности:

1 ViPNet SIES Core подключается к ViPNet SIES Workstation обособленно от защищаемого устройства. ViPNet SIES Workstation подключается к ViPNet SIES MC по протоколу TLS.

2 Администратор ViPNet SIES MC с рабочего места подключается к веб-интерфейсу ViPNet SIES MC по протоколу TLS и выполняет операцию управления SIES-узлом.

3. ViPNet SIES MC формирует команду управления, упаковывает команду в защищенный конверт в адрес SIES-узла. ViPNet SIES Workstation получает от ViPNet SIES MC команду управления для ViPNet SIES Core.
4. ViPNet SIES Workstation транслирует ViPNet SIES Core команду управления ViPNet SIES MC. ViPNet SIES Core обрабатывает команду ViPNet SIES MC.
5. ViPNet SIES Core возвращает результат обработки команды на ViPNet SIES Workstation.
6. Результат выполнения команды загружается с ViPNet SIES Workstation на ViPNet SIES MC для обработки и отображения администратору ViPNet SIES MC.

Управление ViPNet SIES Unit выполняется аналогично.

Организация защиты данных индустриальной системы с применением ViPNet SIES

Защита данных на устройствах среднего и нижнего уровней системы строится на применении ViPNet SIES Core и ViPNet SIES Unit. После интеграции в каждое защищаемое устройство ViPNet SIES Core и ViPNet SIES Unit становятся базовыми элементами системы защиты данных индустриальных устройств.

Защита данных на устройствах верхнего уровня системы — OPC-серверы, SCADA-серверы, системы мониторинга и сбора информации — организуется с помощью ViPNet SIES Unit.

Пример организации защиты данных индустриальной системы с помощью компонентов комплекса ViPNet SIES приведен на рисунке ниже. Защита данных в IIoT-системах организуется аналогичным образом.

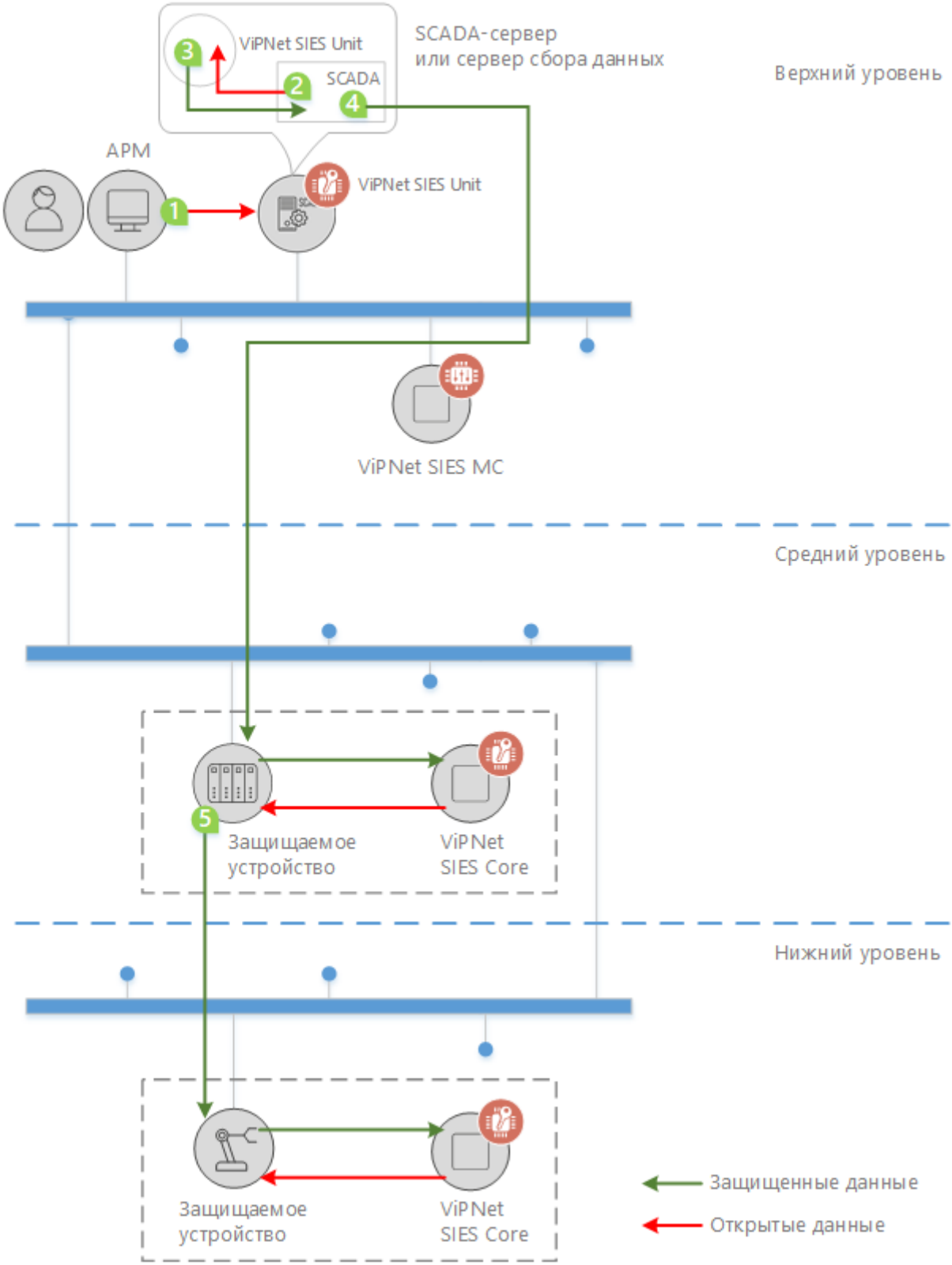

Рисунок 6. Защита данных индустриальной системы с помощью компонентов ViPNet SIES

Цифрами на схеме обозначены элементы потока данных, защищаемых развернутыми SIES-узлами. Организация защиты данных с помощью комплекса ViPNet SIES зависит от индивидуальных

особенностей системы. Например, защита команды диспетчера системы может проходить в следующей последовательности:

1. Диспетчер отправляет команду управления программируемым логическим контроллером (ПЛК) с АРМ диспетчера в SCADA-сервер.
2. SCADA-сервер в открытом виде отправляет данные ViPNet SIES Unit.
3. ViPNet SIES Unit возвращает защищенные данные SCADA-серверу.
4. SCADA-сервер передает защищенные данные ПЛК со встроенным ViPNet SIES Core. Получив защищенные данные, SIES-узел выполняет следующие действия:
   - По команде ПЛК ViPNet SIES Core обрабатывает защищенные данные и возвращает ПЛК открытую команду диспетчера.
   - ПЛК формирует команду управления исполнительным устройством.
   - ПЛК передает сформированную команду в открытом виде на обработку ViPNet SIES Core.
   - ViPNet SIES Core обрабатывает команду и возвращает ПЛК защищенные данные.
5. ПЛК передает защищенные данные исполнительному устройству со встроенным ViPNet SIES Core. Получив защищенные данные, SIES-узел выполняет следующие действия:
   - По команде исполнительного устройства ViPNet SIES Core обрабатывает защищенные данные и возвращает исполнительному устройству открытую команду ПЛК.
   - Исполнительное устройство выполняет команду ПЛК и формирует ответ с результатом исполнения команды.

Ответ исполнительного устройства диспетчеру отправляется в обратной последовательности в защищенном виде за счет применения функций ViPNet SIES Core.

В приведенном выше сценарии для передачи защищенных данных по каналам связи системы может потребоваться использование защищенного профиля протокола взаимодействия устройств системы (индустриального протокола).

Варианты использования защищенных профилей для некоторых распространенных протоколов приведены в документе «ViPNet SIES. Защита индустриальных протоколов».

Достоинства комплекса продуктов ViPNet SIES

Комплекс продуктов ViPNet SIES позволяет разработчику системы:

- интегрировать компоненты комплекса ViPNet SIES без значительной модификации топологии информационных потоков в систему, работающую по промышленным протоколам;
- реализовать различные сценарии защиты информации, в том числе с учетом мер, предусмотренных нормативными правовыми актами и документами;
- определять логику обработки защищаемой информации в зависимости от объема и критичности к задержке доставки, позволяющую выстраивать потоки информации в соответствии с требованиями к производственным процессам;
- определять логику процесса обработки защищаемой информации и реакции системы на факты нарушения информационной безопасности;
- определять логику оперативного отключения криптографической обработки данных защищаемых устройств в ходе эксплуатации для обеспечения доступности системы;
- централизованно управлять ключевой информацией.

SIES-узлы — функционально завершенные средства криптографической защиты информации, позволяющие защищаемым устройствам вызывать только разрешенные криптографические функции через прикладной интерфейс.

2

Защита критической информационной инфраструктуры

Об использовании комплекса ViPNet SIES для защиты значимого объекта критической информационной инфраструктуры 28

Идентификация и аутентификация (ИАФ) 29

Управление доступом (УПД) 31

Ограничение программной среды (ОПС) 32

Аудит безопасности (АУД) 33

Обеспечение целостности (ОЦЛ) 34

Обеспечение доступности (ОДТ) 35

Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) 37

Управление конфигурацией (УКФ) 39

Управление обновлениями программного обеспечения (ОПО) 40

Об использовании комплекса ViPNet SIES для защиты значимого объекта критической информационной инфраструктуры

С помощью комплекса ViPNet SIES можно обеспечить различные аспекты безопасности информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей, отнесенных к значимым объектам критической информационной инфраструктуры 1-й, 2-й и 3-й категорий значимости в соответствии со статьей 7 Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г.

Меры обеспечения безопасности приведены в приложении к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России № 239 «Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости» от 25 декабря 2017 г. с учетом изменений согласно приказа ФСТЭК России № 138 от 9 августа 2018 г. и приказа ФСТЭК России № 60 от 26 марта 2019 г.

В этом разделе приведены только те меры, для реализации которых можно использовать компоненты комплекса ViPNet SIES.

Для каждой меры в графе «Сценарий работы комплекса ViPNet SIES» приведены дополнительные пояснения и наименования сценариев защиты данных из документа «ViPNet SIES. Сценарии работы», которые следует реализовать для обеспечения указанной меры безопасности.

Идентификация и аутентификация (ИАФ)

Таблица 5. Меры обеспечения безопасности (ИАФ)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя • Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ Внешнего пользователя нужно предварительно зарегистрировать
ИАФ.2	Идентификация и аутентификация устройств	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение конфиденциальности (см. глоссарий, стр. 48) информации • Обеспечение целостности информации Аутентификацию обеспечивают протоколы CRISP (см. глоссарий, стр. 44) и CMS (см. глоссарий, стр. 44) с электронной подписью
ИАФ.3	Управление идентификаторами	+	+	+	• ViPNet SIES MC	• Поддержка реализации меры за счет возможности регистрации защищаемых устройств и функций ключевого центра

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ИАФ.4	Управление средствами аутентификации	+	+	+	• ViPNet SIES MC	• Поддержка реализации меры за счет возможности управления прикладной ключевой подсистемой SIES-узлов
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя • Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ Внешнего пользователя нужно предварительно зарегистрировать
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности информации Данные сценарии позволяют защитить информацию любого типа

Управление доступом (УПД)

Таблица 6. Меры обеспечения безопасности (УПД)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
УПД.1	Управление учетными записями пользователей	+	+	+	• ViPNet SIES MC	• Поддержка реализации меры путем управления учетными записями пользователей с помощью SIES-узлов типа «Пользователь». Мера реализуется на защищаемом устройстве
УПД.2	Реализация политик управления доступом	+	+	+	• ViPNet SIES MC	• Поддержка реализации меры с помощью управления прикладными связями между SIES-узлами. Мера реализуется на защищаемом устройстве
УПД.3	Доверенная загрузка		+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Реализуется на защищаемом устройстве за счет возможности проверки целостности и аутентичности ПО перед его загрузкой
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+	• ViPNet SIES MC	• Поддержка реализации меры с помощью SIES-узлов типа «Пользователь» и управления прикладными связями между SIES-узлами. Мера реализуется на защищаемом устройстве
УПД.13	Реализация защищенного удаленного доступа	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ

Ограничение программной среды (ОПС)

Таблица 7. Меры обеспечения безопасности (ОПС)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+	• ViPNet SIES Core • ViPNet SIES Unit	• Реализуется на защищаемом устройстве за счет возможности проверки целостности и аутентичности ПО перед его загрузкой
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление файла конфигурации • Доверенное обновление ПО защищаемого устройства

Аудит безопасности (АУД)

Таблица 8. Меры обеспечения безопасности (АУД)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
АУД.4	Регистрация событий безопасности	+	+	+	• ViPNet SIES MC • ViPNet SIES Core • ViPNet SIES Unit	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES
АУД.6	Защита информации о событиях безопасности	+	+	+	• ViPNet SIES MC • ViPNet SIES Core • ViPNet SIES Unit	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES

Обеспечение целостности (ОЦЛ)

Таблица 9. Меры обеспечения безопасности (ОЦЛ)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства • Обеспечение целостности информации • Внутренний контроль целостности ПО ViPNet SIES Core • Внутренний контроль целостности ПО ViPNet SIES Unit • Внутренний контроль целостности ПО ViPNet SIES MC
ОЦЛ.2	Контроль целостности информации				• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение целостности информации
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+	• ViPNet SIES MC	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+	• ViPNet SIES MC	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+	• ViPNet SIES MC	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES

Обеспечение доступности (ОДТ)

Таблица 10. Меры обеспечения безопасности (ОДТ)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+	• ViPNet SIES MC	• ViPNet SIES обеспечивает поддержку меры за счет возможности мониторинга компонентов комплекса ViPNet SIES в системе
ОДТ.4	Резервное копирование информации	+	+	+	• ViPNet SIES MC • ViPNet SIES Unit	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES • ViPNet SIES обеспечивает поддержку меры за счет возможности резервного копирования рабочей информации ViPNet SIES Unit и ViPNet SIES MC
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+	• ViPNet SIES MC • ViPNet SIES Unit	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES • ViPNet SIES обеспечивает поддержку меры за счет возможности восстановления рабочей информации ViPNet SIES Unit и ViPNet SIES MC из резервной копии с последующей синхронизацией прикладных связей на SIES-узлах

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+	• ViPNet SIES MC • ViPNet SIES Unit	• Мера защиты, реализованная для защиты самих продуктов комплекса ViPNet SIES

Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)

Таблица 11. Меры обеспечения безопасности (ЗИС)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+	• ViPNet SIES MC	• ViPNet SIES обеспечивает поддержку меры за счет возможности управления компонентами комплекса ViPNet SIES в системе с помощью ViPNet SIES MC
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение конфиденциальности информации
ЗИС.13	Защита неизменяемых данных		+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Контроль целостности неизменяемых данных • Обеспечение конфиденциальности информации • Обеспечение целостности информации
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности информации

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ЗИС.28	Исключение возможности отрицания отправки информации		+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства • Доверенное обновление файла конфигурации • Обеспечение неотказуемости от авторства данных
ЗИС.32	Защита беспроводных соединений	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности информации

Управление конфигурацией (УКФ)

Таблица 12. Меры обеспечения безопасности (УКФ)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя • Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ • Доверенное обновление ПО защищаемого устройства
УКФ.4	Контроль действий по внесению изменений				• ViPNet SIES Core • ViPNet SIES Unit	• Защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя • Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ • Доверенное обновление файла конфигурации • Доверенное обновление ПО защищаемого устройства

Управление обновлениями программного обеспечения (ОПО)

Таблица 13. Меры обеспечения безопасности (ОПО)

Обозначение и номер меры	Мера обеспечения безопасности значимого объекта	Категория значимости 3	Категория значимости 2	Категория значимости 1	Используемые компоненты комплекса ViPNet SIES	Сценарий работы комплекса ViPNet SIES и рекомендации по реализации
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства
ОПО.4	Установка обновлений программного обеспечения	+	+	+	• ViPNet SIES Core • ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства

A

История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet SIES.

Версия 2.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet SIES версии 2.2 по сравнению с версией 2.1.

- **Добавлен новый компонент комплекса ViPNet SIES**

  В набор компонентов комплекса ViPNet SIES добавлен программный модуль ViPNet SIES Unit — прикладная служба для криптографической обработки данных устройствами верхнего уровня индустриальных (см. глоссарий, стр. 47) и IIoT–систем (см. глоссарий, стр. 45):

  - SCADA-серверы (см. глоссарий, стр. 46);
  - автоматизированные рабочие места операторов;
  - автоматизированные рабочие места инженеров;
  - серверы сбора и обработки информации IIoT–систем.

  Подробнее см. раздел ViPNet SIES Unit (на стр. 18).

- **Изменен комплект документации**

  В комплект добавлен документ «ViPNet SIES. Руководство разработчика». Документ содержит методику интеграции в комплекс ViPNet SIES стороннего компонента для криптографической обработки данных защищаемого устройства и организации взаимодействия с другими защищаемыми устройствами, интегрированными с SIES-узлами. Документ предоставляется по запросу в компанию ИнфоТеКС.

Документ «ViPNet SIES. Защита индустриальных протоколов» также предоставляется по запросу в ИнфоТеКС.

Версия 2.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet SIES версии 2.1 по сравнению с версией 2.0.

- **Поддержка многоадресных защищенных рассылок между индустриальными устройствами**

  Реализована защита многоадресных сообщений и сообщений в рамках взаимодействия по подписочной модели.

  Для поддержки криптографической обработки данных на SIES-узлах при взаимодействии группы защищаемых устройств (см. глоссарий, стр. 47) реализована возможность добавления мультивещательных прикладных связей между защищаемыми устройствами.

  Подробнее см. документ «ViPNet SIES. Сценарии работы».

- **Поддержка сценариев защиты данных в индустриальных системах с резервированием защищаемых устройств**

  Для бесперебойной защиты данных в индустриальной системе с помощью комплекса ViPNet SIES реализована поддержка криптографической обработки данных на SIES-узлах, интегрированных с резервированными защищаемыми устройствами.

  Подробнее см. документ «ViPNet SIES. Сценарии эксплуатации».

- **Расширены рекомендации по защите индустриальных протоколов**

  Добавлены рекомендации по защите протоколов Modbus TCP и Modbus RTU с помощью комплекса ViPNet SIES.

  Подробнее см. документ «ViPNet SIES. Защита индустриальных протоколов».

- **Изменен комплект документации**

  В комплект добавлены следующие документы:

  - «ViPNet SIES. Пример интеграции с MasterSCADA», содержащий описание применения функций ViPNet SIES Core, ViPNet PKI Client SIES Unit и ViPNet SIES MC в прикладном проекте пакета программ ИнСАТ MasterSCADA;
  - «ViPNet SIES OPC UA Server. Пример реализации шлюзового компонента», содержащий описание примера реализации шлюзового компонента для обмена защищенными конвертами между ViPNet SIES MC и устройством операторского уровня индустриальной системы для доставки конвертов защищаемым устройствам по каналам связи индустриальной системы.

Версия 2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet SIES версии 2.0 по сравнению с версией 1.6.

- **Расширен набор компонентов комплекса ViPNet SIES**

  В набор компонентов комплекса ViPNet SIES добавлен программный комплекс ViPNet PKI Client с криптографическим модулем SIES Unit — средство защиты информации, обрабатываемой устройствами уровня операторского управления систем (например, SCADA, OPC, DCS, HMI).

  Подробнее см. раздел ViPNet PKI Client SIES Unit.

- **Расширены сценарии применения комплекса ViPNet SIES**

  Добавлены следующие бизнес-сценарии:

  - защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя;
  - защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ;
  - криптографическое преобразование пароля пользователя для хранения на защищаемом устройстве.

  Существующие бизнес-сценарии применения комплекса ViPNet SIES для защиты данных системы расширены за счет использования возможностей ViPNet PKI Client SIES Unit и расширения функциональных возможностей действующих компонентов комплекса ViPNet SIES.

  Подробнее см. документ «ViPNet SIES. Сценарии работы».

- **Изменен комплект документации**

  В комплект добавлены следующие документы:

  - «ViPNet SIES. Сценарии эксплуатации», содержащий описание решений типовых задач, возникающих в ходе эксплуатации комплекса ViPNet SIES в системе;
  - «ViPNet SIES. Практикум», содержащий пример внедрения комплекса ViPNet SIES в систему;
  - «ViPNet SIES. Защита индустриальных протоколов», содержащий рекомендации по применению решения ViPNet SIES для защиты данных, передаваемых по протоколам сетей передачи данных систем.

B

Глоссарий

API (Application Programming Interface)

Интерфейс прикладного программирования — набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. Используется программистами в ходе разработки приложений.

CMS (Cryptographic Message Syntax)

Стандарт, описывающий структуру криптографических сообщений (контейнеров), содержащих сведения для их корректного открытия или использования. Защищаемые данные могут передаваться как в составе CMS-сообщений, так и отдельно. С помощью CMS-сообщений можно организовать защищенный обмен данными между защищаемыми устройствами — участниками парной или резервированной парной прикладной связи. Создание и обработку CMS-сообщений выполняют SIES-узлы.

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.

HMI (Human-machine interface)

Человеко-машинный интерфейс (ЧМИ) — средство взаимодействия оператора с технической системой.

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).

OPC (Object linking and embedding for Process Control)

Семейство программных технологий, предоставляющих единый интерфейс управления объектами автоматизации и технологическими процессами. Object Linking and Embedding (OLE) — технология связывания и внедрения объектов в другие документы и объекты.

PAC (Programmable Automation Controller)

Промышленный контроллер автоматизации.

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

PLC (Programmable Logic Controller)

Программируемый логический контроллер (ПЛК).

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.

RTU (Remote Terminal Unit)

Устройство сбора и передачи информации (УСПИ) или устройство связи с объектом (УСО).

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.

VA (Virtual Appliance)

Виртуальное устройство — образ предварительно настроенной и готовой к использованию виртуальной машины с установленным специализированным программным обеспечением. Предназначен для установки на платформу виртуализации (гипервизор).

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 OPC UA Server

Шлюзовой компонент, обеспечивающий обмен защищенными конвертами между ViPNet SIES MC и SIES-узлами по протоколу OPC UA.

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.

Автоматизированное рабочее место (АРМ)

Программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида автоматизированной системы. Объединяет программно-аппаратные средства для взаимодействия человека с компьютером, предоставляя возможность ввода и вывода информации.

Аутентификация

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

Защищаемое устройство

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

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.

Индустриальный объект

Элемент инфраструктуры индустриальной системы, обеспечивающий полный цикл функционирования производства или отдельного технологического процесса.

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 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.

Криптография

Совокупность методов обеспечения конфиденциальности (невозможности прочтения посторонним), целостности (невозможности незаметного изменения), аутентификации (проверки подлинности авторства или иных свойств), а также невозможности отказа от авторства информации.

Неотказуемость

Неотрекаемость от авторства информации, а также факта отправки или получения информации.

Программно-аппаратный комплекс (ПАК)

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

Программное обеспечение (ПО)

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

Сертификат 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.

Средство криптографической защиты информации (СКЗИ)

Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем и выполнять криптографическое преобразование информации для обеспечения ее безопасности.

Удостоверяющий центр

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

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.