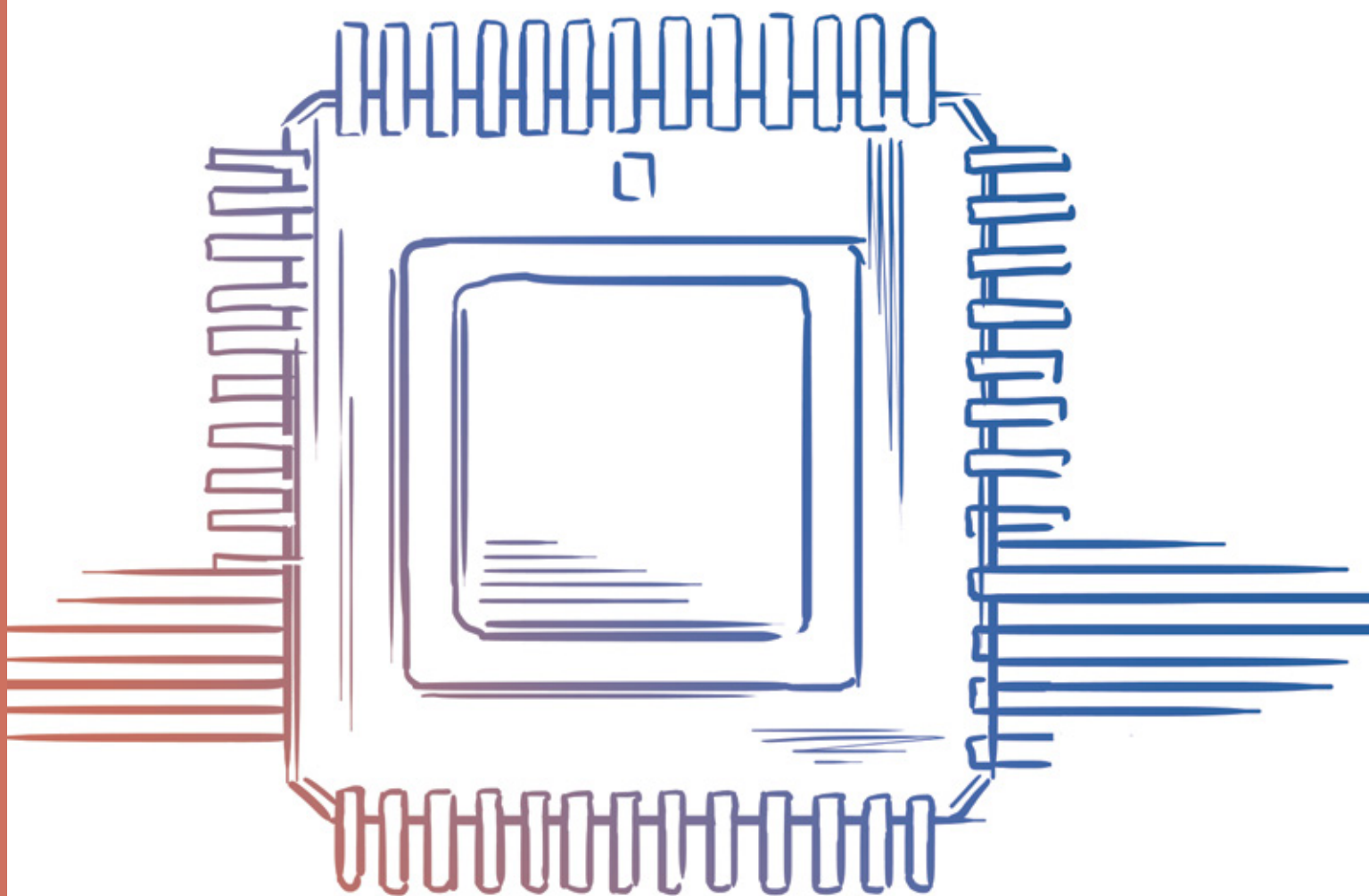


ViPNet SIES

Встраиваемые средства защиты
информации для промышленных систем



Решение ViPNet SIES

ViPNet SIES – это решение для криптографической защиты информации в АСУ ТП, М2М, IIoT, ИСУЭ и встраиваемых системах, позволяющее реализовать защиту на уровне конечных узлов и коммуникаций между ними

Компоненты решения ViPNet SIES предназначены для интеграции с защищаемыми устройствами АСУ ТП уровня оперативно-диспетчерского управления (SCADA/OPC-серверы, рабочие станции, АРМ), автоматического управления (программируемые логические контроллеры (PLC), терминалы (RTU), интеллектуальные полевые устройства) устройствами М2М, IIoT и ИСУЭ. ViPNet SIES предоставляет защищаемым устройствам возможность использования криптографических функций на уровне прикладного программного обеспечения для реализации различных сценариев информационной безопасности.

Решение ViPNet SIES включает в себя следующие продукты:

- > **ПАК ViPNet SIES Core** – для встраивания в устройства уровня автоматического управления: ПЛК, терминалы, IIoT-шлюзы, коммуникационные шлюзы
- > **ПАК ViPNet SIES Core Nano** – для встраивания в устройства полевого уровня и IIoT-устройства: датчики, исполнительные устройства и пр.
- > **ПО ViPNet SIES Unit** – для интеграции с устройствами уровня оперативно-диспетчерского управления: SCADA/OPC-серверами, серверами сбора данных, серверами телемеханики, рабочими станциями, АРМ
- > **ПО ViPNet SIES Unit Router** – для масштабирования ViPNet SIES Unit, обеспечивает единую точку входа при подключении нескольких ViPNet SIES Unit к защищаемому устройству
- > **СКЗИ ViPNet SIES MC** – для централизованного управления ключевой информацией и жизненным циклом СКЗИ ViPNet SIES
- > **ПО ViPNet SIES Workstation** – для первоначальной загрузки ключевой информации в СКЗИ ViPNet SIES Core и ViPNet SIES Unit и их локального обслуживания
- > **ПАК ViPNet SIES Nano Loader** – для загрузки ключевой информации в СКЗИ ViPNet SIES Core Nano

ViPNet SIES предоставляет защищаемым устройствам возможность использования криптографических функций на уровне прикладного ПО для реализации различных сценариев ИБ устройств в концепции secure by design. Сценарии защиты информации

можно организовать в промышленной системе с любой архитектурой независимо от сферы функционирования объекта управления. Решение ViPNet SIES применимо независимо от структуры промышленной системы и управляемого ей процесса.



ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

- > API, содержащий целевые криптографические и служебные функции
 - > Защищенное хранение ключевой информации
 - > Пассивная работа в режиме ответа на запросы
 - > Автоматизированное централизованное управление жизненным циклом ключевой информации
 - > Удаленный централизованный мониторинг состояния и администрирование компонентов
 - > Открытый API для интеграции СКЗИ сторонних разработчиков
 - > Возможность коммуникаций точка-точка, звезда, шина, мультикаст, подписочная модель
 - > Криптографические алгоритмы: ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
 - > Промышленный криптографический протокол CRISP (ГОСТ Р 71252–2024 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для промышленных систем») с малым объемом дополнительных данных
-

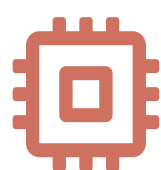
ФУНКЦИИ

ViPNet SIES выполняет криптографические операции по алгоритмам ГОСТ:

- > зашифрование и расшифрование блока данных по криптографическому протоколу CRISP
 - > вычисление и проверка имитовставки для блока данных по криптографическому протоколу CRISP
 - > зашифрование и расшифрование блока данных по криптографическому протоколу CMS
 - > вычисление и проверка значения хэш-кода для блока данных
 - > создание и проверка усиленной неквалифицированной электронной подписи (ЭП) по криптографическому протоколу CMS
-

ПРЕИМУЩЕСТВА

- > Гибкий подход к реализации сценариев защиты информации, в том числе удовлетворяющих нормативно-правовым документам
- > Отсутствие влияния на штатный режим функционирования промышленной системы
- > Учет особенностей функционирования программного обеспечения и технических средств промышленной системы
- > Совместимость с промышленными протоколами, позволяющая интегрировать СКЗИ в промышленную систему без модификации топологии информационных потоков
- > Работа в сложных условиях окружающей среды с ограничениями по электропитанию, габаритам и особыми условиями обслуживания
- > Управление СКЗИ независимо от управления промышленной системой
- > Легкость масштабирования при модернизации промышленной системы
- > Управление, хранение и защита криптографических ключей, поддержание жизненного цикла криптографической инфраструктуры без использования ресурсов промышленной системы
- > Соответствие требованиям ФСБ России к СКЗИ
- > Криптографическая обработка данных в соответствии с российскими ГОСТ и рекомендациями Технического комитета Росстандарта «Криптографическая защита информации» (ТК 026)
- > Возможность выбора объема и типа защищаемых данных в зависимости от специфики промышленной системы

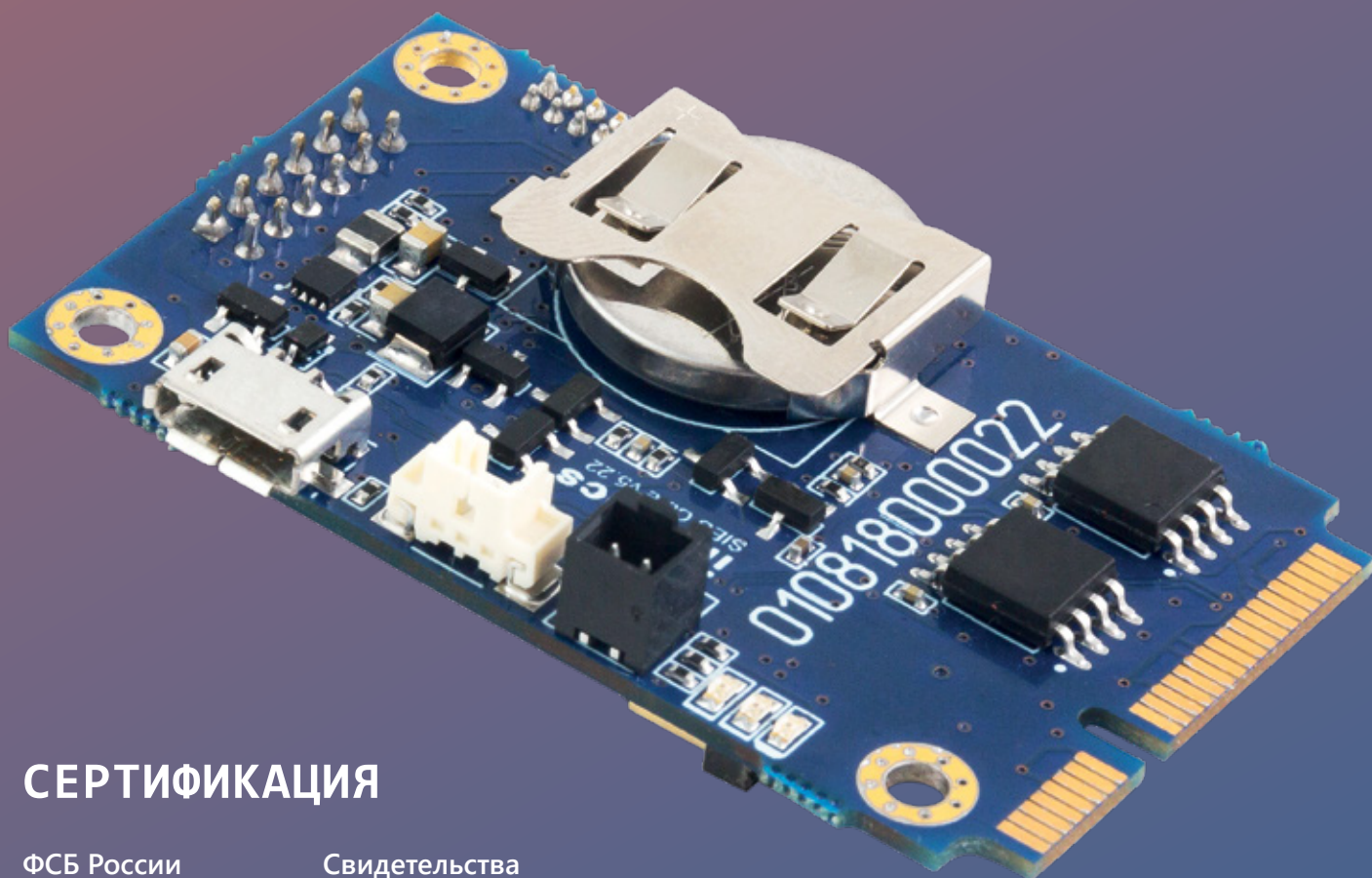


VIPNet SIES Core

Программно-аппаратный комплекс (ПАК) VIPNet SIES Core предназначен для интеграции с такими защищаемыми устройствами, как программируемые логические контроллеры (PLC), промышленные контроллеры автоматизации (PAC), терминалы (RTU), интеллектуальные устройства (IED), IIoT-устройства, устройства сбора и передачи данных (УСПД), оконечное оборудование (различные исполнительные устройства)

ПРЕИМУЩЕСТВА

01. ПАК ViPNet SIES Core является функционально законченным средством криптографической защиты информации (СКЗИ) и может эксплуатироваться вне контролируемой зоны
02. Все криптографические вычисления и хранение дополнительной информации осуществляются внутри ПАК ViPNet SIES Core, что позволяет не расходовать вычислительные ресурсы защищаемого им устройства на выполнение криптографических преобразований информации.
03. ПАК ViPNet SIES Core является пассивным устройством и работает в режиме ответа на запросы защищаемого им устройства. При этом объем и тип защищаемых данных самостоятельно определяется разработчиком АСУ или М2М.
04. Для реализации сценариев защиты информации защищаемое устройство вызывает требуемые криптографические функции при помощи API-интерфейса.
05. Поддерживает работу с промышленными протоколами. Для защиты передаваемых данных используется промышленный криптографический протокол с малым объемом вспомогательных данных.
06. Обеспечивает информационную безопасность на уровне данных, не требуя внесения изменений на канальном уровне коммуникаций информационной системы.
07. ПАК ViPNet SIES Core не зависит от архитектуры и операционной системы защищаемого устройства. ViPNet SIES Core можно интегрировать в защищаемые устройства без операционной системы (bare metal).



СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ класса КСЗ

Свидетельства
> В реестре российского ПО
> В реестре Минпромторга

ПРИНЦИП РАБОТЫ

ПАК ViPNet SIES Core интегрируется с защищаемыми устройствами через межплатные интерфейсы и в пассивном режиме выполняет запросы на криптографические операции с данными. Защищаемое устройство обращается к ПАК ViPNet SIES Core через API-интерфейс напрямую или с использованием SIES Core SDK. Структуру и состав данных (команды управления, телеметрическую информацию, сервисные команды) определяет разработчик АСУ ТП или М2М.

ViPNet SIES Core выполняет запрошенную операцию и возвращает результат в виде криптографического преобразования обработанных данных или их анализа. В зависимости от запрошенной криптографической операции защищаемое устройство может использовать результат обработки блока данных для принятия решения о достоверности данных, либо использовать результат обработки блока данных в защищенном обмене с другими защищаемыми устройствами.

Технические характеристики

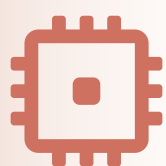
Микроконтроллер	STMicroelectronics STM32 F4 или GigaDevice GD32 F4	
Хранение данных	SPI NOR Flash 16 МБ	
Операционная система	FreeRTOS	
Криптографические алгоритмы	ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ 34.10-2018, ГОСТ 34.11-2018	
Интерфейс интеграции с защищаемым устройством	ViPNet SIES Core: UART, USB, SPI ViPNet SIES Core PCIe: USB, I2C (mini-PCIe)	
Напряжение питания (постоянный ток)	4–15 В (основное питание) 3–5 В (резервное питание)	
Потребляемый ток	В рабочем режиме: - не более 60 мА (STM32F4) - не более 80 мА (GD32F4)	В режиме энергосбережения: - не более 60 мкА (STM32F4) - не более 6 мА (GD32F4)

Размерные характеристики

Типоразмер	PCI Express® Full-Mini Card
Габариты (Д x Ш x В), мм	51 x 30 x 11,2
Масса	Не более 7 г (без встраиваемой батареи)
Условия эксплуатации	Диапазон рабочих температур -40..+70 °С Допустимая относительная влажность воздуха в помещении эксплуатации до 98% при температуре 25 °С

Производительность ViPNet SIES Core*	UART	USB	SPI
Скорость шифрования в криптографическом контексте, Кбит/с	216	505	667
Скорость расшифрования в криптографическом контексте, Кбит/с	205	456	571
Скорость выработки имитовставки, Кбит/с	400	864	1143
Скорость проверки имитовставки, Кбит/с	348	741	889
Скорость хеширования, Кбит/с	290	912	1143
Время формирования электронной подписи, мс	94	78	75
Время проверки электронной подписи, мс	160	145	142

*Оценка производительности при обработке блока данных 1024 байт



VIPNet SIES Core Nano

Криптографический чип для защиты информации устройств автоматизации, IoT и приборов учета

Средство криптографической защиты информации, реализованное в виде миниатюрного чипа российского производства

Чип ViPNet SIES Core Nano входит в состав решения ViPNet SIES и предназначен для монтажа на печатную плату защищаемого оконечного оборудования автоматизированных систем управления (АСУ), приборов учета электроэнергии, устройств интернета вещей (IoT), в том числе промышленного интернета вещей (IIoT).

Программный интерфейс ViPNet SIES Core Nano состоит из высокоуровневых команд, не требующих от разработчиков прикладного ПО защищаемых устройств глубоких знаний в области криптографии, управления жизненным циклом ключей и прочих специфических навыков.

Взаимодействие с чипом ведется на уровне простых понятных команд, таких как зашифровать/расшифровать блок данных, вычислить/проверить имитовставку, вычислить/проверить хэш-код для блока данных.

Все криптографические функции выполняются непосредственно крипточипом, ключевая информация хранится в специальной защищенной области памяти чипа, а срок ее хранения может достигать 16 лет.

ОСНОВНЫЕ ФУНКЦИИ

ViPNet SIES Core Nano выполняет следующие функции обеспечения конфиденциальности и/или целостности данных:

- > вычисление и проверку имитовставки для блока данных по протоколу CRISP
- > зашифрование и расшифрование блока данных по протоколу CRISP
- > контроль и защиту от навязывания повторных сообщений
- > вычисление и проверку значения хэш-кода для блока данных

Используя криптографические функции ViPNet SIES Core Nano, можно реализовывать следующие меры защиты информации:

- > обеспечение целостности данных
- > обеспечение конфиденциальности данных
- > защита данных от подмены
- > обеспечение идентификации и аутентификации источника данных

ПРИНЦИП РАБОТЫ

ViPNet SIES Core Nano реализован в виде системы на кристалле (System-on-a-Chip, SoC), монтируемой на печатную плату защищаемого устройства. Для интеграции крипточипа с защищаемым устройством используется интерфейс SPI.

ViPNet SIES Core Nano работает в пассивном режиме, выполняя криптографическую обработку данных по команде защищаемого устройства. Защищаемое устройство через документированный интерфейс (Application Programming Interface, API) отправляет крипточипу блок данных и код команды, определяющий требуемую обработку блока данных. ViPNet SIES Core Nano выполняет запрошенную криптографическую операцию над переданным блоком данных и возвращает защищаемому устройству результат в виде преобразованного блока данных или результата его обработки.

Структуру и состав данных для защиты (команды управления, телеметрическую информацию, сервисные команды) задает разработчик защищаемого устройства. Он же определяет алгоритмы обработки результата запрошенной криптографической операции прикладным ПО защищаемого устройства.

Защиту данных крипточип обеспечивает с помощью криптографического протокола CRISP (ГОСТ Р 71252–2024). Протокол CRISP имеет минимальный объем накладных расходов и не требует установления сессии между защищаемыми устройствами, что позволяет применять его для защиты большинства известных IoT-протоколов (LoRaWAN, XNB, NB-IoT и др.)

Ключевая информация ViPNet SIES Core Nano вырабатывается во внешнем ключевом центре ViPNet SIES HSM и загружается в крипточип при помощи APM загрузки ключей ViPNet SIES Nano Loader. Мониторинг работы крипточипа в процессе эксплуатации, загрузка временных ключей связи, настройка привязки к защищаемому устройству, а также связей с другими SIES-узлами выполняется централизованно из единого центра управления ViPNet SIES MC.

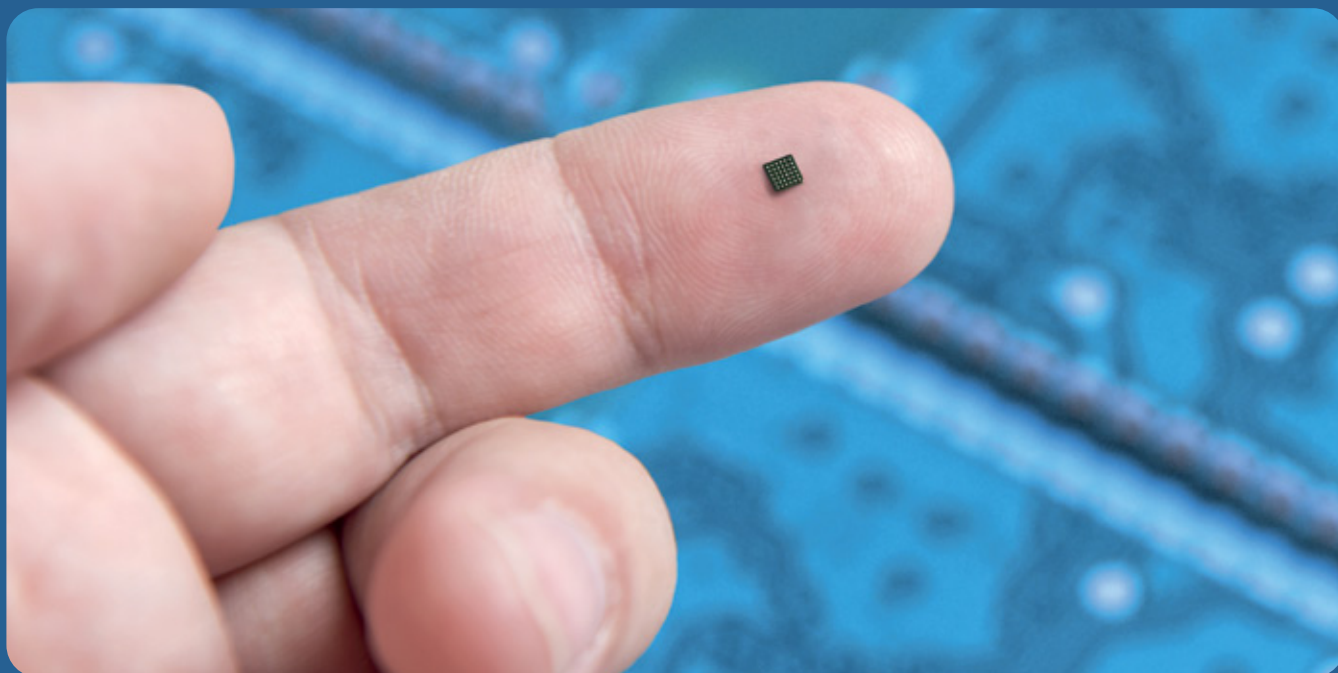
ПРЕИМУЩЕСТВА

- > низкое энергопотребление
- > не требует обслуживания
- > высокий класс защиты
- > эксплуатация вне контролируемой зоны
- > не требует смены ключей в течение всего срока службы изделия
- > протокол CRISP, подходящий для защиты данных в большинстве известных IoT-протоколов
- > централизованное управление из ViPNet SIES MC
- > полностью российская разработка

Ключи в ViPNet SIES Core Nano хранятся в специальной защищенной области памяти в неизменяемом и неизвлекаемом виде. Благодаря высокой степени защиты от инженерного проникновения в соответствии с требованиями к СКЗИ-НР крипточип может эксплуатироваться вне контролируемой зоны, а срок хранения и использования ключевой информации может достигать 16 лет.

СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ класса КСЗ



ХАРАКТЕРИСТИКИ

Форм-фактор

Исполнение	микросхема
Корпус	QFN40
Число выводов	40
Габаритные размеры корпуса (Д x Ш x В), мм	6 x 6 x 0,75
Расстояние между выводами, мм	0,5
Рабочая температура, °C	–40..+85

Интерфейсы взаимодействия

Интерфейс связи с защищаемым устройством	SPI
Интерфейс управления ViPNet SIES MC	SPI (через защищаемое устройство)
Криптографические протоколы	ГОСТ Р 71252–2024 (CRISP, наборы 3 и 4)
Криптографические алгоритмы	ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ 34.11-2018

Ключевая информация

Прикладной основной ключ защиты и прикладной резервный ключ защиты устройства (3 комплекта)	срок службы 16 лет
Служебный основной ключ защиты и служебный резервный ключ защиты для управления из ViPNet SIES MC	срок службы 16 лет

Питание

Питание (постоянный ток), В	3,3
-----------------------------	-----

Соответствие требованиям

Класс СКЗИ	КСЗ
Защита от атак инженерного проникновения	в соответствии с требованиями к СКЗИ-НР
Страна происхождения	Российская Федерация



VipNet SIES Unit

Программный комплекс (ПК) VipNet SIES Unit предназначен для защиты устройств уровня оперативно-диспетчерского управления АСУ ТП, таких как SCADA-серверы, OPC-серверы, рабочие станции, АРМ

ПРИНЦИП РАБОТЫ

ПК ViPNet SIES Unit работает под управлением операционных систем Windows и Linux. ПК ViPNet SIES Unit устанавливается на выделенный сервер или непосредственно на защищаемые устройства – серверы и рабочие станции уровня оперативно-диспетчерского управления АСУ ТП, например, SCADA-сервер, OPC-сервер, АРМ оператора, АРМ инженера и др. Защищаемое устройство взаимодействует с ПК ViPNet SIES Unit на уровне прикладного программного обеспечения (ПО) посредством программного интерфейса приложения API.

ПК ViPNet SIES Unit работает в пассивном режиме, выполняя криптографические операции с данными по запросу прикладного ПО защищаемого устройства. Структуру и состав данных (команды управления, телеметрическая информация, сервисные команды и др.), а также метод защиты определяет разработчик АСУ ТП или М2М.

ПК ViPNet SIES Unit выполняет запрошенную операцию и возвращает результат в виде криптографического преобразования обработанных данных или их анализа. В зависимости от запрошенной криптографической операции защищаемое устройство может использовать результат обработки блока данных для принятия решения о достоверности данных либо использовать результат обработки блока данных в защищенном обмене с другими защищаемыми устройствами.

ПРЕИМУЩЕСТВА

- > Функционально законченное средство криптографической защиты информации (СКЗИ)
- > Работает как программный сервис, в пассивном режиме отвечая на запросы прикладного ПО защищаемого им устройства. При этом объем и тип защищаемых данных самостоятельно определяется разработчиком АСУ ТП или М2М
- > Для реализации сценариев защиты информации защищаемое устройство вызывает требуемые криптографические функции при помощи API-интерфейса
- > Поддерживает работу с промышленными протоколами. Для защиты передаваемых данных используется промышленный криптографический протокол CRISP с малыми объемом вспомогательных данных
- > Обеспечивает информационную безопасность на уровне данных, не требуя внесения изменений на канальном уровне коммуникаций информационной системы

СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ классов КС1 и КС3

Свидетельства
В реестре российского ПО

ХАРАКТЕРИСТИКИ

Поддерживаемые операционные системы

Windows 10
Windows Server 2012/2012 R2/2016
Astra Linux Special Edition (Смоленск) 1.6/1.7
Альт 8 СП
Debian 10.13/11.6 (x86-64, armhf)
Ubuntu 16.04 LTS/18.04 LTS

Поддержка сред виртуализации KVM

Host OS	Guest OS
Astra Linux Special Edition (Смоленск) 1.7, Альт 8 СП	Astra Linux Special Edition (Смоленск) 1.7, Альт 8 СП, Debian 11

Интерфейс взаимодействия

RESTfull API (HTTP/1.1), gRPC API (HTTP/2)

Криптографические алгоритмы

ГОСТ 34.12-2018, ГОСТ 34.13-2018,
ГОСТ 34.10-2018, ГОСТ 34.11-2018

Варианты установки

на защищаемое устройство или выделенный сервер

Исполнения по количеству поддерживаемых связей

50, 500, 2000, 10 000, 100 000, 1 000 000

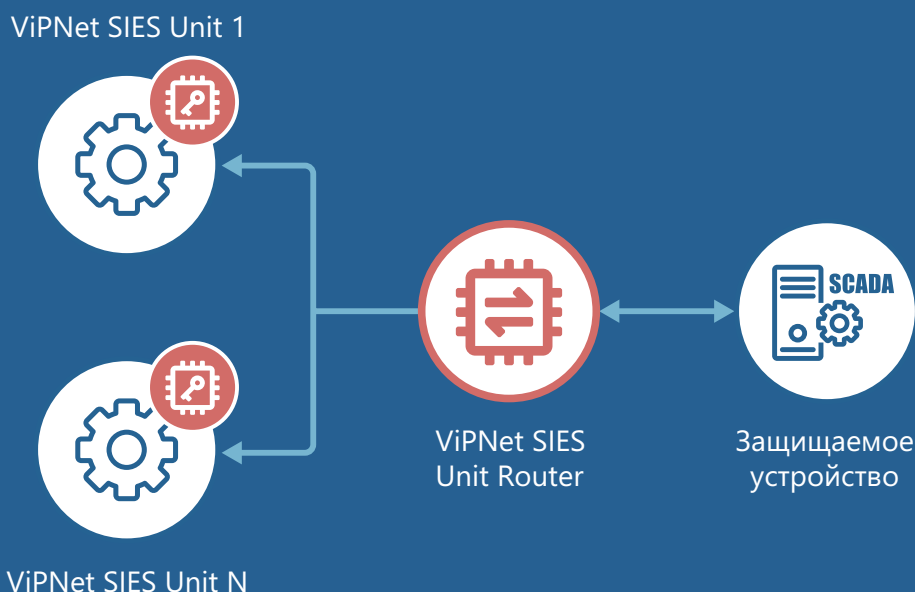
ViPNet SIES Unit Router

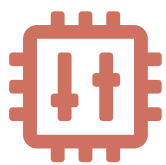
Программный комплекс, обеспечивающий масштабирование ViPNet SIES Unit

>> ViPNet SIES Unit Router позволяет повысить производительность ViPNet SIES Unit за счет масштабирования. Если производительности ViPNet SIES Unit недостаточно, распределите запросы защищаемого устройства на криптографические операции между несколькими ViPNet SIES Unit с помощью ViPNet SIES Unit Router.

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

- > Масштабирование ViPNet SIES Unit
- > Единая точка входа для запросов с защищаемых устройств
- > Распределение нагрузки для работы навстречу 2 млн. SIES-узлов
- > Поддержка API-интерфейса ViPNet SIES Unit для интеграции с защищаемыми устройствами: RESTfull API (HTTP/ 1.1), gRPC (HTTP/2)
- > Самостоятельная генерация карты маршрутизации запросов
- > Возможность объединения в кластер (до 20 узлов ViPNet SIES Unit Router)
- > Поддерживаемые операционные системы: Astra Linux Special Edition («Смоленск») 1.7, Альт 8 СП





VipNet SIES MC

VipNet SIES MC позволяет управлять жизненным циклом продуктов SIES и СКЗИ сторонних разработчиков как единой платформой: разворачивает решение VipNet SIES и СКЗИ других производителей доверенным образом, обеспечивает ввод в эксплуатацию компонентов решения VipNet SIES и СКЗИ сторонних производителей и позволяет обновлять как сами компоненты решения, так и их ключевую информацию. VipNet SIES MC отвечает за управление компонентами решения на всех стадиях их жизненного цикла от ввода в эксплуатацию до вывода из обращения

ПРЕИМУЩЕСТВА

01. Быстрый ввод в эксплуатацию защищенной системы с СКЗИ
02. Снижение затрат на обслуживание СКЗИ за счет автоматизации, смены ключевой информации и периодического контроля
03. Повышение прозрачности в управлении СКЗИ за счет наличия функционала инвентаризации
04. Возможность интеграции в защищенную систему СКЗИ сторонних производителей для управления ими
05. Нет необходимости установки дополнительного ПО на рабочие места администратора системы безопасности. Для подключения администраторов можно использовать любой браузер
06. Подходит для работы в компаниях как с филиально-распределенными системами, так и для сервис-провайдеров

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

- > Разграничение доступа на основе ролевой модели
- > Удаленное подключение администраторов к ПАК ViPNet SIES MC с двухсторонней аутентификацией
- > Безопасный обмен данными с компонентами решения ViPNet SIES (ViPNet SIES Core, ViPNet SIES Core Nano, ViPNet SIES Unit), сторонними СКЗИ
- > API для интеграции с АСУ и IIoT-системами
- > Использование каналов АСУ и IIoT-систем как транспорта для взаимодействия с компонентами решения ViPNet SIES (ViPNet SIES Core, ViPNet SIES Core Nano, ViPNet SIES Unit) сторонними СКЗИ
- > Ключевой центр и технологический УЦ для АСУ и IIoT-систем
- > Аппаратный датчик случайных чисел в ПАК ViPNet SIES MC
- > Криптографические операции по алгоритмам ГОСТ

ОСНОВНЫЕ ФУНКЦИИ

- > Инициализация ViPNet SIES Core, ViPNet SIES Unit
- > Ввод в эксплуатацию компонентов решения ViPNet SIES
- > Мониторинг компонентов решения ViPNet SIES
- > Управление ключевой информацией и сертификатами компонентов решения ViPNet SIES
- > Вывод из эксплуатации компонентов решения ViPNet SIES
- > Обновление программного обеспечения компонентов решения ViPNet SIES
- > Организация защищенного взаимодействия между защищаемыми устройствами с помощью компонентов решения ViPNet SIES
- > Проведение мероприятий при компрометации компонентов решения ViPNet SIES

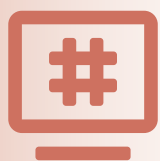
Функциональные характеристики

Исполнение	ViPNet SIES MC3000	ViPNet SIES MC10000	ViPNet SIES MC IoT	ViPNet SIES MC VA
СКЗИ	СКЗИ класса KC3	СКЗИ класса KC3	В процессе сертификации	СКЗИ класса KC1
Максимальное количество SIES-устройств	3 000	1 000 000	2 000 000	5 000
Максимальное количество узлов типа «Пользователь»	3 000	10 000	1 000 000	5 000
Максимальное количество администраторов безопасности	300	1000	2 000	500
Количество служб доставки	100	200	1 000	100
Форм-фактор	Desktop	1U Server	-	VA
Размеры (Ш x В x Г), мм	170 x 41,5 x 138	444 x 44 x 383	-	-
Аппаратная платформа	X86, 8 ГБ ОЗУ, 500 ГБ HDD, VGA 2x USB Console (RJ45)	x86, 32 ГБ ОЗУ, 2x2 ТБ HDD, 1x VGA 1 x PS/2 KB/Mouse 1x COM DB9 2x USB 3.0	x86, 64 ГБ ОЗУ, 2x 4 ТБ SSD, 1x VGA, 1 x PS/2 KB/Mouse 1x COM DB9 2x USB 3.0	Не менее: > 2-ядерный процессор; > 8 ГБ ОЗУ; > 50 ГБ на жестком диске; > 1x USB; > 2x Ethernet 10/100/1000 Мбит/с Платформа виртуализации: > VMWare vSphere ESXi 6.7 и 7.0; > VMWare Workstation 15.0 и 16.0; > Oracle VM VirtualBox 6.1.4
Аппаратный датчик случайных чисел	+	+	+	-
Масса, кг	0,5	7,5	7,8	-
Напряжение питания	100 – 240 В, 50 Гц	100 – 240 В, 50 Гц	100 – 240 В, 50 Гц	-
Мощность, Вт	36	310	310	-
Сетевые порты	4x Ethernet 10/100/1000 Мбит/с RJ45; 1xEthernet 1 Гбит/с SFP	4x Ethernet 10/100/1000 Мбит/с RJ45; 4xEthernet 1 Гбит/с SFP	4 x Ethernet 10/100/1000 Мбит/с RJ45; 4 x Ethernet 1 Гбит/с SFP	-
Поддерживаемые браузеры	Microsoft Internet Explorer версии 11 и выше, Microsoft Edge версии 12 и выше, Google Chrome версии 57 и выше на Windows и Linux, Firefox версии 45 и выше на Windows и Linux			

СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ класса KC1 и KC3

Свидетельства
> В реестре российского ПО
> В реестре Минпромторга



VipNet SIES Workstation

АРМ для подготовки к эксплуатации
и локального обслуживания VipNet
SIES Core и VipNet SIES Unit

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Подготовка к эксплуатации

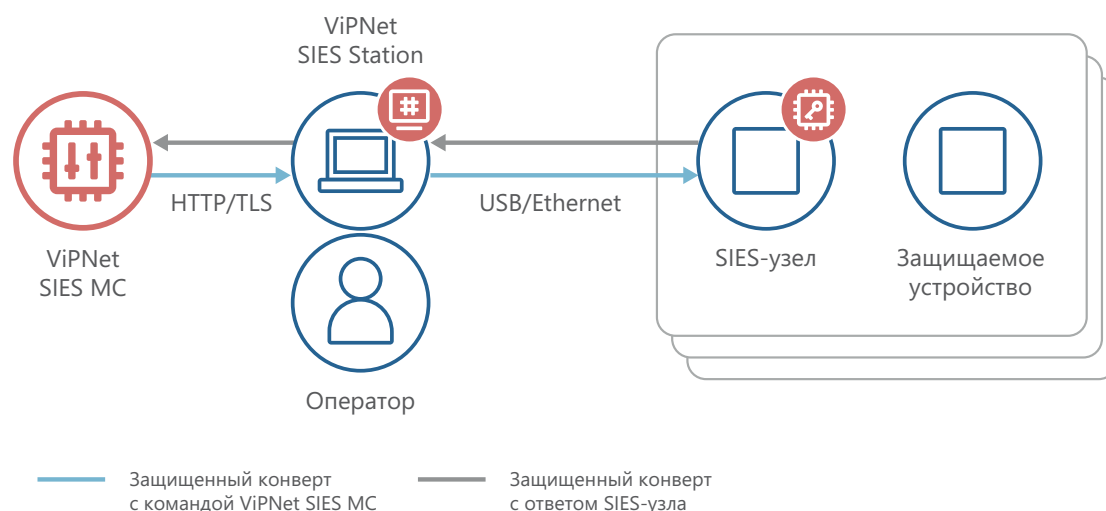
- > Инициализация ViPNet SIES Core
- > Выбор интерфейсов передачи данных ViPNet SIES Core для взаимодействия с защищаемым устройством и ViPNet SIES Workstation
- > Инициализация ViPNet SIES Unit

Обслуживание

- > Передача команд ViPNet SIES MC на ViPNet SIES Core в отсутствие канала связи между защищаемым устройством и ViPNet SIES MC
- > Передача команд ViPNet SIES MC на ViPNet SIES Unit в отсутствие канала связи между защищаемым устройством и ViPNet SIES MC

ПРЕИМУЩЕСТВА

01. Удобный и интуитивно понятный веб-интерфейс
02. Обеспечение инициализации SIES-узлов на стороне заказчика
03. Возможность локального управления настройками и ключевой информацией SIES-узлов при отсутствии каналов связи с центром управления ViPNet SIES MC
04. Облегчение процесса инициализации и сокращение времени на ввод в эксплуатацию SIES-узлов



VIPNet

SIES

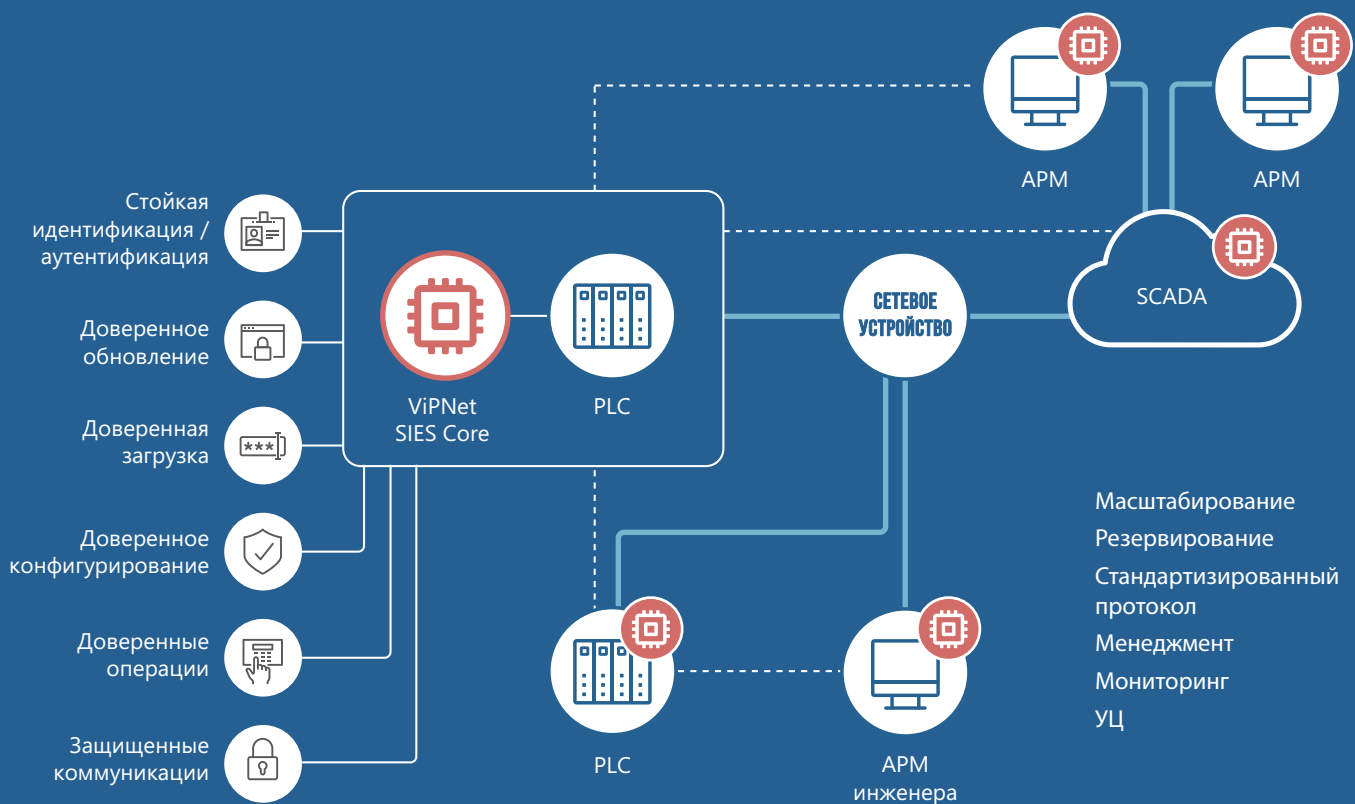
Сценарии

использования

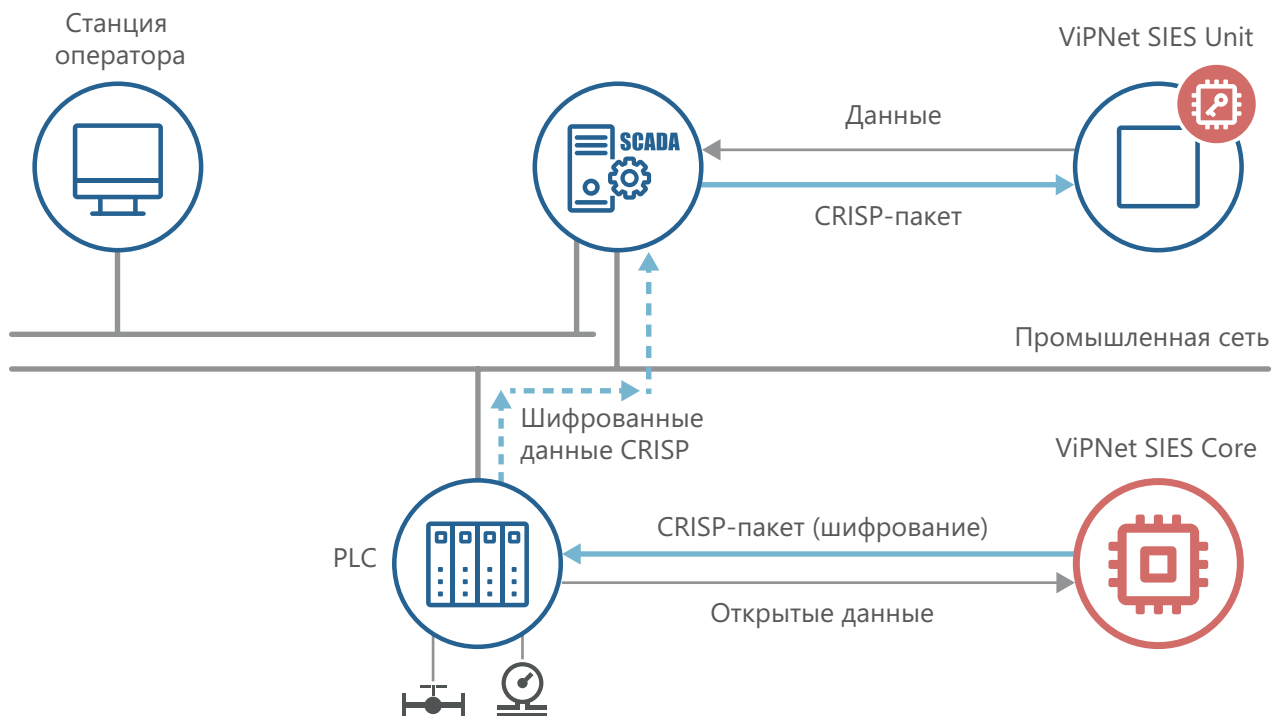
СЦЕНАРИИ

С помощью решения ViPNet SIES можно реализовать следующие сценарии защиты информации:

- | | |
|---|--|
| 01. Идентификация и аутентификация устройств и пользователей | 05. Защита коммуникаций:
> обеспечение целостности данных, передаваемых между защищаемыми устройствами
> обеспечение конфиденциальности данных, передаваемых между защищаемыми устройствами
> обеспечение неотрекаемости от авторства данных, передаваемых между защищаемыми устройствами |
| 02. Доверенная загрузка защищаемого устройства | |
| 03. Доверенное обновление программного обеспечения защищаемого устройства | |
| 04. Доверенное конфигурирование защищаемого устройства | |



ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ



Обеспечение конфиденциальности передаваемой информации

Между PLC и SCADA-сервером передается конфиденциальная информация, например, составляющая коммерческую тайну предприятия. Необходимо защитить информацию от доступа к ней третьих лиц при передаче по незащищенной промышленной сети. Для обеспечения конфиденциальности передаваемой между PLC и SCADA-сервером информации выполняется шифрование передаваемых данных с использованием протокола CRISP.

Для этого:

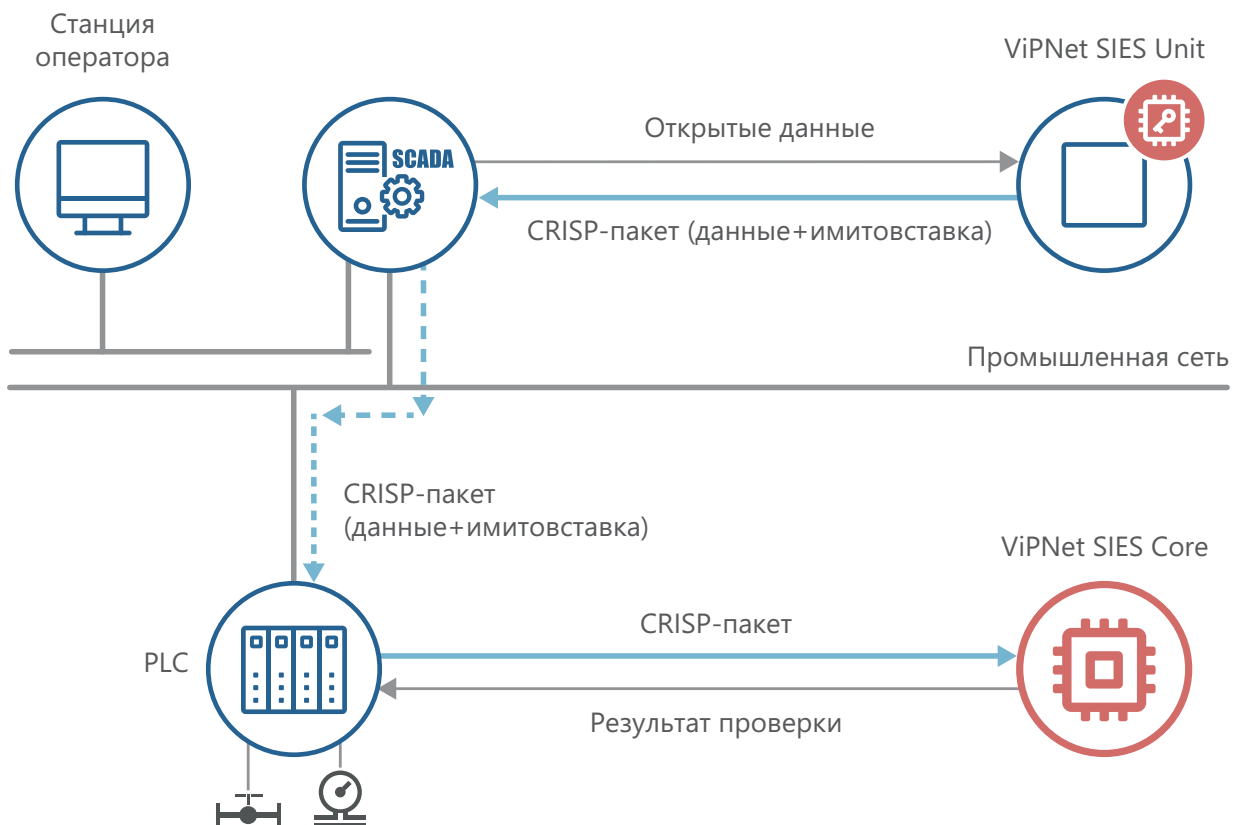
- > На SCADA-сервер устанавливается ПК ViPNet SIES Unit
- > В PLC интегрируется ПАК ViPNet SIES Core
- > Данные перед отправкой из PLC в SCADA передаются в ПАК ViPNet SIES Core, где они шифруются с использованием протокола CRISP, и возвращаются в PLC
- > Зашифрованные с использованием протокола CRISP данные передаются по существующей незащищенной промышленной сети из PLC в SCADA
- > SCADA получает от PLC зашифрованные данные и передает их в ПК ViPNet SIES Unit для расшифровки
- > ПК ViPNet SIES Unit возвращает SCADA расшифрованные данные

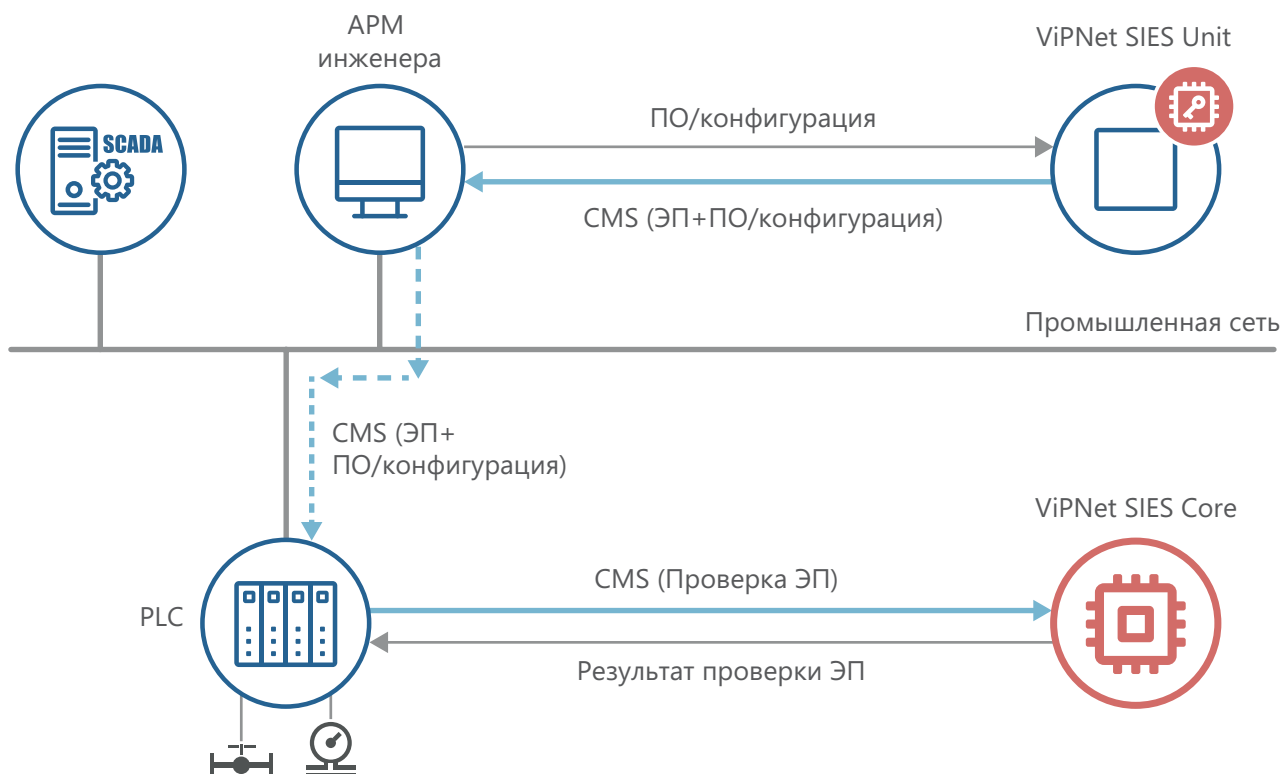
Обеспечение целостности передаваемой информации

Обеспечение целостности передаваемых команд управления технологическим процессом или новых установок технологического процесса и защита от перехвата и несанкционированного изменения осуществляется при помощи имитозащиты с использованием протокола CRISP.

Для этого:

- > На SCADA-сервер устанавливается ПК ViPNet SIES Unit
- > В PLC интегрируется ПAK ViPNet SIES Core
- > Данные перед отправкой из SCADA в PLC передаются в ПК ViPNet SIES Unit, где для них вычисляется имитовставка. ПК ViPNet SIES Unit формирует CRISP-пакет, включающий данные и имитовставку, и возвращает его в SCADA
- > CRISP-пакет, включающий данные и имитовставку, передается по существующей незащищенной промышленной сети из SCADA в PLC. PLC получает от SCADA CRISP-пакет и передает его в ПAK ViPNet SIES Core для проверки имитовставки
- > Результат проверки возвращается в PLC. В случае положительного результата информация считается переданной без искажений и может быть использована в технологическом процессе





Доверенное обновление ПО или конфигурации

Для защиты передаваемого файла с новой версией ПО или конфигурации контроллера от несанкционированного изменения или подмены используется электронная подпись (ЭП)

- > С этой целью прикладное ПО АРМ инженера перед отправкой файла в PLC передает его в ПК ViPNet SIES Unit для вычисления ЭП
- > ПК ViPNet SIES Unit формирует защищенный ЭП конверт CMS Signed Data и возвращает его в прикладное ПО для передачи в PLC
- > Защищенный CMS-конверт передается в PLC по промышленной сети
- > PLC передает полученный CMS-конверт в интегрированный в него ПАК ViPNet SIES Core для проверки ЭП
- > ПАК ViPNet SIES Core проверяет ЭП и возвращает PLC ответ с результатом проверки
- > При успешном результате проверки ЭП PLC может принять решение о применении полученной новой версии ПО или конфигурации



+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТекс». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы [™] или [®] в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.

Изобретения, примененные в представленных продуктах и решениях ИнфоТекс, защищены следующими патентами РФ: 2706176

IS25_00RU