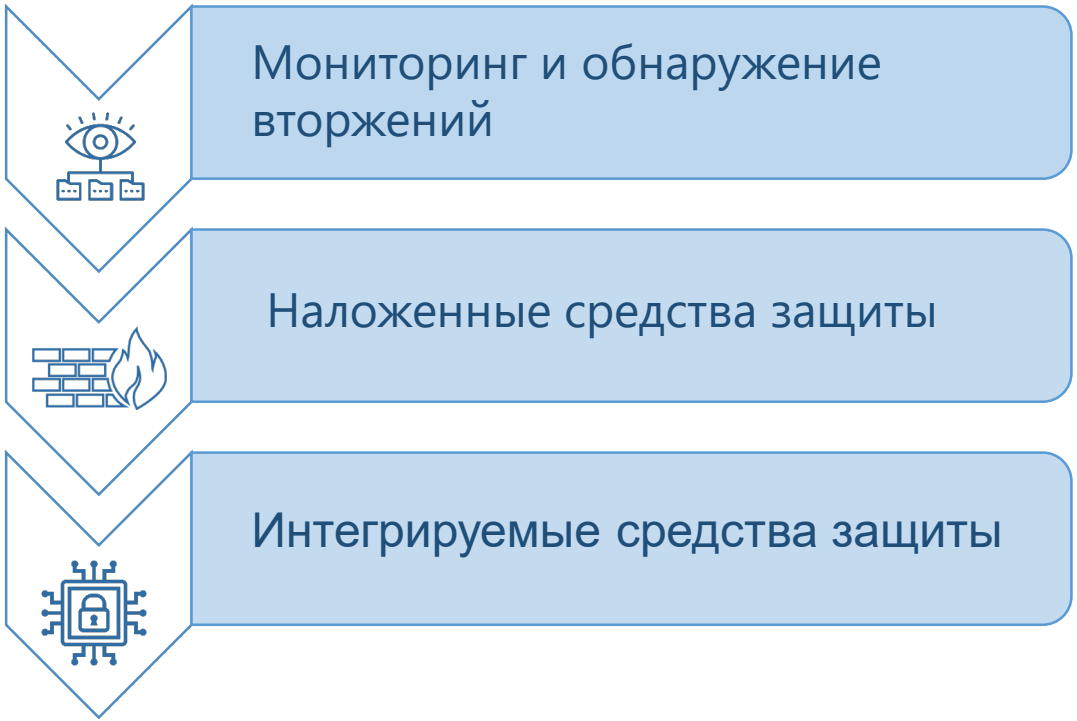
ViPNet SIES –
решение для защиты информации в промышленных системах

Информационная безопасность промышленных систем



Решение ViPNet SIES

Security for Industrial and Embedded Solutions (SIES)

SIES

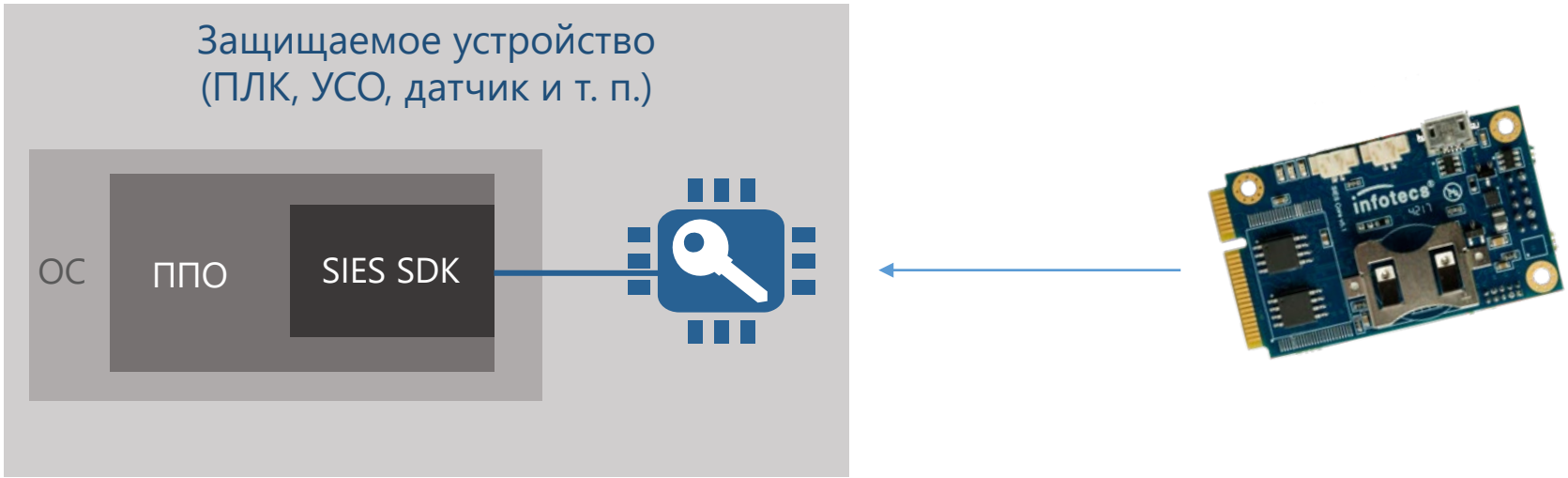
- Управление — ViPNet SIES MC, ViPNet SIES Workstation
- Защита верхнего уровня АСУ — ViPNet PKI Client SIES Unit
- Защита нижнего уровня АСУ — ViPNet SIES Core

Решение ViPNet SIES

Индустриальные криптомодули ViPNet SIES Core

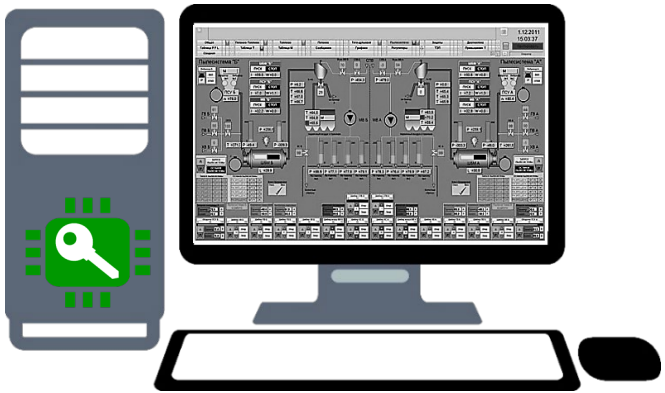
- Функционально законченное СКЗИ, соответствующее классам КС1, КС3
- Интеграция в защищаемое устройство при помощи интерфейсов UART, USB
- Доступ к криптографическим функциям по SIES API и SIES Core SDK
- Поддержка промышленных протоколов
- Пассивное устройство, выполняет функции защиты по вызову ППО
- Шифрование, имитозащита, усиленная неквалифицированная ЭП (ГОСТ)
- Индустриальное исполнение (-40^0... +75^{0}C)

Встраивание ViPNet SIES Core



ViPNet SIES Core

ViPNet PKI Client SIES Unit для защиты верхнего уровня АСУ



- ПО устанавливается на защищаемый узел верхнего уровня АСУ
- СКЗИ, соответствующее классам КС1, КС3
- Пассивный режим работы, выполняет функции защиты по вызову ППО
- Доступ к криптографическим функциям через Web API
- Поддержка промышленных протоколов
- Шифрование, имитозащита, усиленная неквалифицированная ЭП (ГОСТ)
- Централизованное управление из ViPNet SIES MC

Компоненты решения ViPNet SIES

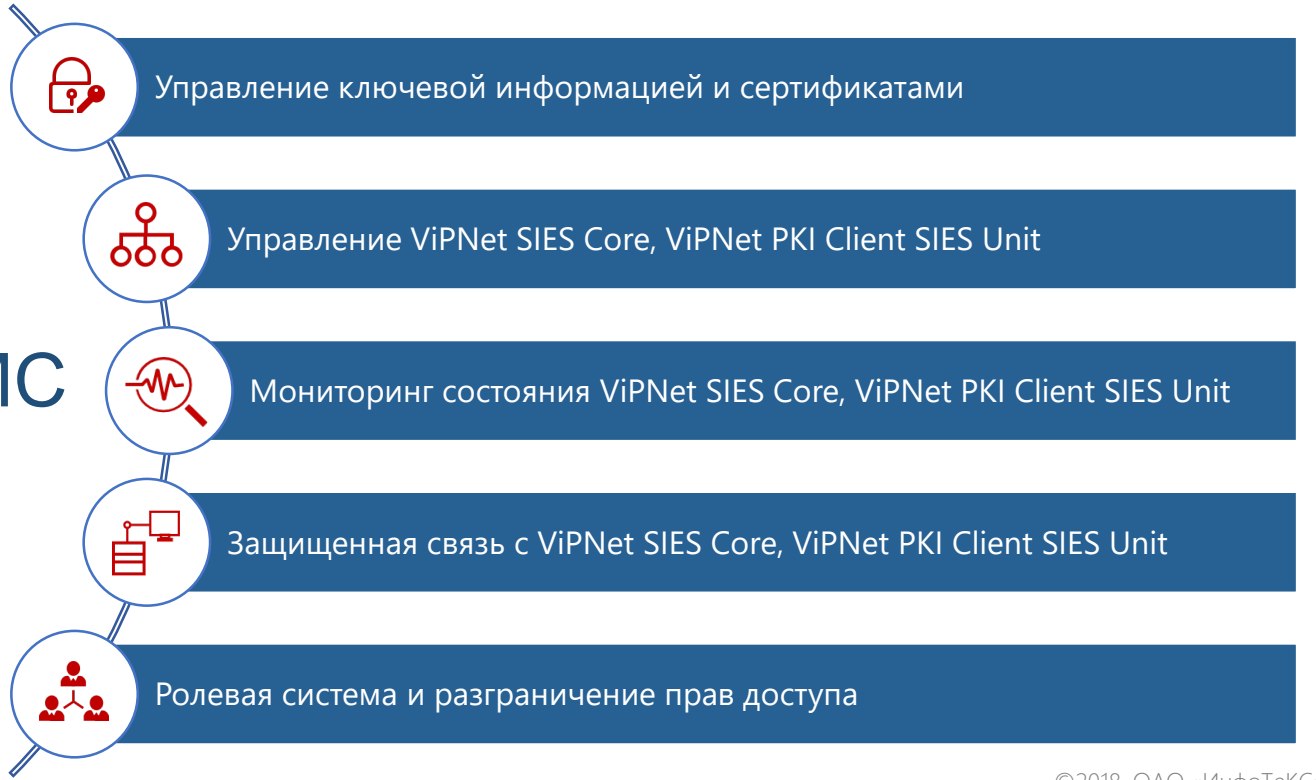
	ViPNet SIES Core	ViPNet PKI Client SIES Unit
Уровень АСУ ТП	Автоматизированного управления, Полевой (нижний)	Оперативно-диспетчерского управления (верхний)
Интерфейс интеграции в устройство	UART, USB	Инсталляция на ЗУ под управлением ОС Windows
API	SIES Core API [+ SDK]	Web API
Исполнение	SOM-модуль, 4 -15 В DC, -40^0…$+75^0$C	Программное обеспечение
Криптография	ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015	

ViPNet SIES Management Center
центр управления

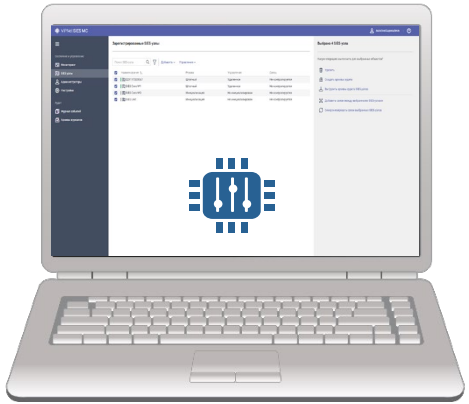
- Программно-аппаратный комплекс для управления решением ViPNet SIES
- СКЗИ, соответствующее классам КС1, КС3
- Технологический УЦ для защищаемой АСУ
- Передача управляющей информации по каналам АСУ
- Удаленный доступ для администрирования
- Многопользовательский режим
- Исполнение VA для тестирования (демо версия)

Центр управления ViPNet SIES MC

ViPNet SIES MC



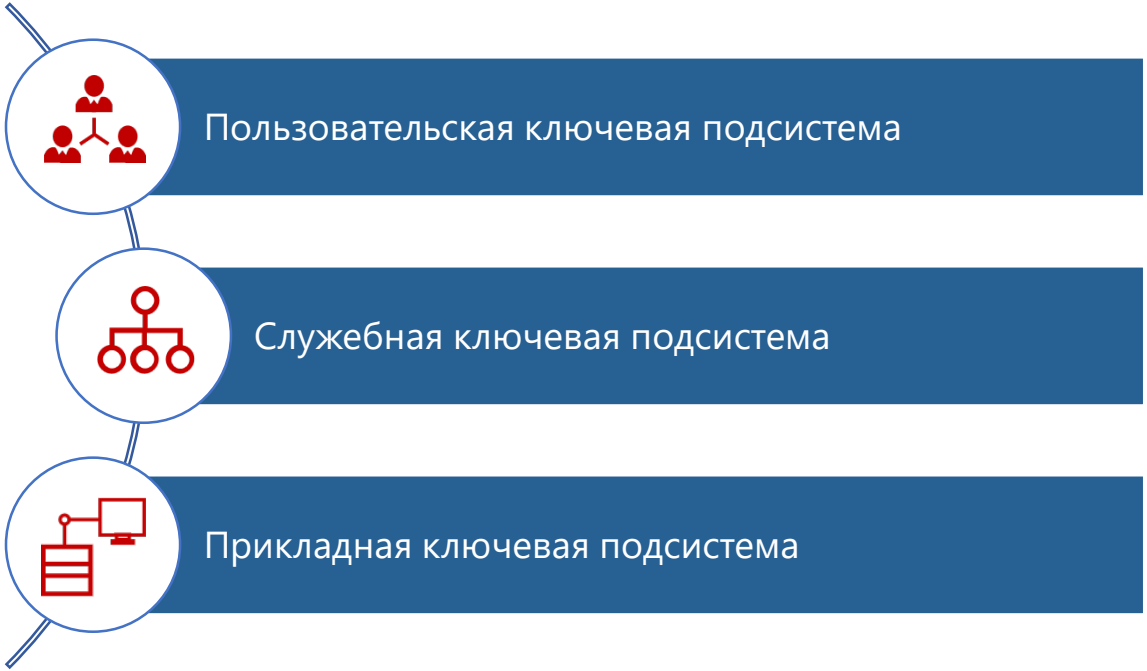
ViPNet SIES WorkStation
АРМ локального обслуживания



- Инициализация SIES-узлов
- Настройка параметров ViPNet SIES Core
- Локальное обслуживание SIES-узлов
- Передача защищенных данных от ViPNet SIES MC

Ключевая система ViPNet SIES

ViPNet SIES

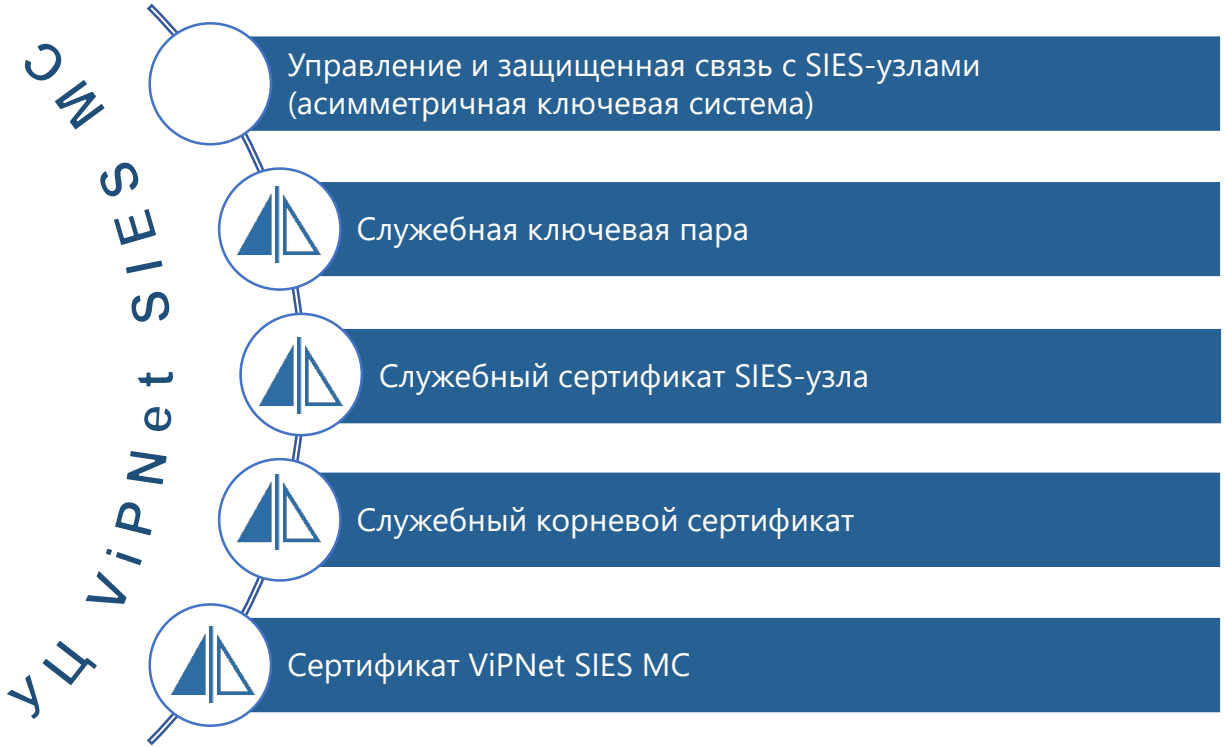


Ключевая система ViPNet SIES

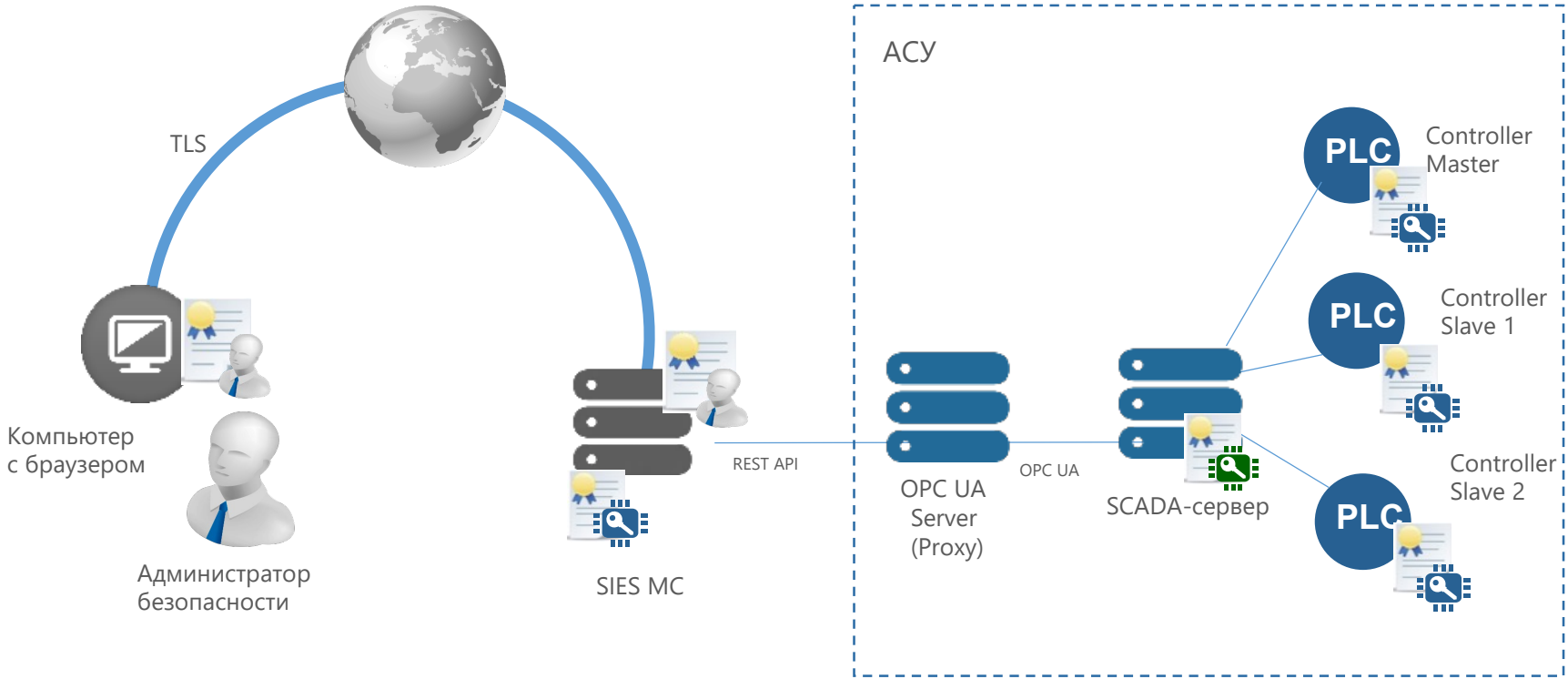
Пользовательская ключевая подсистема

Ключевая система ViPNet SIES

Служебная ключевая подсистема



Служебная ключевая подсистема



Ключевая система ViPNet SIES

Прикладная ключевая подсистема

Прикладная ключевая подсистема

АСИММЕТРИЧНАЯ

- Защищенный контейнер CMS Enveloped Data (PKCS#7)
- Формат с прикрепленными или открепленными данными
- Шифрование данных
- Усиленная неквалифицированная (технологическая) электронная подпись

СИММЕТРИЧНАЯ

- Предраспределённые симметричные ключи
- Парные (один к одному) связи между SIES-узлами
- Шифрование
- Имитозащита
- Промышленный криптографический протокол CRISP

Прикладная ключевая подсистема

CRISP (Cryptographic Industrial Security Protocol) - протокол защищенной передачи данных для индустриальных систем, M2M и IoT/IIoT коммуникаций

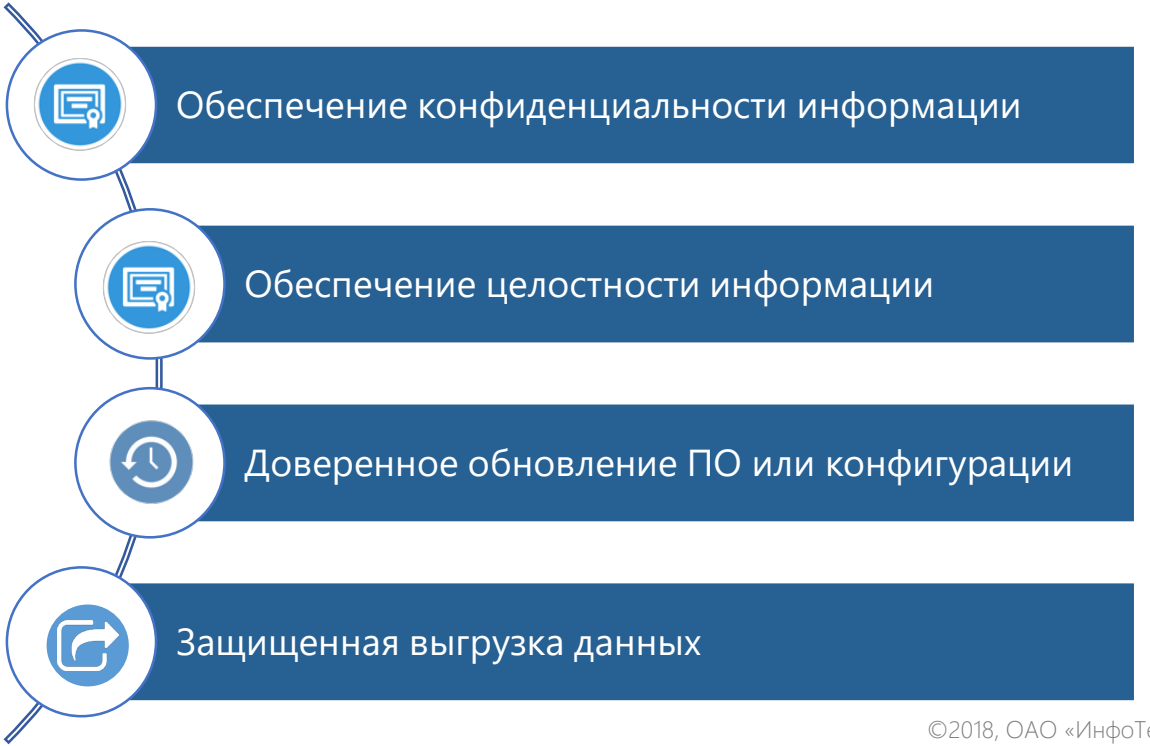
- Предраспределённые симметричные ключи
- Аутентификация источника сообщений (у абонентов общий секретный ключ)
- Поддержка адресных (один к одному) сообщений
- Обязательное обеспечение целостности при помощи имитовставки
- Обеспечение конфиденциальности при помощи блочного шифра
- Защита от навязывания повторных сообщений
- Малый размер вспомогательных данных – 10 байт + имитовставка

ViPNet SIES

Сценарии использования

Сценарии использования

ViPNet SIES



Обеспечение конфиденциальности передаваемой информации

Проблема

Между ПЛК и SCADA-сервером передается конфиденциальная информация, например, составляющая коммерческую тайну предприятия.

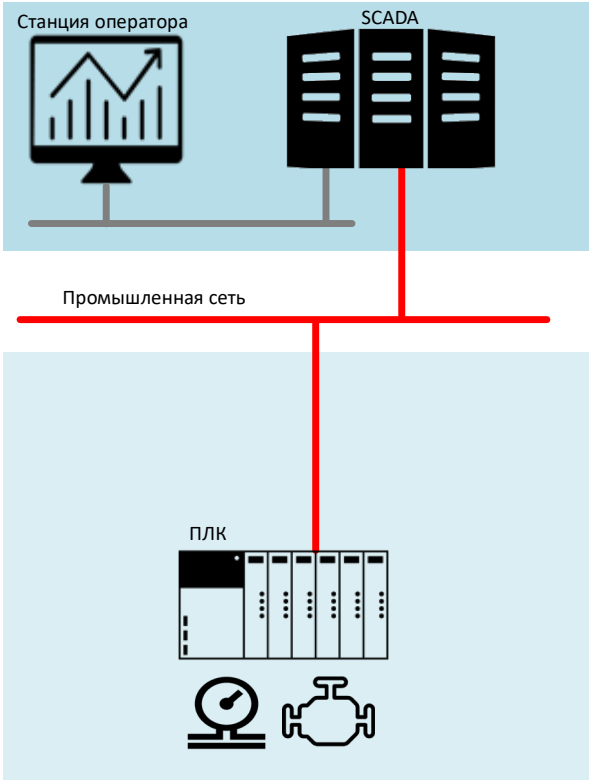
Блоки информации имеют небольшой размер от единиц до сотен байт.

При передаче по незащищенным каналам связи информация может быть перехвачена третьей стороной.

При передаче информации могут использоваться специфические промышленные протоколы, не позволяющие использовать наложенные средства защиты каналов.

Задача

Необходимо защитить информацию от доступа к ней третьих лиц.
То есть требуется обеспечить конфиденциальность информации, передаваемой по промышленной сети.



Обеспечение конфиденциальности передаваемой информации

Решение

Шифрование передаваемых данных с использованием протокола CRISP.

На SCADA-сервер устанавливается ПО ViPNet PKI Client SIES Unit

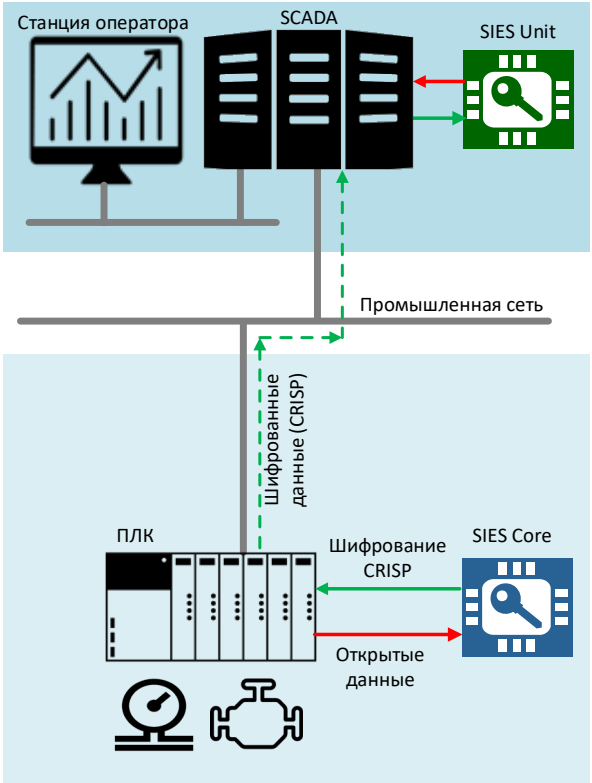
В ПЛК интегрируется криптомодуль ViPNet SIES Core.

Данные перед отправкой из ПЛК в SCADA передаются в ViPNet SIES Core, где они шифруются с использованием протокола CRISP и возвращаются в ПЛК.

Зашифрованные с использованием протокола CRISP данные передаются по существующей незащищенной промышленной сети из ПЛК в SCADA.

SCADA получает от ПЛК зашифрованные данные и передает их в ViPNet PKI Client SIES Unit для расшифрования.

ViPNet PKI Client SIES Unit возвращает SCADA расшифрованные данные.



Обеспечение целостности передаваемой информации

Проблема

От SCADA в ПЛК передается команда управления технологическим процессом или новая уставка технологического процесса.

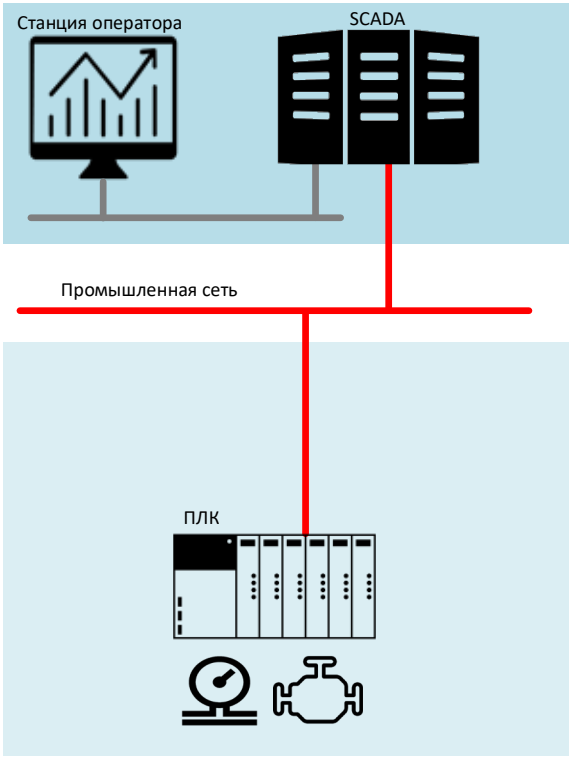
Блоки информации имеют небольшой размер от единиц до сотен байт.

Информация передается по незащищенной промышленной сети с использованием специфических промышленных протоколов, не позволяющих применить наложенные средства защиты каналов.

Перехват и несанкционированное изменение передаваемой информации может негативно отразиться на ходе технологического процесса и привести к необратимым последствиям.

Задача

Необходимо защитить передаваемую информацию от несанкционированного изменения третьими лицами.
То есть требуется обеспечить целостность информации, передаваемой по промышленной сети.



Обеспечение целостности передаваемой информации

Решение

Имитозащита передаваемых данных с использованием протокола CRISP.

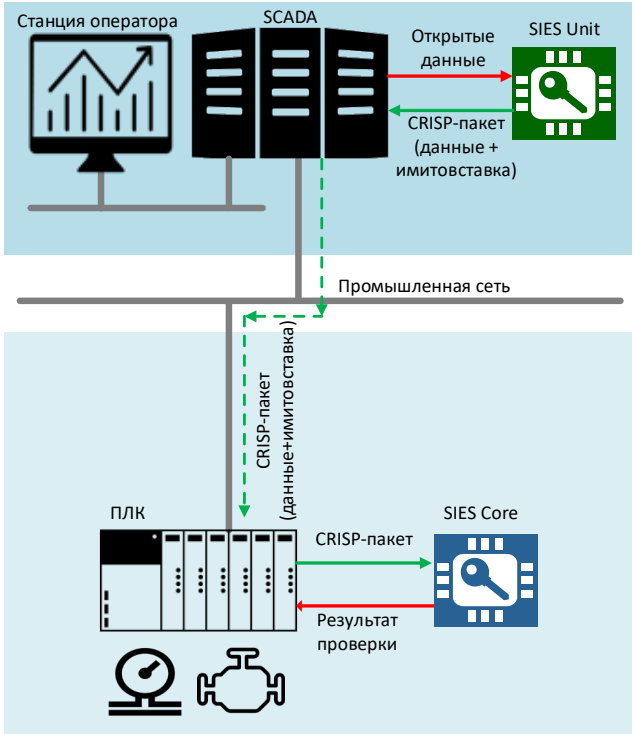
На SCADA-сервер устанавливается ПО ViPNet PKI Client SIES Unit

В ПЛК интегрируется криптомодуль ViPNet SIES Core.

Данные перед отправкой из SCADA в ПЛК передаются в ViPNet PKI Client SIES Unit, где для них вычисляется имитовставка. ViPNet PKI Client SIES Unit формирует CRISP-пакет, включающий данные и имитовставку и возвращает его в SCADA.

CRISP-пакет, включающий данные и имитовставку, передаётся по существующей незащищенной промышленной сети изSCADA в ПЛК. ПЛК получает от SCADA CRISP-пакет и передает его в ViPNet SIES Core для проверки имитовставки.

Результат проверки возвращается в ПЛК. В случае положительного результата информация считается переданной без искажений и может быть использована в технологическом процессе.



Доверенное обновление ПО или конфигурации

Проблема

С инженерной станции в ПЛК передается файл с новой версией ПО или конфигурации контроллера.

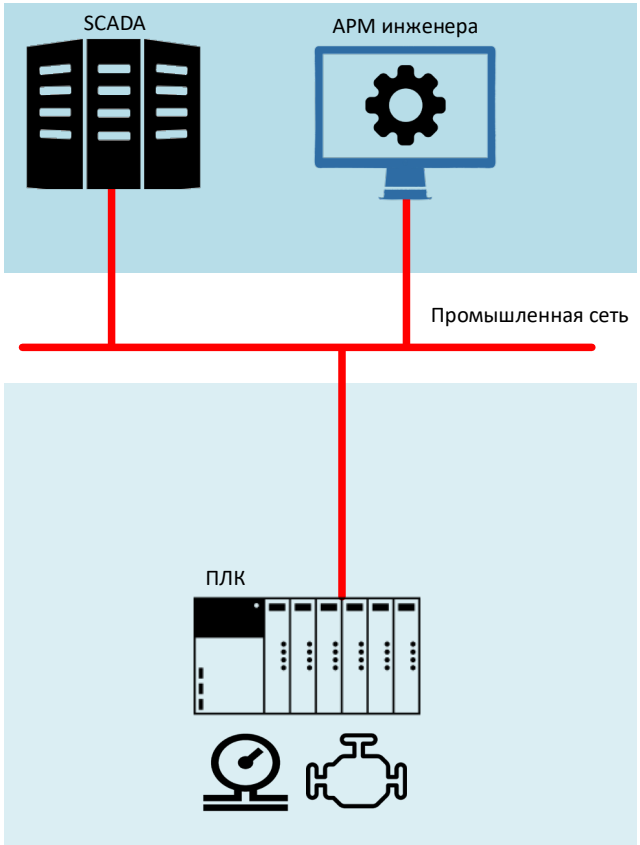
Файл может иметь значительный размер - до мегабайт.

Информация передается по незащищенной промышленной сети с использованием специфических промышленных протоколов, не позволяющих применить наложенные средства защиты каналов.

Передаваемый файл может быть перехвачен, изменен или подменен злоумышленником при передаче.

Задача

Необходимо защитить передаваемый файл от несанкционированного изменения или подмены при его передаче с инженерной станции в ПЛК. ПЛК должен иметь возможность убедиться в неизменности полученного файла, а также в том, что он получен от доверенного источника.



Доверенное обновление ПО или конфигурации

Решение

Использование электронной подписи для защиты передаваемого файла от несанкционированного изменения или подмены.

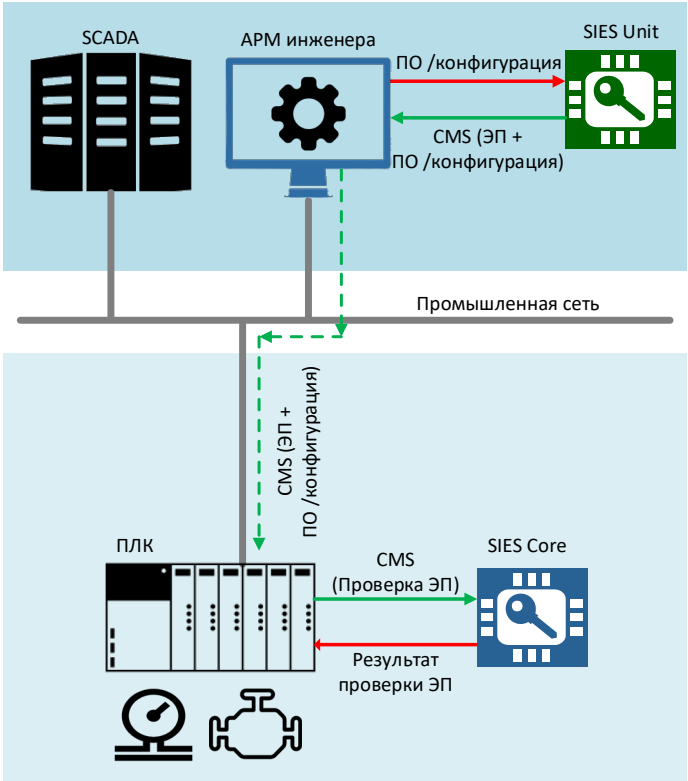
С этой целью прикладное ПО АРМ инженера перед отправкой файла в ПЛК передает его в ViPNet PKI Client SIES Unit для вычисления ЭП. ViPNet PKI Client SIES Unit формирует защищенный ЭП конверт CMS Signed Data и возвращает его в прикладное ПО для передачи в ПЛК.

Защищенный CMS конверт передается в ПЛК по промышленной сети.

ПЛК передает полученный CMS конверт в интегрированный в него криптомодуль ViPNet SIES Core для проверки ЭП.

ViPNet SIES Core проверяет ЭП и возвращает ПЛК ответ с результатом проверки.

При успешном результате проверки ЭП ПЛК может принять решение о применении полученной новой версии ПО или конфигурации.



Защищенная выгрузка данных

Проблема

ПЛК в процессе работы накапливает во внутренней памяти конфиденциальные данные, например, журналы работы.

Файл с данными может иметь значительный размер - до мегабайт.

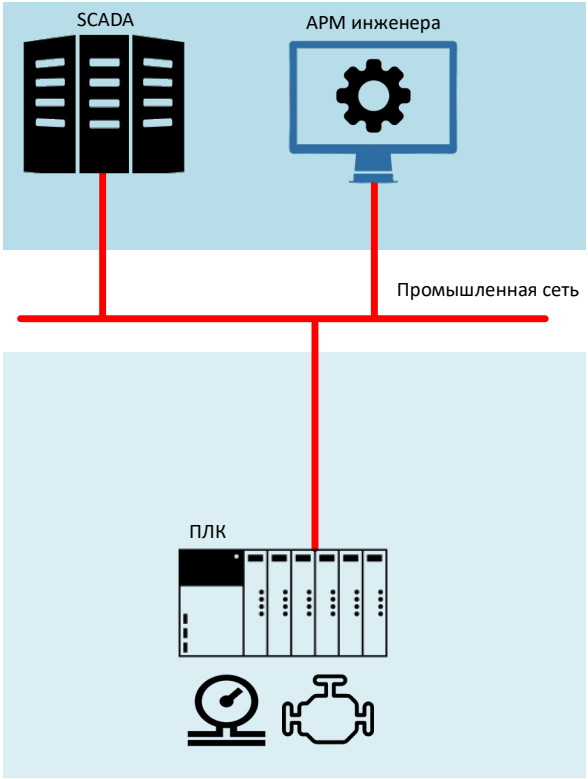
Для обработки этих данных их необходимо передать из ПЛК на АРМ инженера.

Передача данных может осуществляться по незащищенному каналу связи, например, по промышленной сети.

Без применения дополнительных мер при выгрузке данные журналов оказываются в открытом доступе и могут использоваться злоумышленниками для получения конфиденциальной информации или бесконтрольно изменяться для подделки данных.

Задача

Необходимо защитить передаваемые данные от доступа третьих лиц, несанкционированного изменения или подмены при их передаче по открытым каналам. Необходимо обеспечить конфиденциальность, целостность и аутентичность передаваемых данных.



Защищенная выгрузка данных

Решение

Для обеспечения целостности, аутентичности и конфиденциальности передаваемой информации использовать шифрование и ЭП данных.

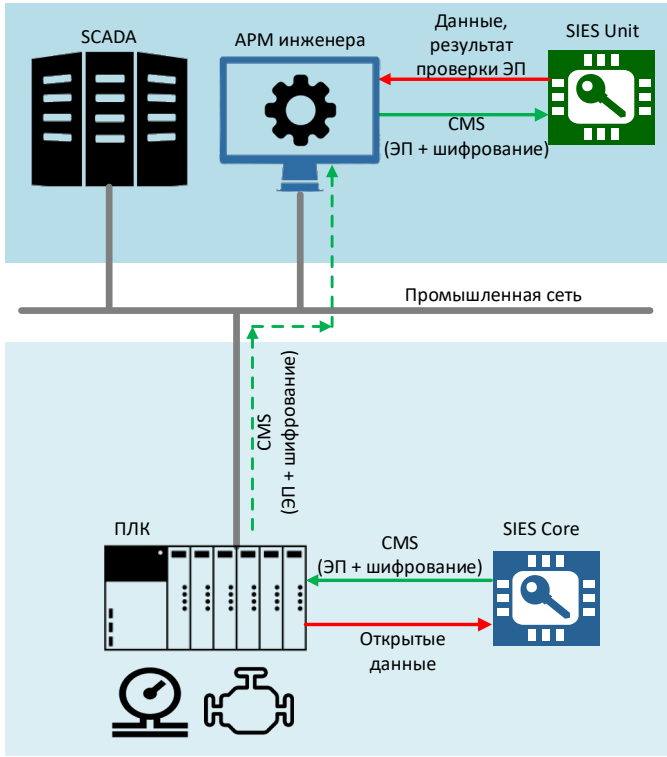
С этой целью ПЛК перед отправкой данных на АРМ инженера передает их в ViPNet SIES Core для зашифрования и вычисления ЭП. ViPNet SIES Core формирует защищенный CMS конверт с зашифрованными и подписанными ЭП данными и возвращает его в ПЛК для передачи на АРМ инженера.

Защищенный CMS конверт передается на АРМ инженера по промышленной сети или другому незащищенному каналу.

АРМ инженера передает полученный CMS конверт в установленный на нем ViPNet PKI Client SIES Unit для расшифрования и проверки ЭП.

ViPNet PKI Client SIES Unit проверяет ЭП, расшифровывает данные и возвращает ПЛК ответ с результатом проверки ЭП и сами данные.

При успешном результате проверки ЭП расшифрованные данные могут быть приняты в обработку.




infotecs
Спасибо за внимание!