

техно infotecs
2019 ФЕСТ

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

12
09 2019

Необходимые и
достаточные сценарии ИБ
для контроллеров и
полевых устройств АСУ

О чем будет доклад?

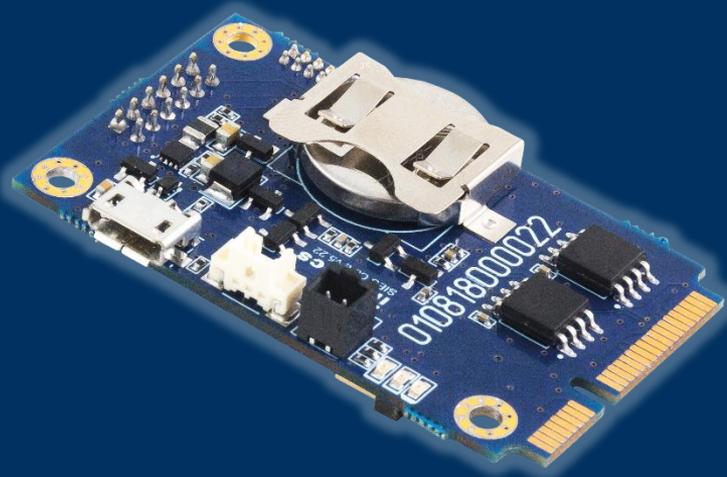
- Криптографический модуль ViPNet SIES Core
- Криптографический протокол CRISP (Cryptographic Industrial Security Protocol)
- Сценарии информационной безопасности для устройств АСУ
- Соотнесение с мерами приказа №239 ФСТЭК России





Криптографический модуль
ViPNet SIES Core

Криптографический модуль ViPNet SIES Core



- Функционально законченное СКЗИ, соответствующее классам КС1, КС3
- Интеграция в защищаемое устройство при помощи интерфейсов UART, USB
- Доступ к криптографическим функциям через SIES Core API и SIES Core SDK
- Поддержка промышленных протоколов
- Пассивное устройство, выполняет функции защиты информации по вызову прикладного ПО
- Обеспечивает информационную безопасность на уровне данных
- Криптографические операции по алгоритмам ГОСТ

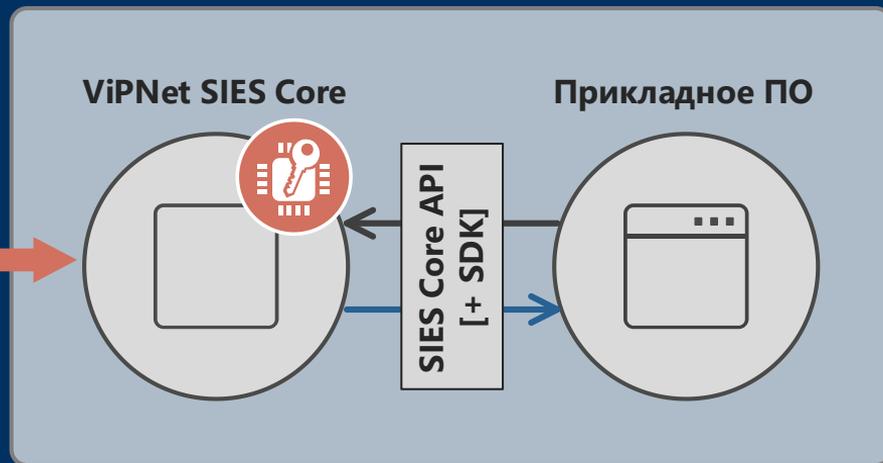


Интеграция ViPNet SIES Core



ViPNet SIES Core

UART / USB



Защищаемое устройство
(ПЛК, УСО, датчик и т.п.)

Функции защиты информации ViPNet SIES Core



Защита информации по протоколу CRISP

- зашифрование и расшифрование блока данных
- вычисление и проверка имитовставки для блока данных
- защита от навязывания повторных сообщений

Защита информации с помощью прикладной PKI

- зашифрование и расшифрование данных в CMS-контейнере
- создание и проверка усиленной неквалифицированной электронной подписи в CMS-контейнере

Другие функции защиты информации

- вычисление и проверка значения хэш-кода для блока данных



Криптографический протокол CRISP

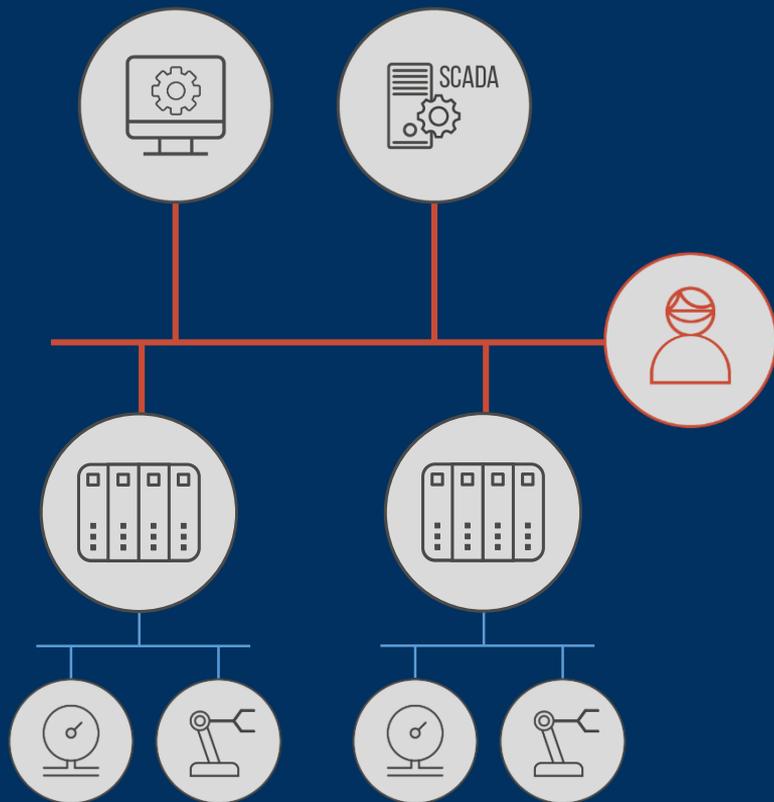


CRISP (Cryptographic Industrial Security Protocol) – неинтерактивный протокол защищенной передачи данных для промышленных систем

- Предраспределённые симметричные ключи
- Аутентификация источника сообщений (у абонентов общий секретный ключ)
- Поддержка адресных и широковещательных сообщений
- Обязательное обеспечение целостности при помощи имитовставки
- Обеспечение конфиденциальности при помощи блочного шифра
- Защита от навязывания повторных сообщений
- Малый размер вспомогательных данных

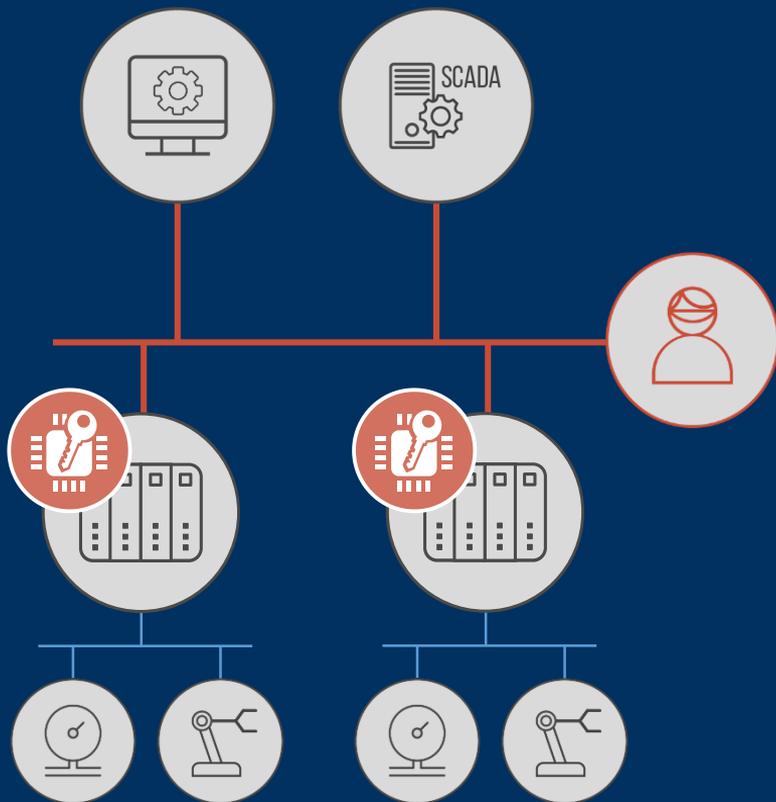


ViPNet SIES Core
сценарии информационной
безопасности для устройств АСУ



Обеспечение конфиденциальности и целостности информации

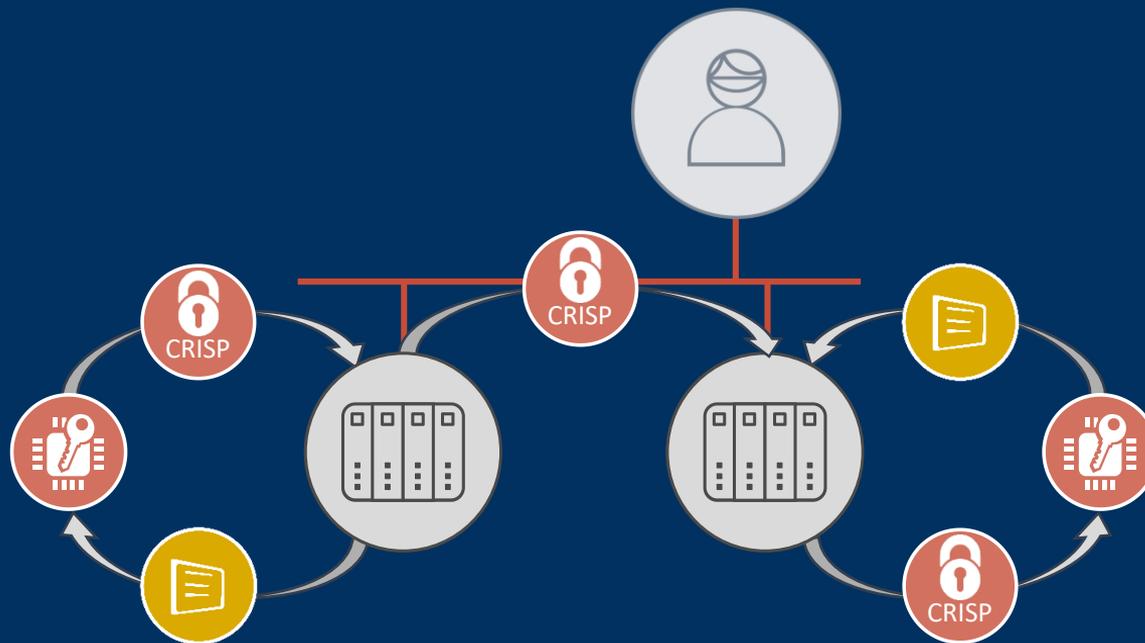
Необходимо защитить информацию,
передаваемую между контроллерами
от доступа к ней третьих лиц



Обеспечение конфиденциальности и целостности информации

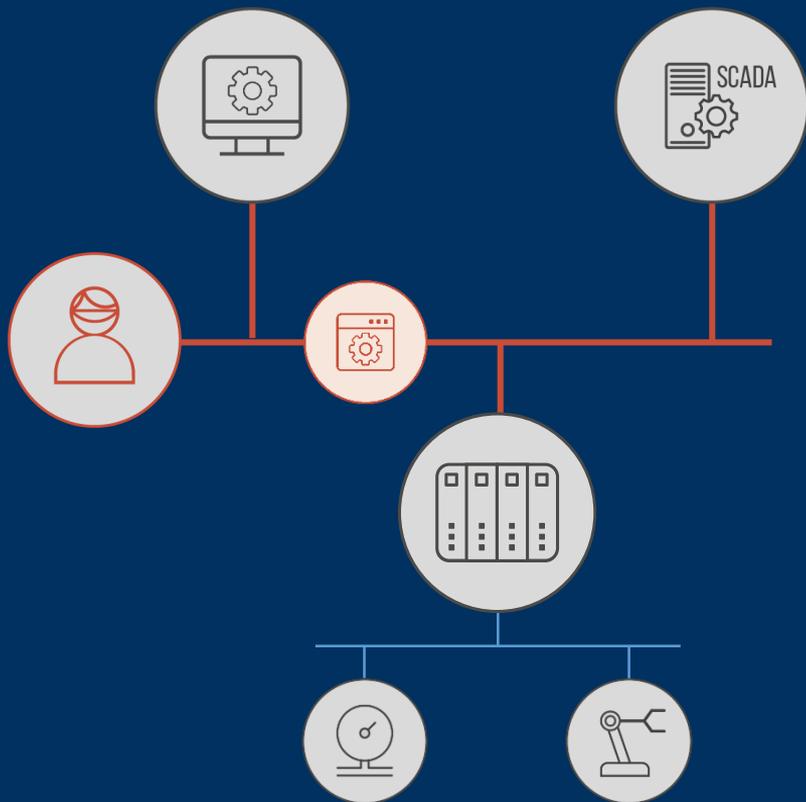
В контроллеры АСУ ТП интегрируем криптографические модули ViPNet SIES Core для защиты данных, передаваемых по технологической сети, с помощью протокола CRISP

Обеспечение конфиденциальности и целостности информации



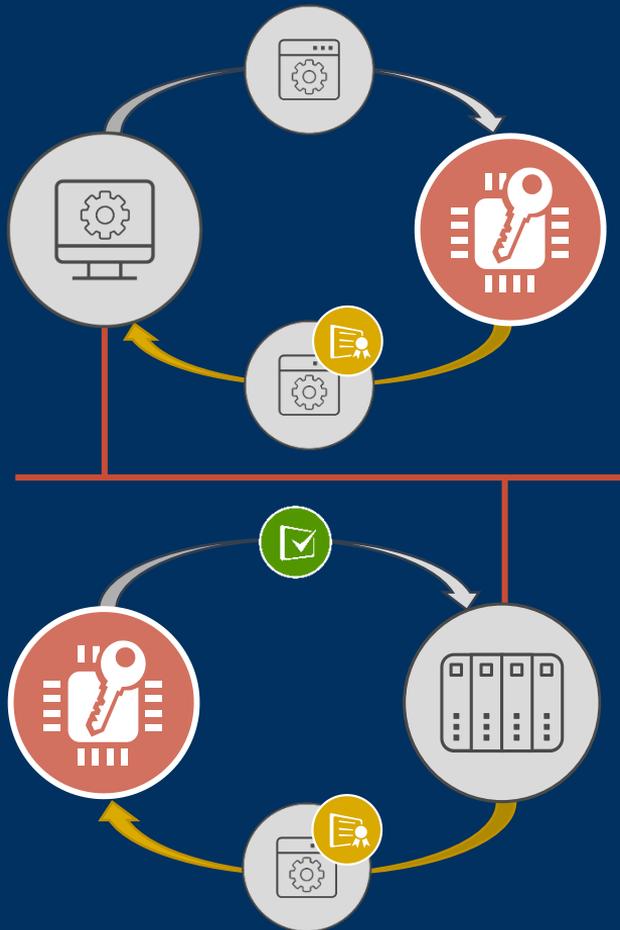
Обеспечение конфиденциальности и целостности информации

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+
ОЦЛ.2	Контроль целостности информации			
ЗИС.13	Защита неизменяемых данных		+	+
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+
ЗИС.32	Защита беспроводных соединений	+	+	+



Доверенное обновление программного обеспечения или конфигурации

Необходимо защитить файл обновления ПО или конфигурации устройства АСУ ТП от несанкционированного изменения или подмены его злоумышленником, исключить возможность загрузки в устройство АСУ ТП недоверенного ПО или конфигурации.

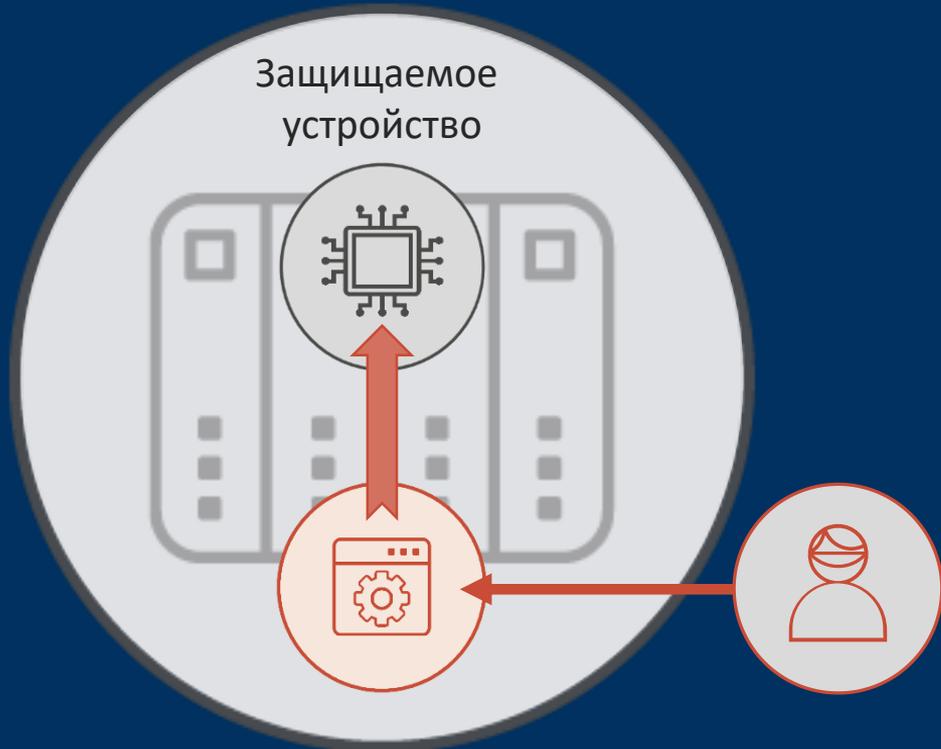


Доверенное обновление программного обеспечения или конфигурации

В устройства АСУ ТП интегрируются продукты ViPNet SIES. Файл с обновлением ПО или конфигурацией заверяется ЭП на станции инженера. Подписанный файл передается в устройство АСУ ТП. Перед применением обновления устройство передает файл в ViPNet SIES Core для проверки ЭП.

Доверенное обновление программного обеспечения или конфигурации

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+



Доверенная загрузка устройства

Злоумышленник может подменить или внести изменения в ПО или ОС устройства АСУ ТП. Загрузка такого ПО или ОС позволит злоумышленнику получить контроль над устройством АСУ ТП.

Необходимо контролировать запуск ОС и ПО защищаемого устройства АСУ ТП



Доверенная загрузка устройства

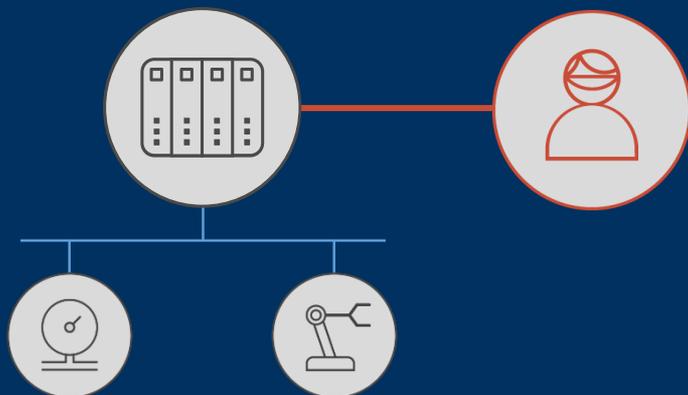
ОС и ПО заверяются ЭП.
В защищаемое устройство АСУ ТП интегрируется ViPNet SIES Core.

Перед запуском ОС или ПО защищаемое устройство обращается к ViPNet SIES Core для проверки ЭП. Запуск ОС или ПО разрешается в случае успешной проверки ЭП.

Доверенная загрузка устройства

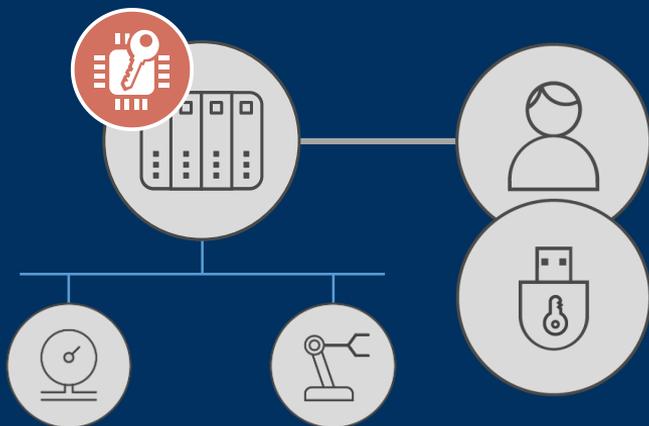
Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
УПД.3	Доверенная загрузка		+	+
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+

Защищенный доступ к устройству с локальной аутентификацией пользователя



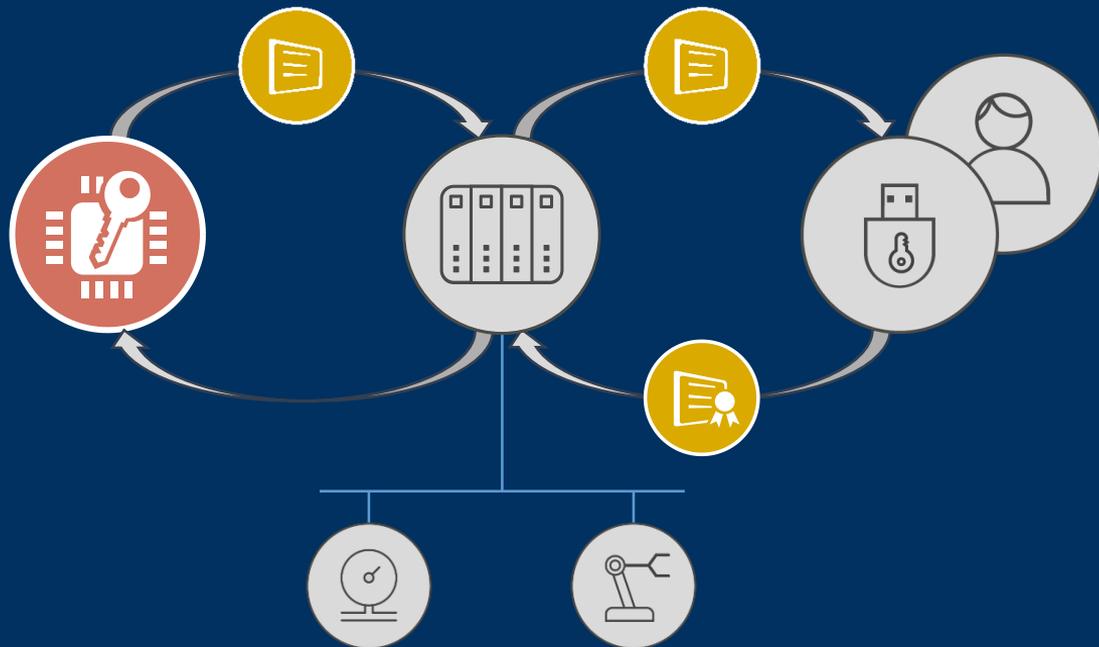
При выполнении локальных операций по настройке или обслуживанию устройства АСУ ТП необходимо выполнить аутентификацию пользователя для предотвращения возможности доступа к устройству злоумышленника и выполнения несанкционированных действий.

Защищенный доступ к устройству с локальной аутентификацией пользователя



Аутентификация пользователя выполняется при помощи ViPNet SIES Core, интегрированного в защищаемое устройство АСУ ТП, и персонального ключевого носителя пользователя, хранящего ключ ЭП.

Защищенный доступ к устройству с локальной аутентификацией пользователя

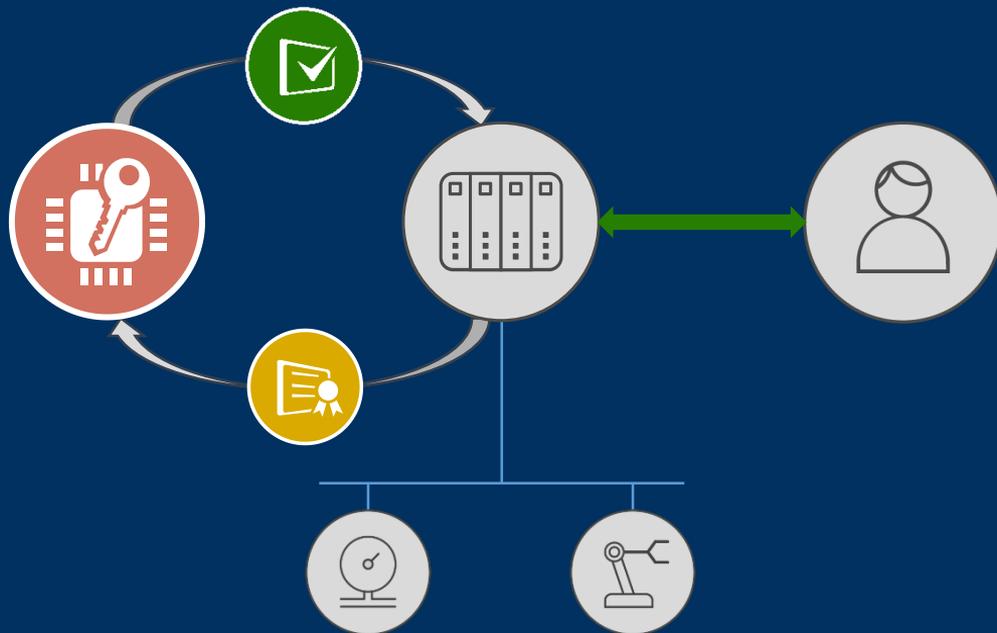


По запросу защищаемого устройства ViPNet SIES Core формирует блок случайных данных и возвращает их защищаемому устройству.

Устройство вызывает функцию формирования ЭП ключевого носителя пользователя для полученного блока данных.

Ключевой носитель вычисляет ЭП с помощью ключа подписи пользователя и возвращает её защищаемому устройству.

Защищенный доступ к устройству с локальной аутентификацией пользователя

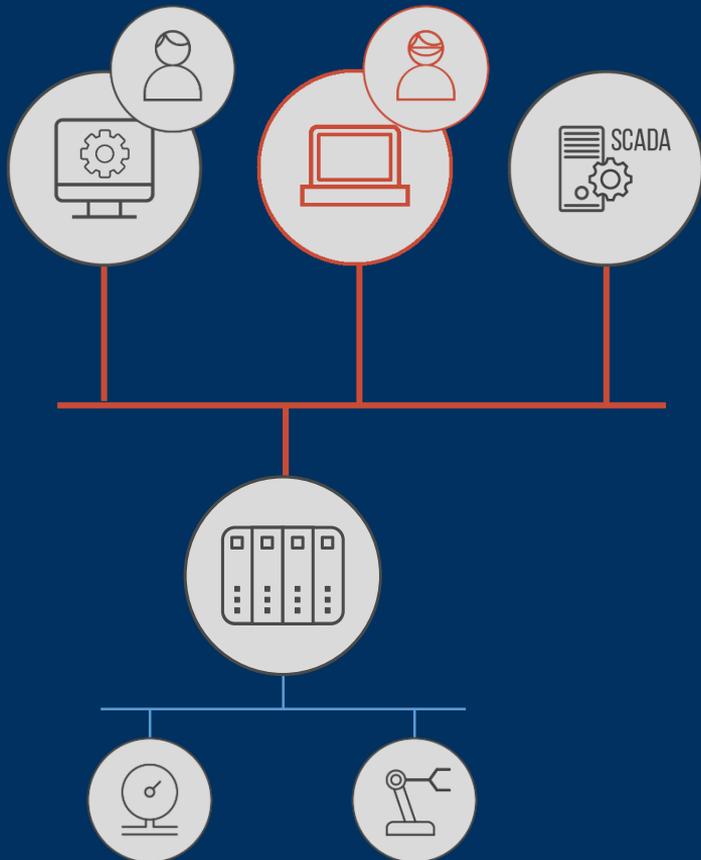


Защищаемое устройство обращается к ViPNet SIES Core для проверки корректности ЭП пользователя.

В случае успешной проверки ЭП пользователю предоставляется доступ к защищаемому устройству.

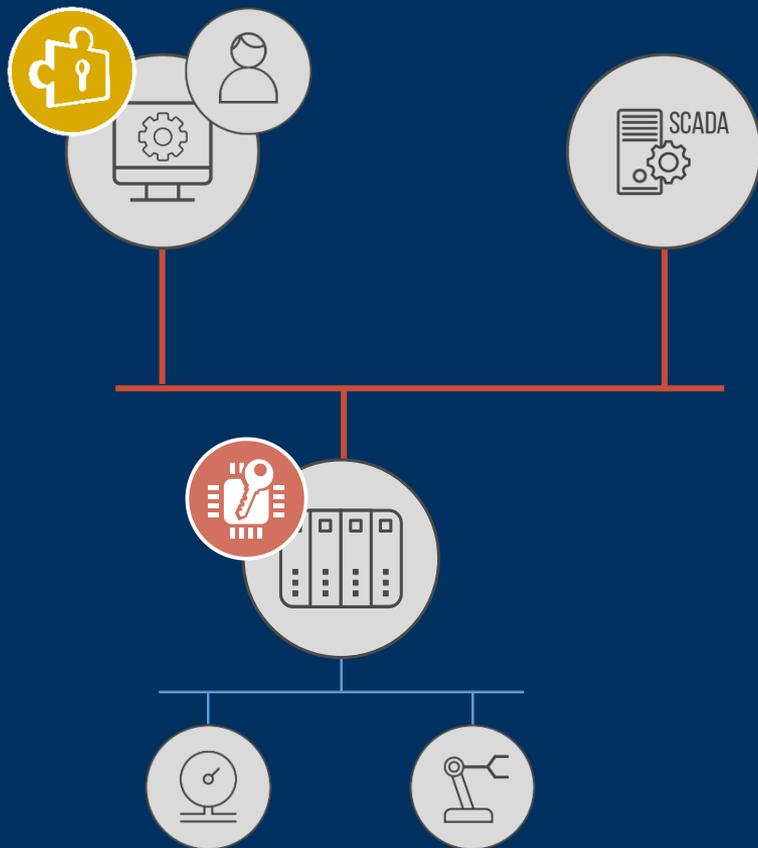
Защищенный доступ к устройству с локальной аутентификацией пользователя

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			



Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ

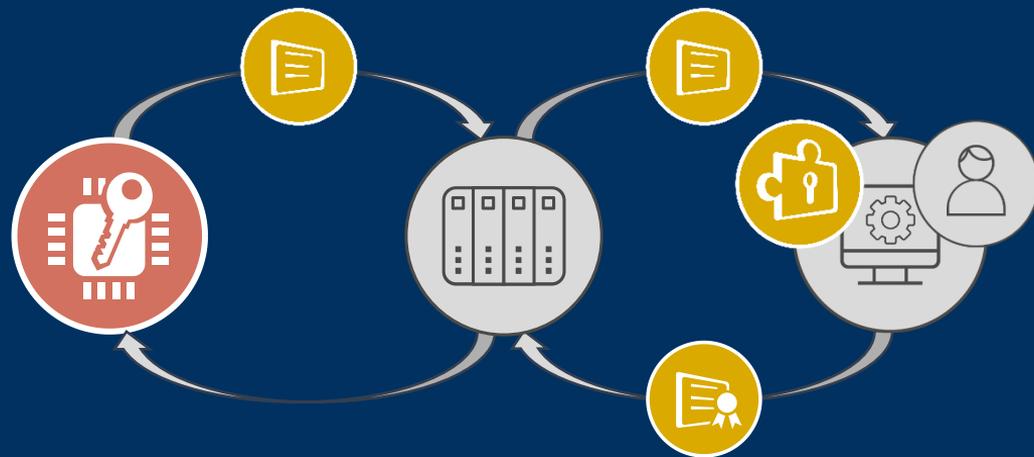
Необходимо выполнить аутентификацию пользователя удаленного АРМ на устройстве АСУ ТП, например, ПЛК для предотвращения возможности доступа к нему злоумышленника.



Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ

Аутентификация пользователя выполняется при помощи ViPNet SIES Core, интегрированного в защищаемое устройство АСУ ТП, криптопровайдера, например, ViPNet CSP и ключа подписи, хранящегося у пользователя.

Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ



По запросу защищаемого устройства ViPNet SIES Core формирует блок случайных данных и возвращает их защищаемому устройству, которое передает их на АРМ пользователя.

Пользователь с помощью криптопровайдера и своего ключа подписи формирует ЭП и возвращает подписанный блок данных защищаемому устройству.

Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ



Защищаемое устройство обращается к VIPNet SIES Core для проверки корректности ЭП пользователя.

В случае успешной проверки ЭП пользователю удаленного АРМ предоставляется доступ к защищаемому устройству.

Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ

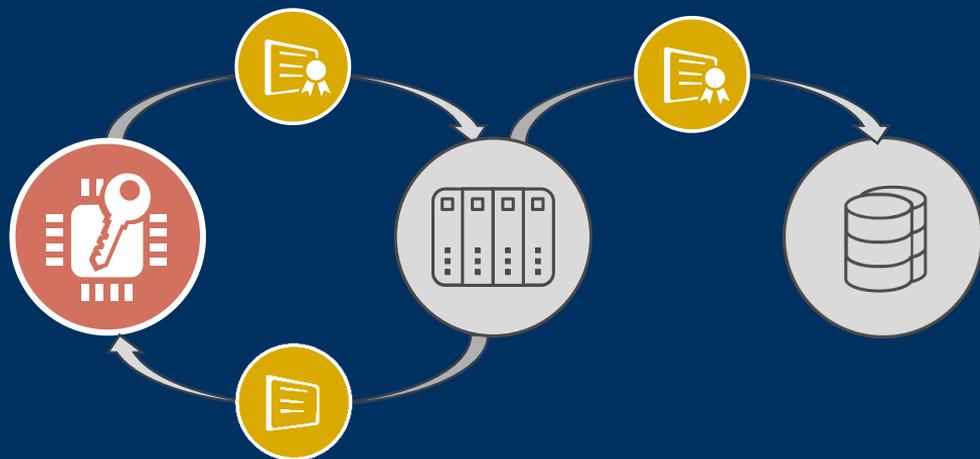
Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			



Контроль целостности хранимых данных

Необходимо обеспечить и контролировать целостность данных, сохраняемых устройством АСУ ТП в процессе работы, для предотвращения их случайного или преднамеренного изменения.

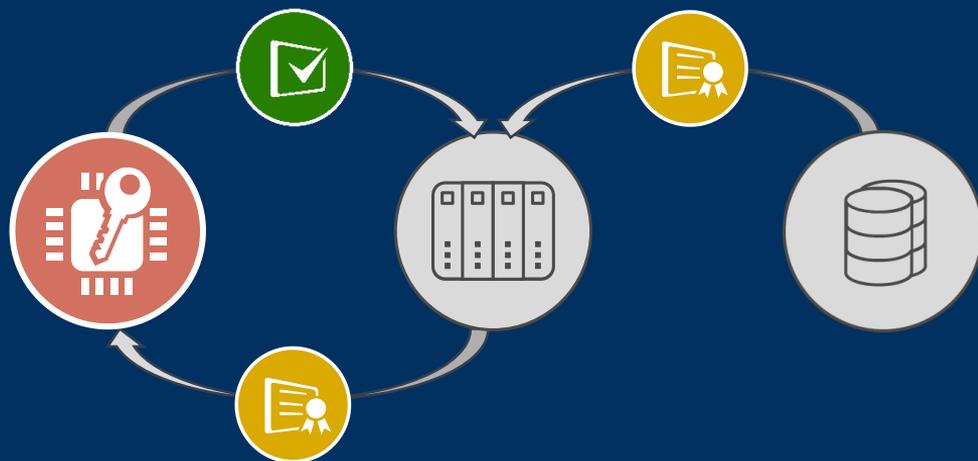
Контроль целостности хранимых данных



Перед сохранением данных, целостность которых необходимо контролировать, защищаемое устройство обращается к интегрированному в него ViPNet SIES Core и вызывает функцию вычисления хэш-кода для сохраняемых данных.

Вычисленные значения хэш-кода вместе с данными сохраняется на защищаемом устройстве.

Контроль целостности хранимых данных



Для контроля целостности защищаемое устройство передаёт данные вместе с хэш-кодом в ViPNet SIES Core.

ViPNet SIES Core выполняет функцию проверки хэш-кода и возвращает защищаемому устройству ответ.

Если хэш-код соответствует данным, их целостность считается ненарушенной.

Контроль целостности хранимых данных

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
ОЦЛ.2	Контроль целостности информации	+	+	+
ЗИС.13	Защита неизменяемых данных		+	+

Встроенные меры защиты ViPNet SIES Core

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
АУД.4	Регистрация событий безопасности	+	+	+
АУД.6	Защита информации о событиях безопасности	+	+	+
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+

Меры защиты реализуемые с помощью ViPNet SIES Core

ИАФ.1	Идентификация и аутентификация пользователей и иницилируемых ими процессов	УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
ИАФ.2	Идентификация и аутентификация устройств	ЗИС.8	Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы
ИАФ.5	Идентификация и аутентификация внешних пользователей	ЗИС.13	Защита неизменяемых данных
ИАФ.7	Защита аутентификационной информации при передаче	ЗИС.19	Защита информации при ее передаче по каналам связи
УПД.3	Доверенная загрузка	ЗИС.28	Исключение возможности отрицания отправки информации
УПД.13	Реализация защищенного удаленного доступа	ЗИС.32	Защита беспроводных соединений
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	ОПО.2	Контроль целостности обновлений программного обеспечения
АУД.4	Регистрация событий безопасности	ОПО.4	Установка обновлений программного обеспечения
АУД.6	Защита информации о событиях безопасности	ОЦЛ.1	Контроль целостности программного обеспечения
УКФ.4	Контроль действий по внесению изменений	ОЦЛ.2	Контроль целостности информации





ТЕХНО infotecs
2019 Фест

Спасибо
за внимание!