Практика применения встраиваемых средств защиты информации в электроэнергетике

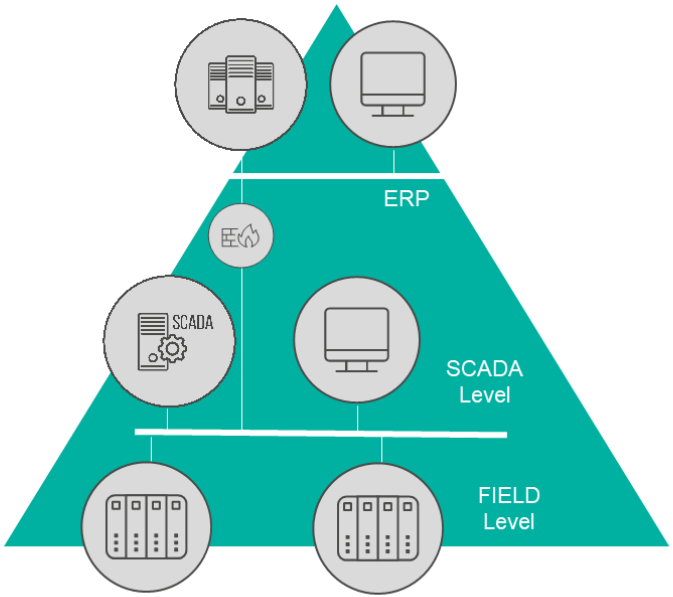
Марина Сорокина, ИнфоТеКС

Защита конечных устройств

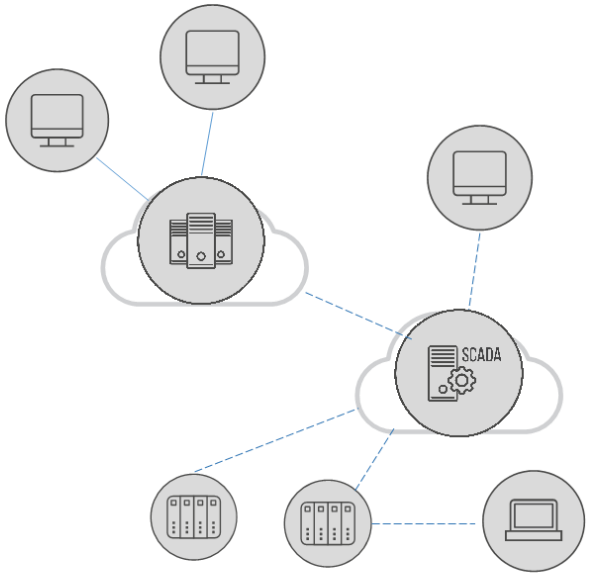
Цифровая трансформация электроэнергетики

- Цифровой РЭС
- Цифровая подстанция
- Цифровой электромонтер
- АСУ предиктивного анализа и мониторинга
- АСУ по управлению и планированию работами эксплуатационных служб
- АСУ учета массовых отключений
- Интеллектуальный учет электроэнергетики
- Модернизация и реконструкция инфраструктуры

Изменение архитектуры АСУ в процессе трансформации



Архитектура классической АСУ



Архитектура Industry 4.0

Изменение архитектуры АСУ в процессе трансформации

Размытие периметра

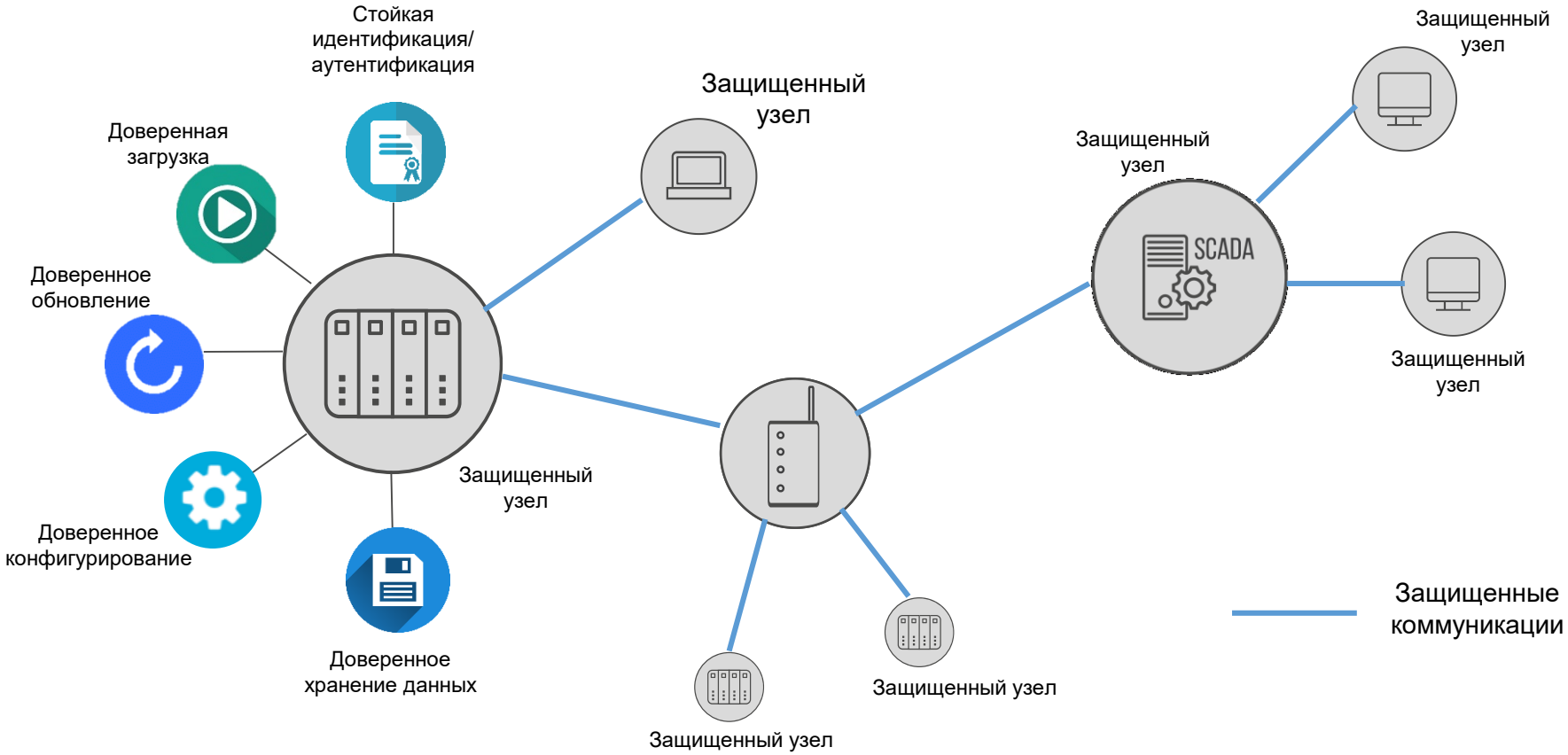
Увеличения количества конечных устройств

Применение беспроводных каналов связи

Кибербезопасность

Новые вызовы: защиты периметра не достаточно

Концепция Endpoint protection



infotecs

Защита конечных узлов

Серия стандартов IEC 62443 “Security for industrial automation and control systems”

IEC 62443-4-2 - требования к поставщикам и разработчиком компонентов АСУ

infotecs

Приложения

Встраиваемые устройства

Сетевые компоненты

Конечные устройства

Требования IEC 62443-4-2

FR 1 – Identification and Authentication Control (IAC)	SL1	SL2	SL3	SL4
CR 1.1 – Human user identification and authentication	+	+	+	+
CR 1.2 – Software process and device identification and authentication		+	+	+
CR 1.3 – Account management	+	+	+	+
CR 1.4 – Identifier management	+	+	+	+
CR 1.5 – Authenticator management	+	+	+	+
NDR 1.6 – Wireless access management	+	+	+	+
CR 1.8 – Public key infrastructure certificates		+	+	+
CR 1.9 – Strength of public key-based authentication		+	+	+
CR 1.10 – Authenticator feedback	+	+	+	+
CR 1.11 – Unsuccessful login attempts	+	+	+	+
CR 1.12 – System use notification	+	+	+	+
NDR 1.13 – Access via untrusted networks	+	+	+	+
CR 1.14 – Strength of symmetric key-based authentication		+	+	+

FR 2 – Use Control (UC)	SL1	SL2	SL3	SL4
CR 2.1 – Authorization enforcement	+	+	+	+
CR 2.2 – Wireless use control	+	+	+	+
CR 2.3 – Use control for portable and mobile devices				
NDR 2.4/ SAR 2.4/ EDR 2.4/HDR 2.4 – Mobile code	+	+	+	+
CR 2.5 – Session lock	+	+	+	+
CR 2.6 – Remote session termination		+	+	+
CR 2.7 – Concurrent session control			+	+
CR 2.8 – Auditable events	+	+	+	+
CR 2.9 – Audit storage capacity	+	+	+	+
CR 2.10 – Response to audit processing failures	+	+	+	+
CR 2.11 – Timestamps	+	+	+	+
CR 2.12 – Non-repudiation	+	+	+	+

Требования IEC 62443-4-2

FR 3 – System Integrity (SI)	SL1	SL2	SL3	SL4
CR 3.1 – Communication integrity	+	+	+	+
SAR 3.2– Protection from malicious code	+	+	+	+
CR 3.3 – Security functionality verification	+	+	+	+
CR 3.4 – Software and information integrity	+	+	+	+
CR 3.5 – Input validation	+	+	+	+
CR 3.6 – Deterministic output		+	+	+
CR 3.7 – Error handling			+	+
CR 3.8 – Session integrity		+	+	+
CR 3.9 – Protection of audit information		+	+	+
EDR 3.10 – Support for updates	+	+	+	+
EDR 3.11 – Physical tamper resistance and detection		+	+	+
EDR 3.12– Provisioning product supplier roots of trust		+	+	+
EDR 3.13 – Provisioning asset owner roots of trust		+	+	+
EDR 3.14 – Integrity of the boot process	+	+	+	+

FR 4 – Data Confidentiality (DC)	SL1	SL2	SL3	SL4
CR 4.1 – Information confidentiality	+	+	+	+
CR 4.2 – Information persistence	+	+	+	+
CR 4.3 – Use of cryptography	+	+	+	+
FR 5 – Restricted Data Flow (RDF)				
CR 5.1 – Network segmentation			+	+
NDR 5.2 – Zone boundary protection		+	+	+
FR 6 – Timely Response to Events (TRE)				
CR 6.1 – Audit log accessibility	+	+	+	+
CR 6.2 – Continuous monitoring		+	+	+
FR 7 – Resource Availability (RA)				
CR 7.1 – Denial of service protection	+	+	+	+
CR 7.2 – Resource management	+	+	+	+
CR 7.3 – Control system backup	+	+	+	+
CR 7.6 – Network and security configuration settings		+	+	+

Требования к встроенным средствам защиты АСТУ электросетевого комплекса (Распоряжение №282) ОАО «Россети» от 17.06.2014

infotecs

АСУ объектового уровня

Системы технологической связи

Системы телемеханики

Системы определения места повреждения

АСКУИЭ

Системы РЗА

Системы противоаварийной автоматики

Системы регистрации аварийных событий

Системы мониторинга и диагностики

Системы сигнализации состояния вспомогательных систем

Требования к встроенным средствам защиты АСТУ электросетевого комплекса (Распоряжение №282) ОАО «Россети» от 17.06.2014

infotecs

- Аудит безопасности
- Контроль доступа
- Идентификация и аутентификация
- Конфигурация безопасности
- Доступность
- Защита среды функционирования
- Защита данных пользователя
- Требования доверия

Security by design

Конечные устройства получают необходимые функции безопасности, реализующие меры защиты, на этапе их разработки:

- ИБ является частью устройства
- Верификация функционала при проведении тестирования и испытаний как конечного устройства, так и системы
- Уменьшение ошибок в конечной системе
- Уменьшение стоимости конечного решения
- Возможность гибкой обработки событий ИБ

Встраиваемые средства защиты информации

Проблемы реализации концепции Security by design

- Необходимость погружения в ИБ разработчиков устройств автоматизации
- Высокая трудоемкость реализации функций ИБ
- Высокая ресурсоемкость исполнения модулей с функциями ИБ
- Отсутствие единых требований и рекомендаций
- Необходимость сертификации
- Необходимость реализации целиком решения, а не только функций для одного устройства
- Необходимость реализации продуктов по управлению функциями ИБ

Встраиваемые средства

- Часть функций ИБ или все функции могут возлагаться на встраиваемые средства защиты
- Встраиваемы средства защита встравиваются в устройства на этапе разработки
- Конфигурирование и установка аппаратных встраиваемых средств защиты осуществляется на этапе производства

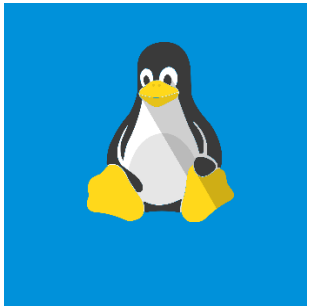
Практические кейсы по применение встраиваемых средств защиты

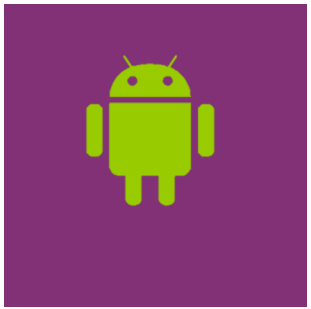
Реализация защищенного канала для контроллеров и устройств автоматизации полевого уровня

ViPNet Client – защита каналов связи рабочих станций и конечных устройств

КОМПЬЮТЕРЫ НОУТБУКИ

ТЕЛЕФОНЫ ПЛАНШЕТЫ





Встраиваемая версия ViPNet Client

LINUX BASED

x86 ARM MIPS МЦСТ ЭЛЬБРУС

КОНТРОЛЛЕРЫ И КОНЕЧНЫЕ УСТРОЙСТВА АВТОМАТИЗАЦИИ

ViPNet Client – защита каналов связи рабочих станций и конечных устройств

infotecs

SCADA LEVEL

Operator workstation
ViPNet Client for Windows
ViPNet Client for Linux

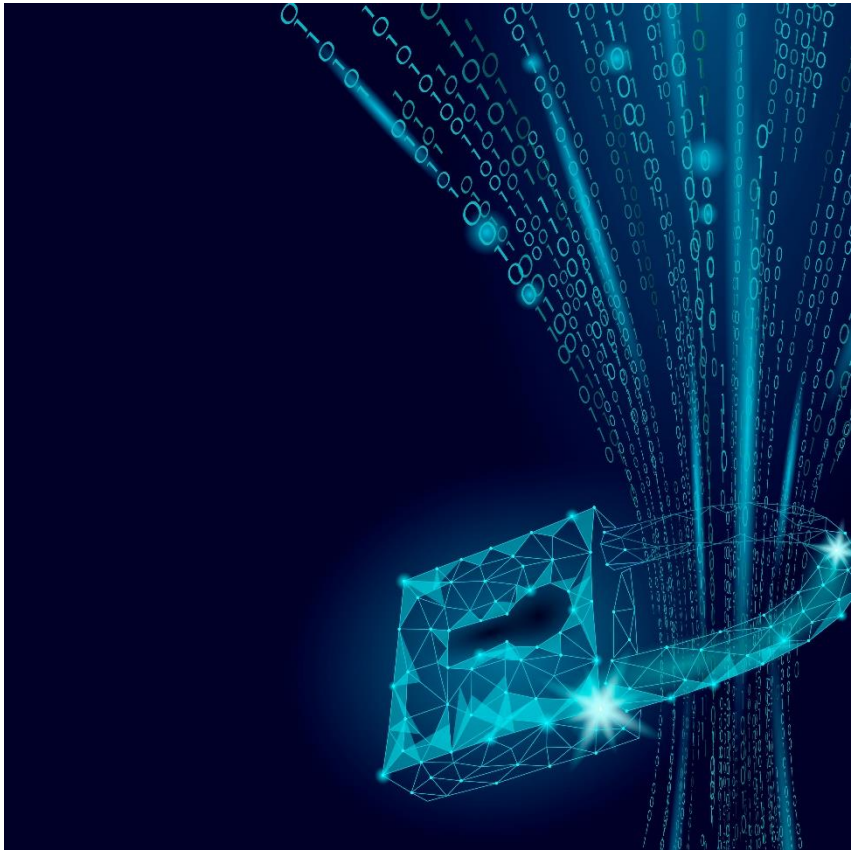
HMI
ViPNet Client for Windows
ViPNet Client for Linux

Mobile Workstation
ViPNet Client for Android
ViPNet Client for iOS

AUTOMATION LEVEL

Engineer Workstation
ViPNet Client for Windows
ViPNet Client for Linux

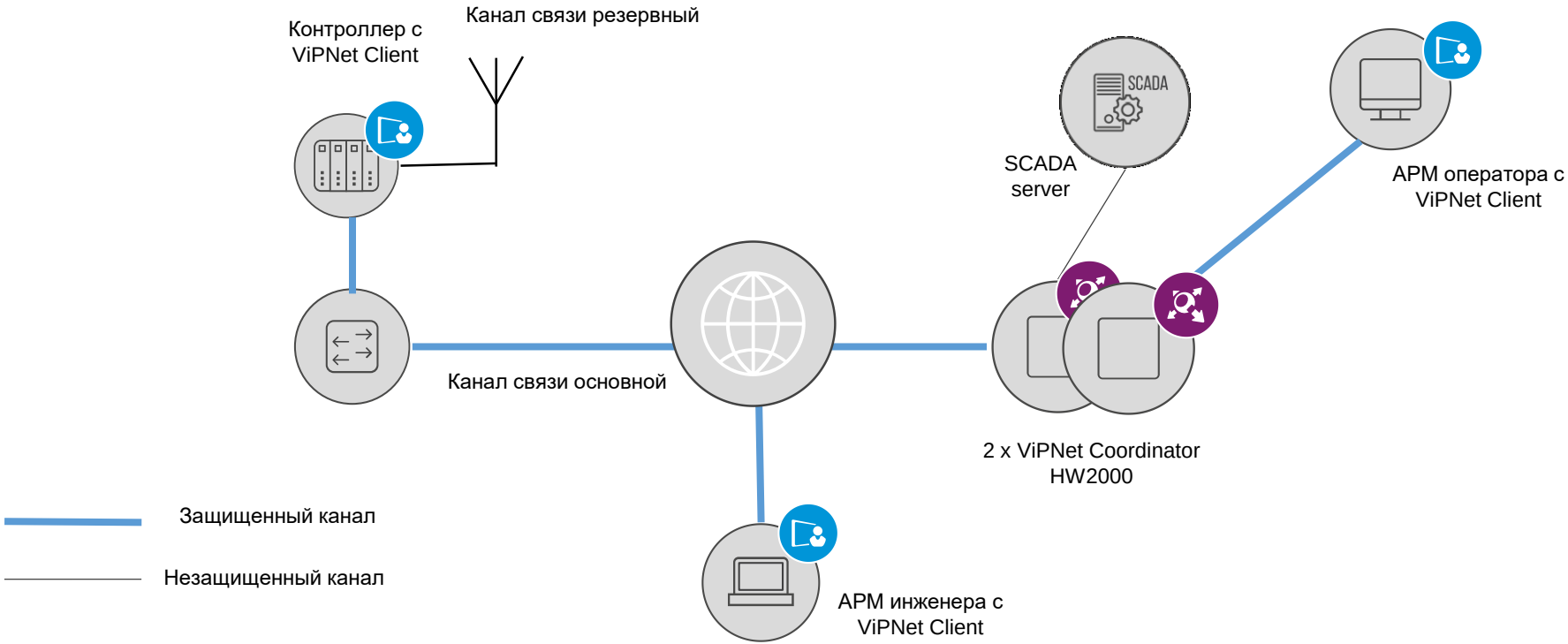
PLC
Встраиваемый
ViPNet Client for Linux



Встраиваемы ViPNet Client для Linux

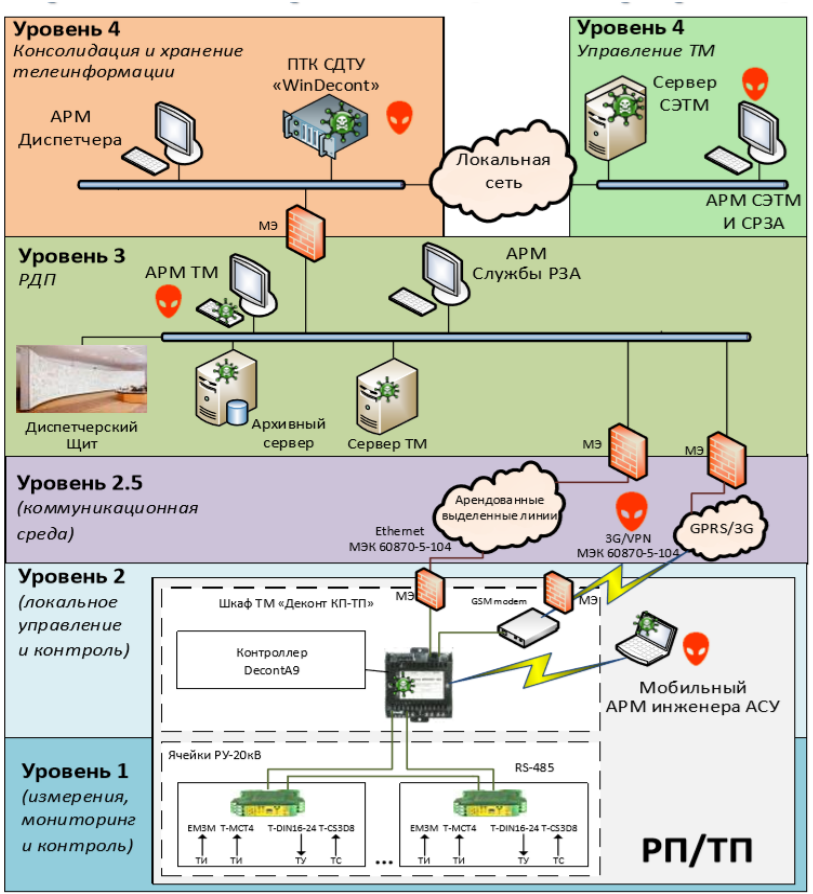
- Законченный продукт, СКЗИ класса КС1
- Совместим со всеми продуктами линейки ViPNet Network Security
- Дистанционное управление ключевой информацией
- Работа в фоновом режиме
- Автоматическая загрузка после рестарта

Встраивание ViPNet Client в контроллеры РЭС, контроллеры ТМ/ТП, УСПД



Endpoint protection для конечных устройств АСУ

Угрозы безопасности информации АСТУ



Информация ограниченного доступа:

- Управляющая
- Контрольно-измерительная
- Идентификационная
- Программно-техническая

Угрозы безопасности:

- Преднамеренные (целевые)
- Непреднамеренные (ошибки)

Способы воздействия:

- Локально
- Удаленно (сетевая атака)

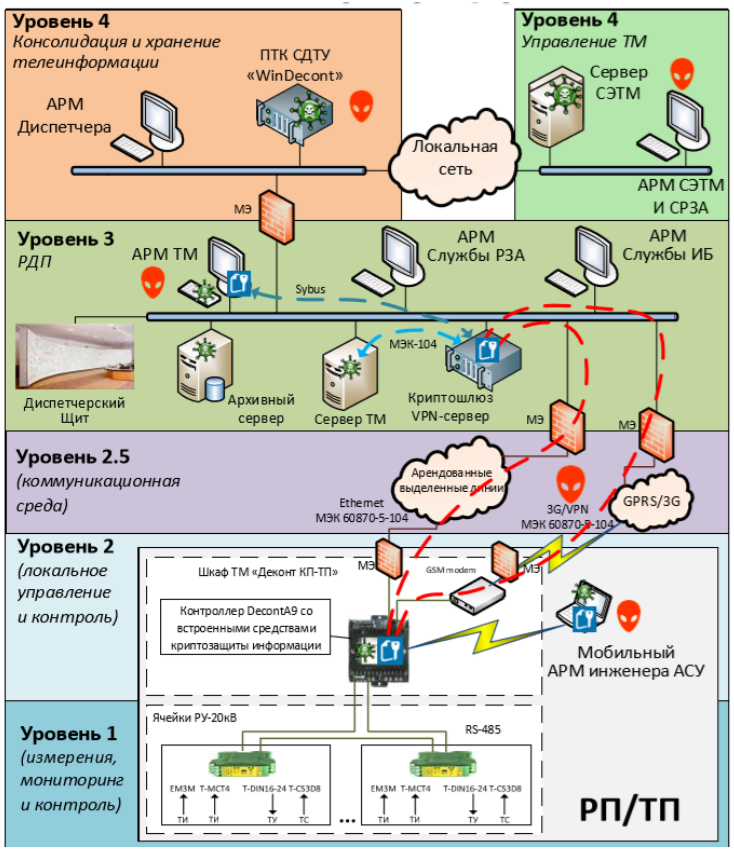
Нарушитель:

- Внешний
- Внутренний

Угрозы безопасности информации АСТУ

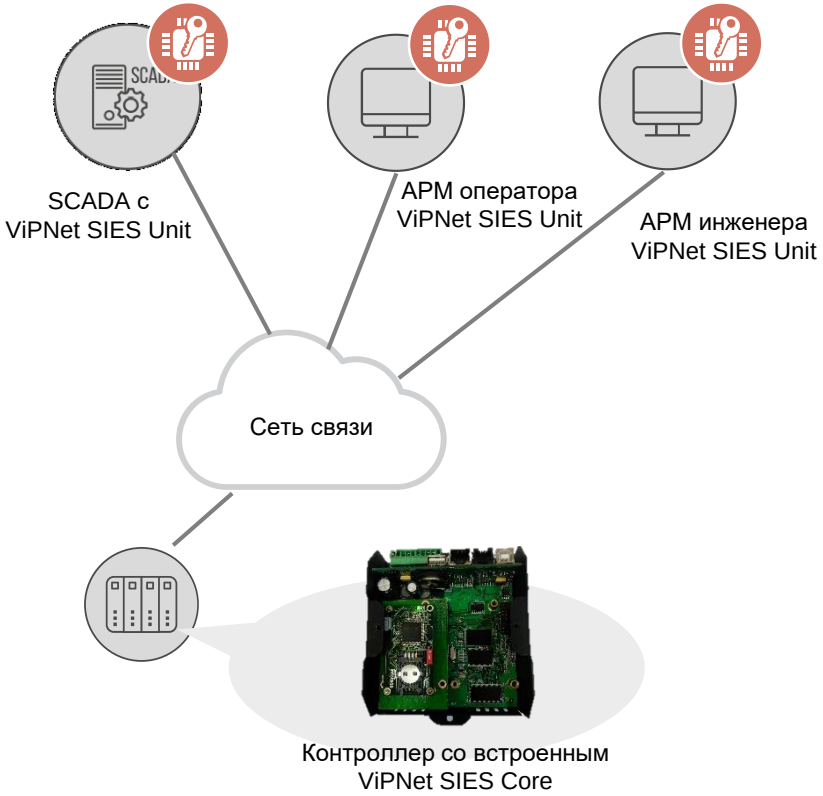
- Авторизация нелегальный пользователей
- Модификация информации при сетевом обмене
- Модификация информации в компонентах АСТУ
- Угрозы неправомерных действий в каналах связи
- Угрозы модификации/разрушения программного окружения исполняемого кода компонентов АСТУ

Защищенные конечные устройства АСТУ



- Организация доверенных коммуникаций
- Обеспечение целостности передаваемой информации по внешним каналам связи
- Организация удаленного достоверного соединения с устройствами АСУ-ТМ
- Доверенная локальная и удаленная загрузка обновлений контроллера
- Безопасное хранение конфигурационных параметров контроллера и телеизмерений
- Усиленная авторизация и взаимная аутентификация пользователей и процессов
- Доверенное конфигурирование АСУ-ТМ

Компоненты защиты



Уровень ОДУ:

- SCADA server SYTrack с ViPNet SIES Unit
- АРМ инженера с ViPNet SIES Unit
- АРМ оператора с ViPNet SIES Unit
- ViPNet SIES MC (управление решением SIES)

Уровень сетевого взаимодействия:

- Доверенные коммуникации – защита криптографическими протоколами CRISP, CMS

Уровень объекта управления

- Контроллер со встроенным модулем ViPNet SIES Core и доверенным ПО, прошедшим сертификацию по ВСрЗИ

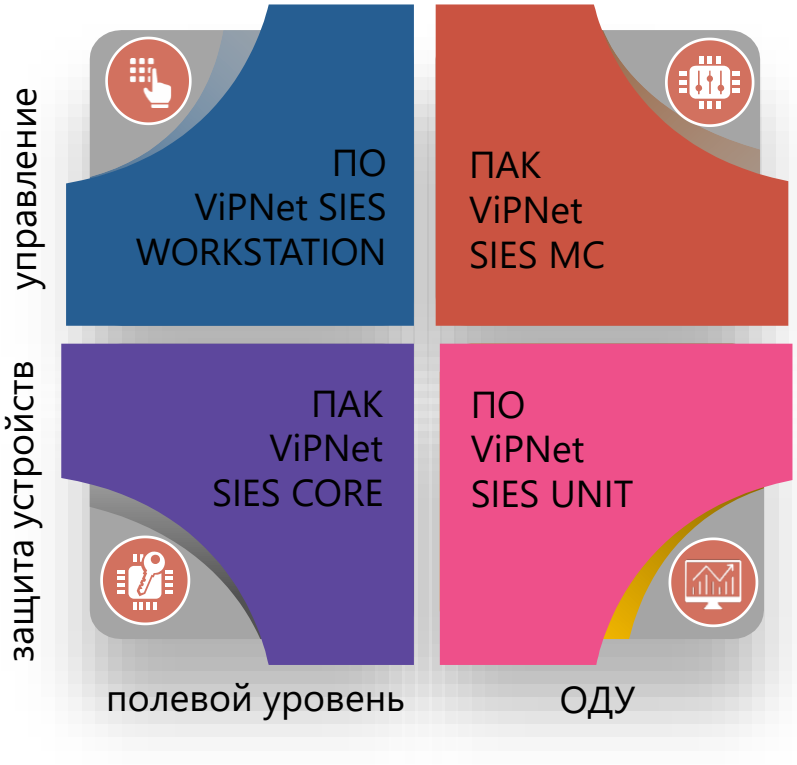
ViPNet SIES – платформа по защите информации

infotecs

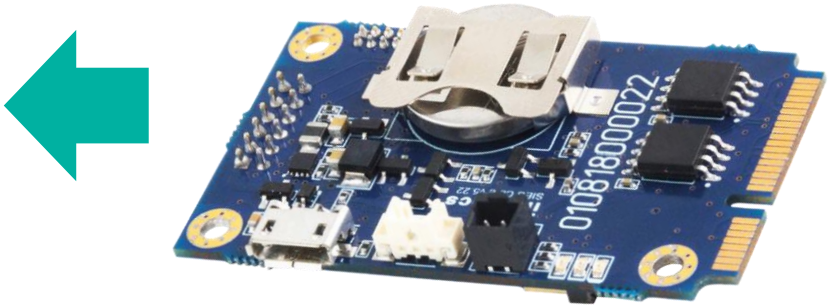
ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНТЕГРАЦИИ В УСТРОЙСТВА АВТОМАТИЗАЦИИ НА ВСЕХ УРОВНЯХ АСУ

ЗАЩИТА КОММУНИКАЦИЙ • ЗАЩИТА КОНЕЧНЫХ УЗЛОВ • ЗАЩИТА ДАННЫХ • АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Состав решения ViPNet SIES



- Законченные СКЗИ класса КС1 и КС3, не требуют оценки влияния
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств



Интеграция ПАК SIES Core

На аппаратном уровне – USB, UART, SPI

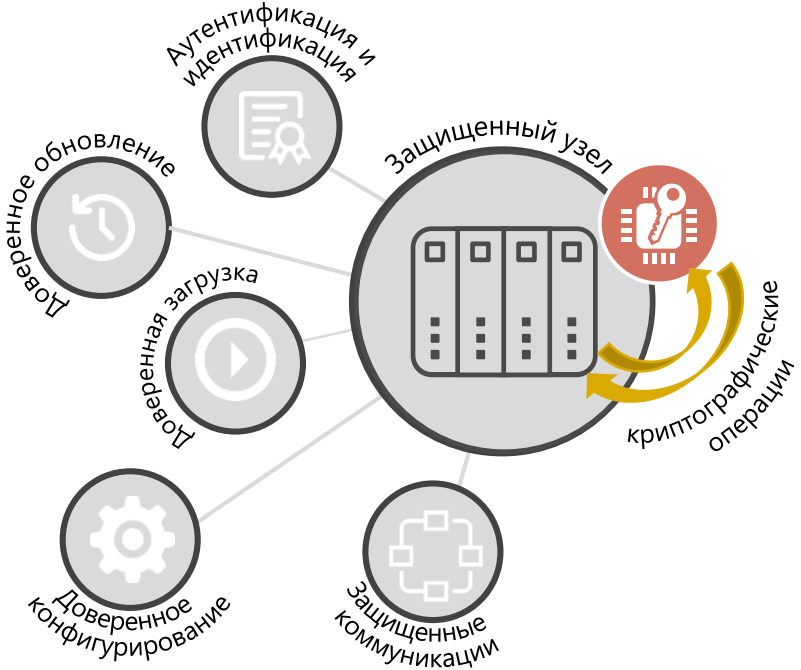
На программном уровне – SIES Core API (RATP+прикладной протокол)

Интеграция ПО ViPNet SIES Unit

Поддерживаемые ОС:

- Windows 7/8/8.1/10 (x86/64)
- Windows Server 2008/R2/2012/2012 R2/ 2016
- Debian 9, Ubuntu 16, Ubuntu 18 и др ОС Linux:
  - gcc v.6 и выше,
  - systemd система инициализации,
  - x86/64 архитектура процессора
  - менеджер пакетов deb/rpm формата
- Astra Linux Special Edition (Смоленск) 1.6 (x86/64)

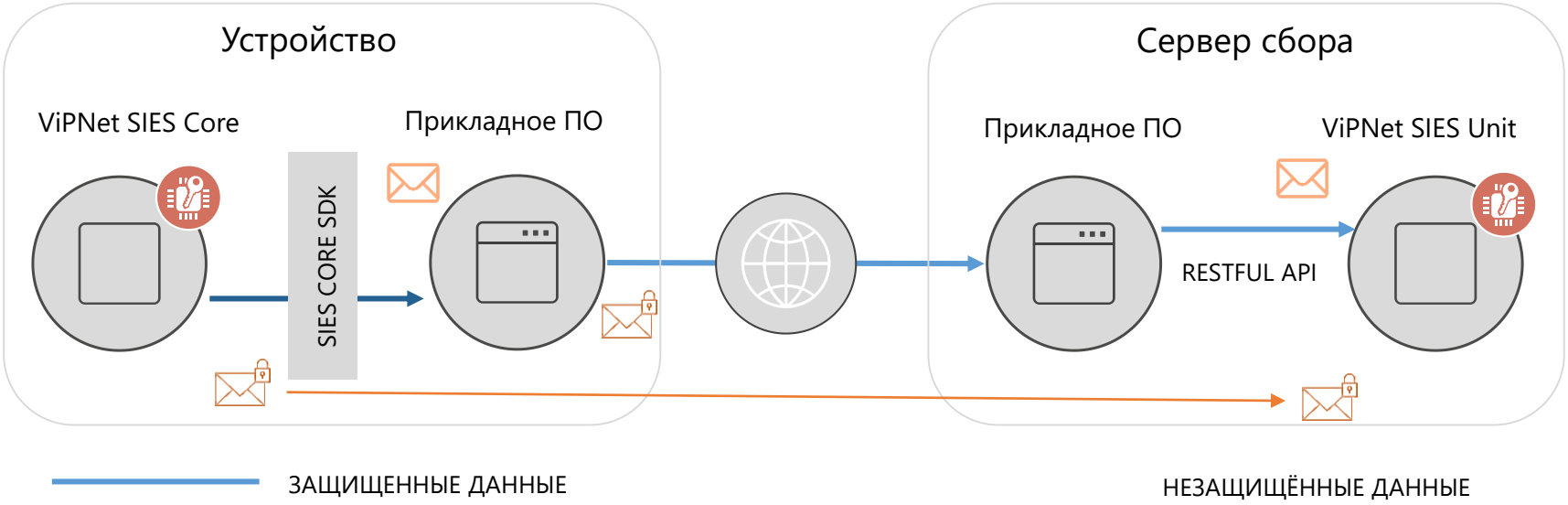
Криптографические сервисы для защищаемых устройств



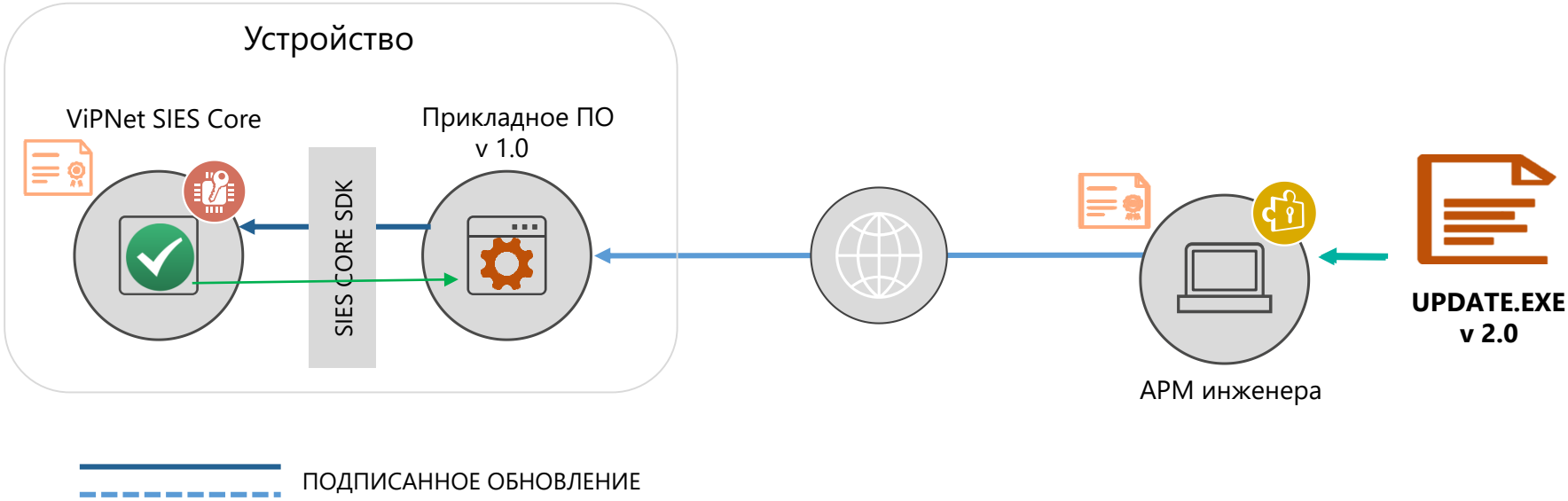
Сценарии защиты информации:

- Обеспечение конфиденциальности передаваемых данных
- Обеспечение аутентичности и целостности передаваемых данных
- Доверенное локальное и удаленное обновление ПО устройства
- Доверенное локальное и удаленное конфигурирование устройства
- Доверенная загрузка устройства
- Двухфакторная аутентификация на устройстве

Защита коммуникаций с помощью ViPNet SIES



Доверенное обновление контроллера с помощью ViPNet SIES



ГОСТ 28147-89

ГОСТ Р 34.11-2012
ГОСТ 34.11-2018

ГОСТ Р 34.12-2015
ГОСТ Р 34.13-2015
ГОСТ 34.12-2018
ГОСТ 34.13-2018

ГОСТ Р 34.10-2012
ГОСТ 34.10-2018

Криптографические операции, доступные защищаемым устройствам

Концепция «Security by design» для АСУ = реальность сегодня

infotecs

Спасибо
за внимание!