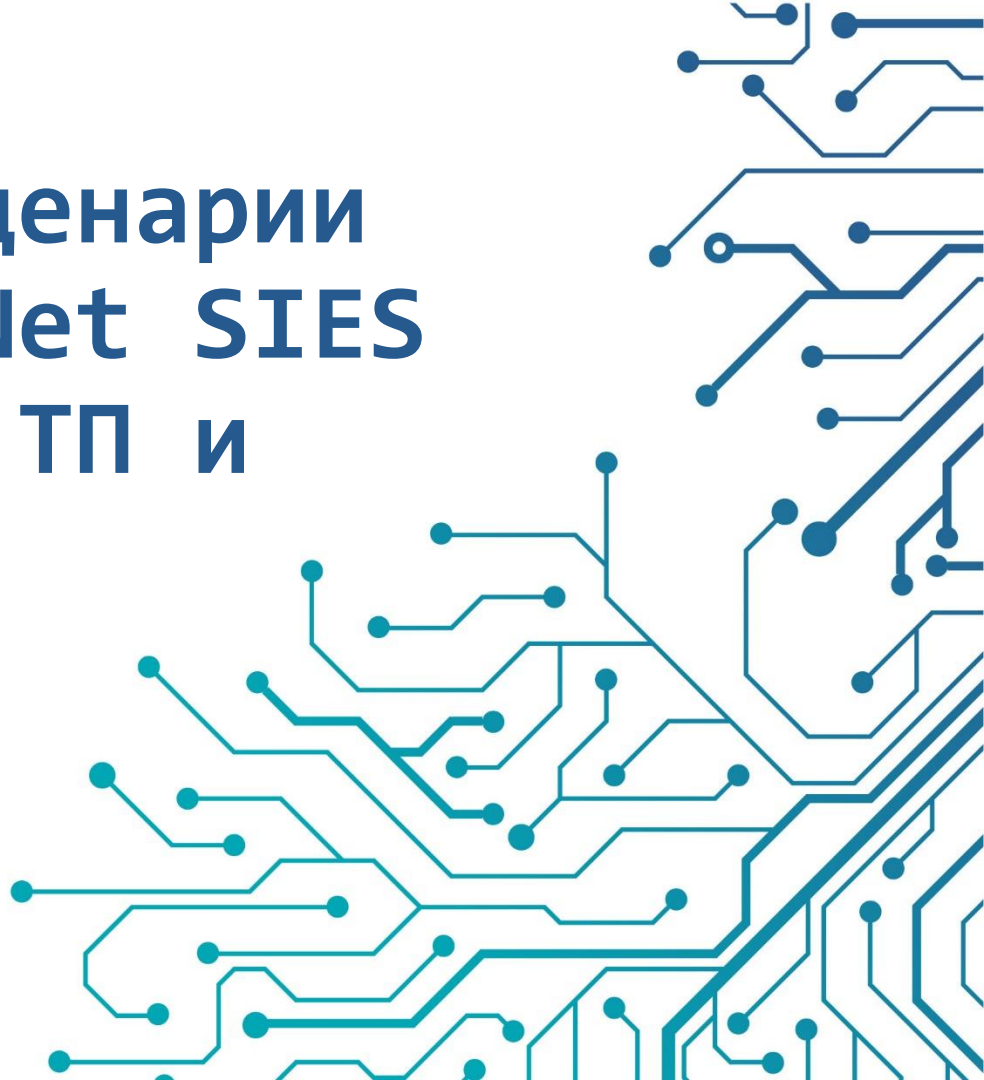
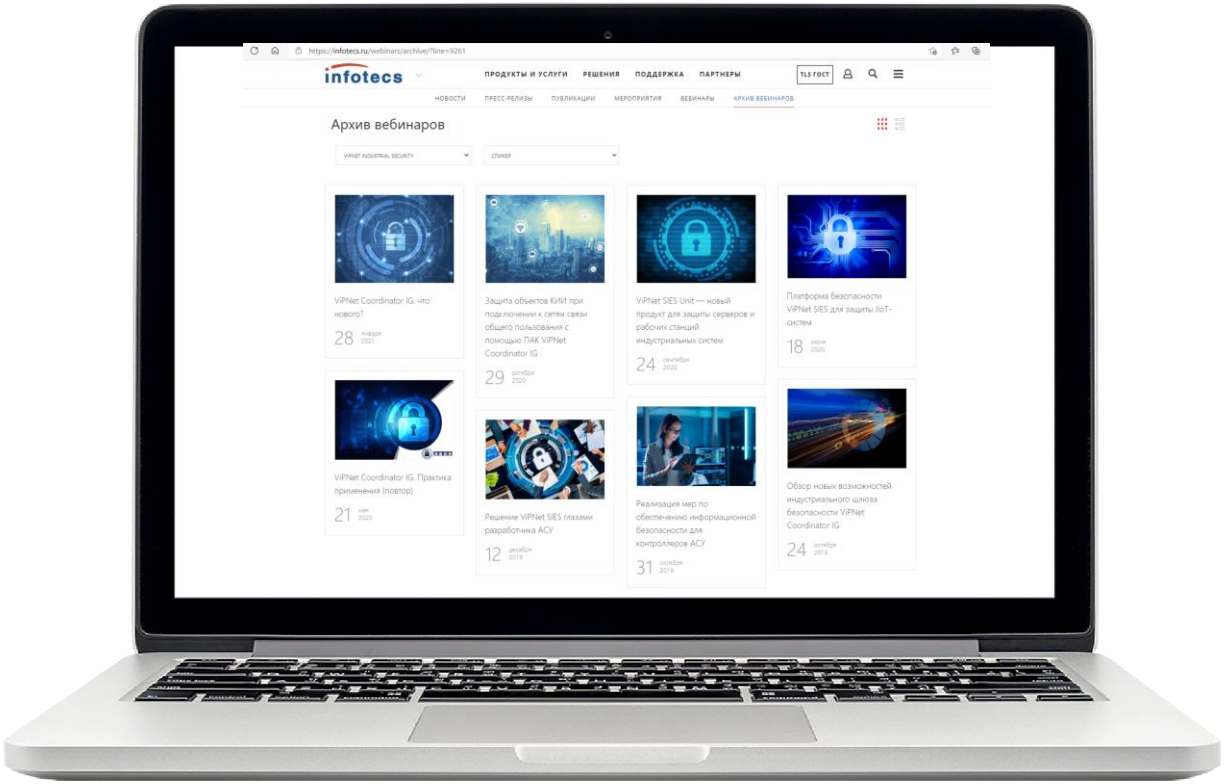
Практические сценарии применения ViPNet SIES для защиты АСУ ТП и IIoT-систем.

Сергей Лыдин
Руководитель направления
отдела клиентских проектов

infotecs



Вебинары по ViPNet SIES

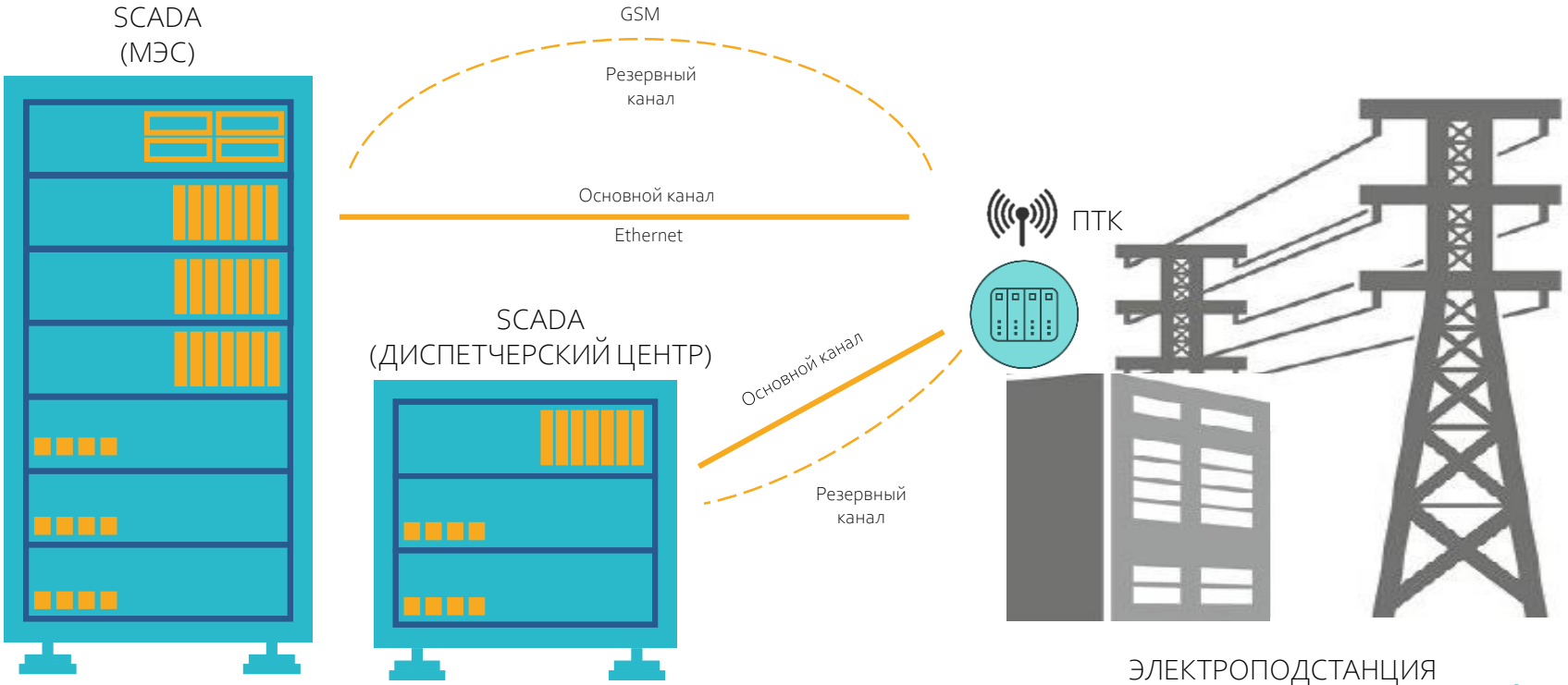


Видео и презентации вебинаров:

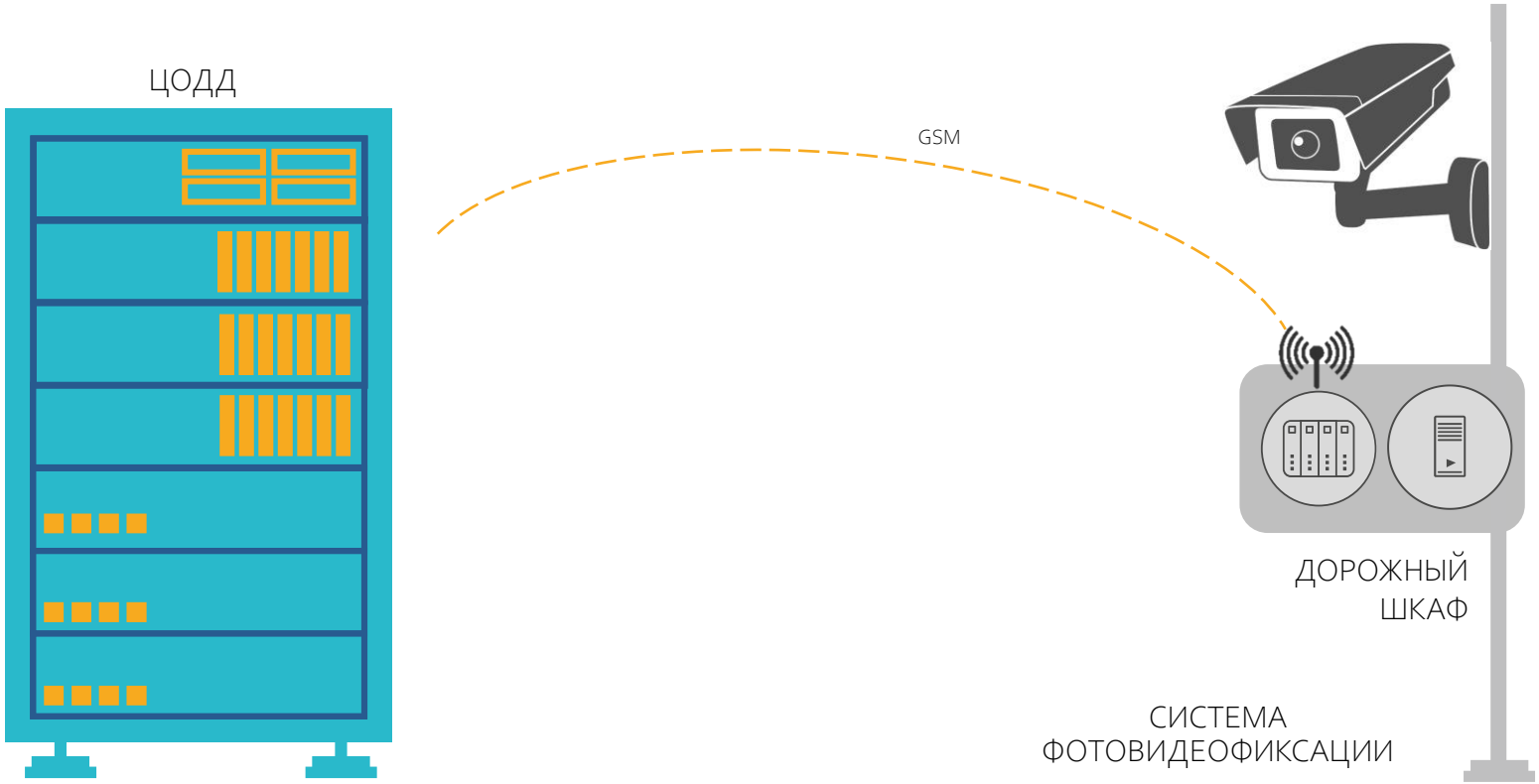
- [Архив вебинаров | ИнфоТеКС (infotecs.ru)]
- https://infotecs.ru/webinars/archive/


ПОЧЕМУ КРИПТОГРАФИЯ?

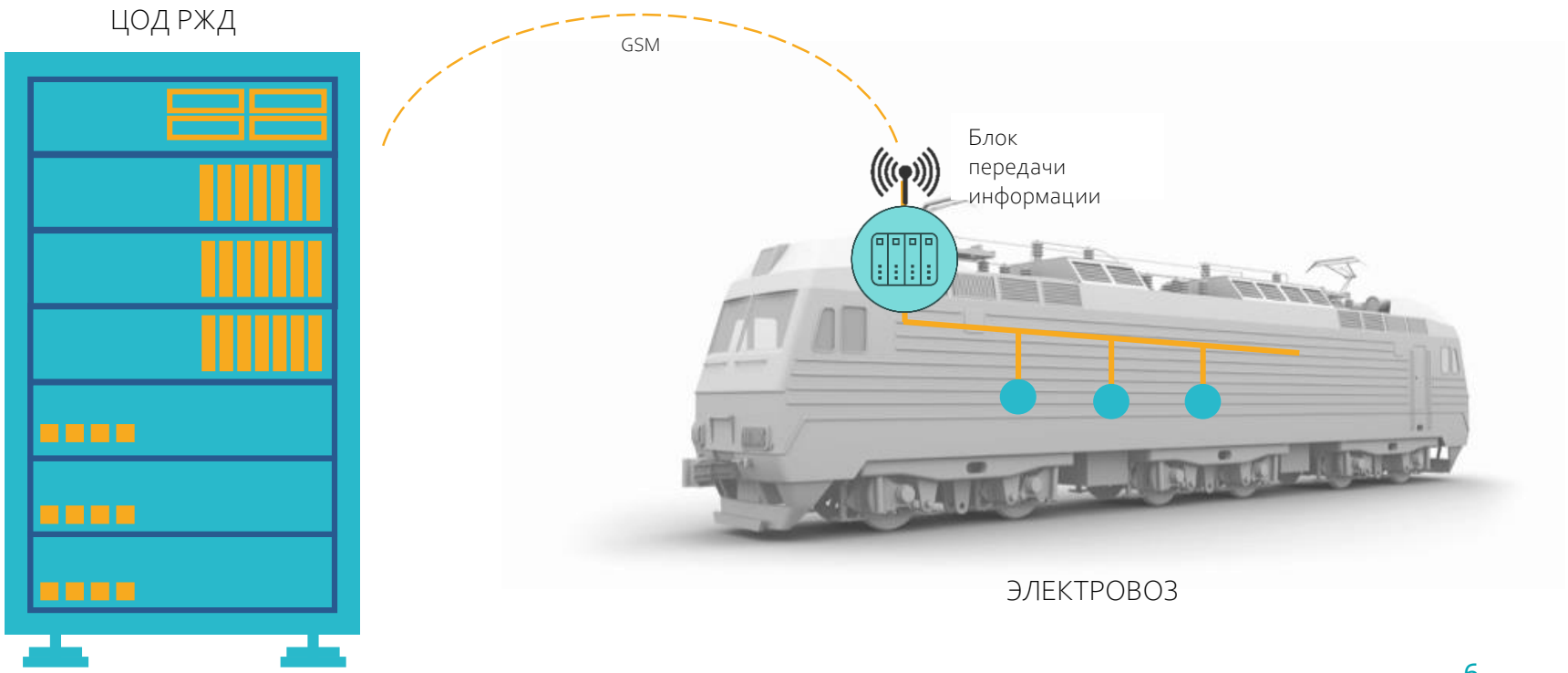
Объекты защиты



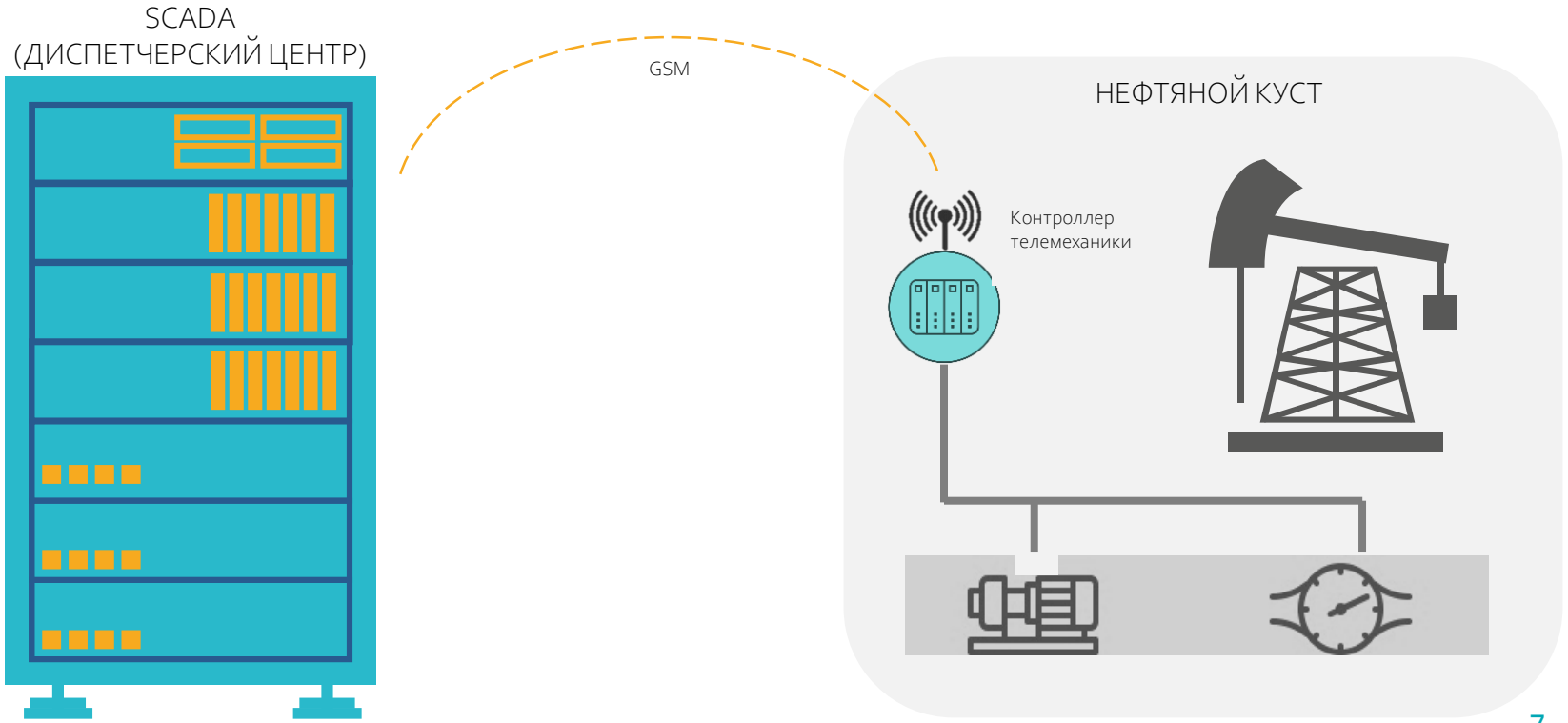
Объекты защиты



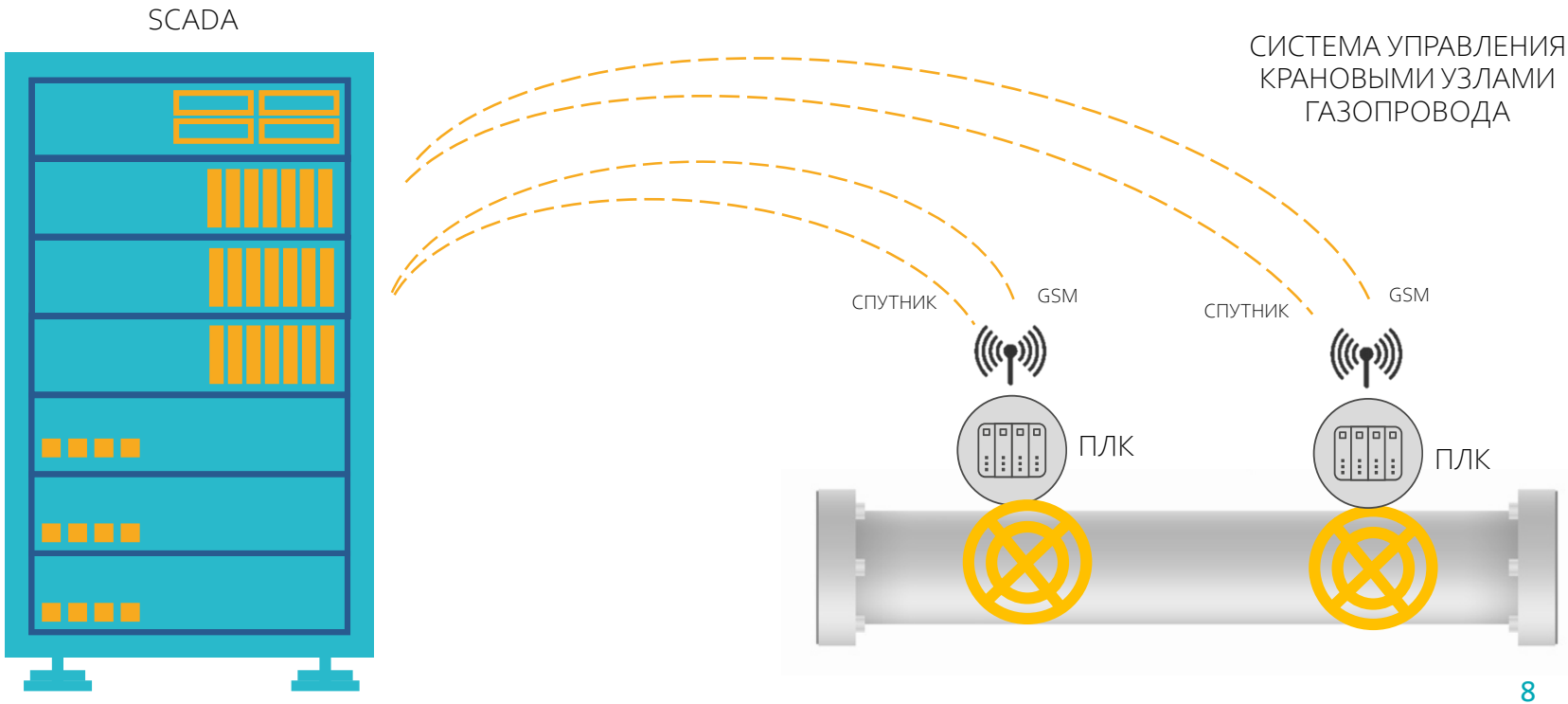
Объекты защиты



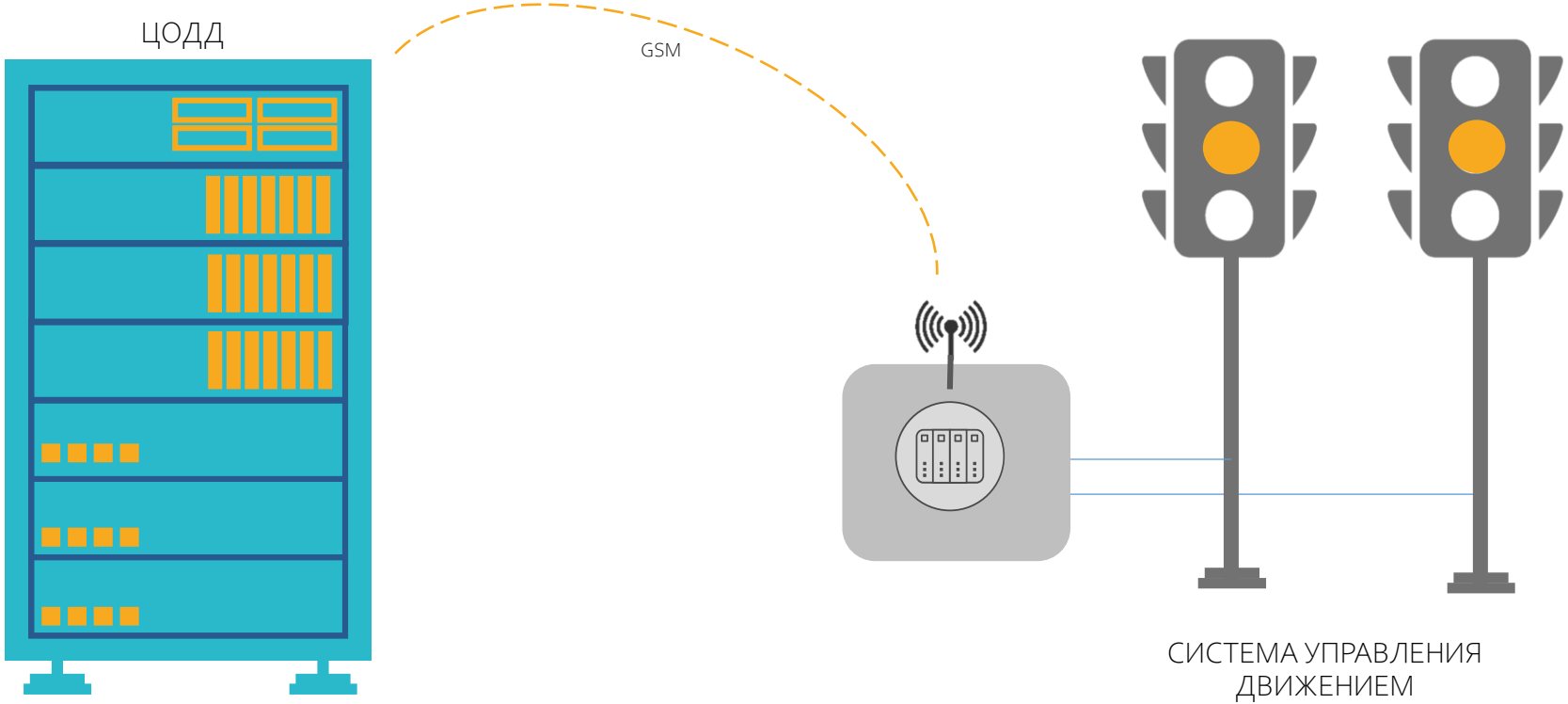
Объекты защиты



Объекты защиты



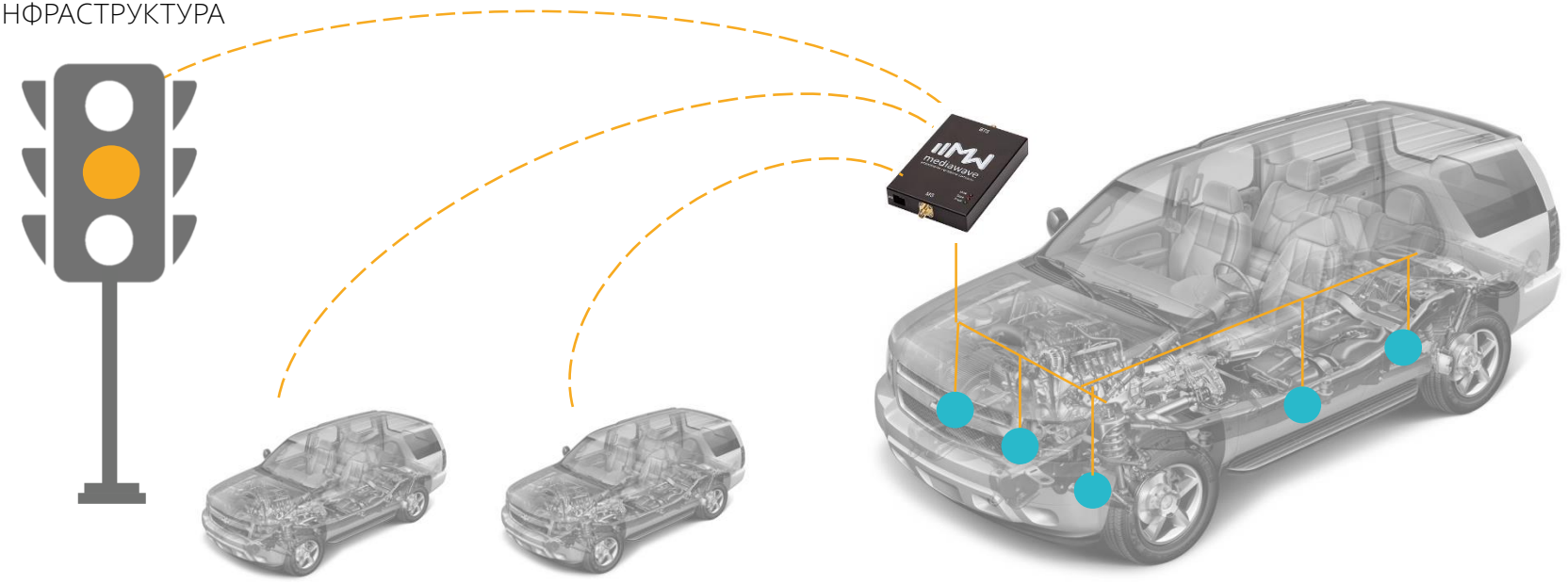
Объекты защиты



Объекты защиты

Объекты защиты

ДОРОЖНАЯ
ИНФРАСТРУКТУРА



ТРАНСПОРТНЫЕ СРЕДСТВА НА ДОРОГЕ

ИНТЕЛЕКТУАЛЬНЫЙ
ТРАНСПОРТ

Объекты защиты

Основные угрозы безопасности информации АСУ ТП и IIoT-систем

- Несанкционированный доступ к данным (искажение данных)
- Перехват управления (навязывание команд, выведение из строя устройств)
- Подмена устройств (передача некорректных данных, нарушение стабильной работы сети устройств)
- Перепрошивка устройств (организация ботнетов, воздействие на объект управления)

Защищаемая информация АСУ ТП и IIoT-систем

Защищаемая информация	Возможности криптографии
• Данные (телеметрия, конфигурация и др.) • Команды управления • Программное обеспечение	• Целостность • Конфиденциальность • Аутентичность

Применение наложенных средств защиты информации

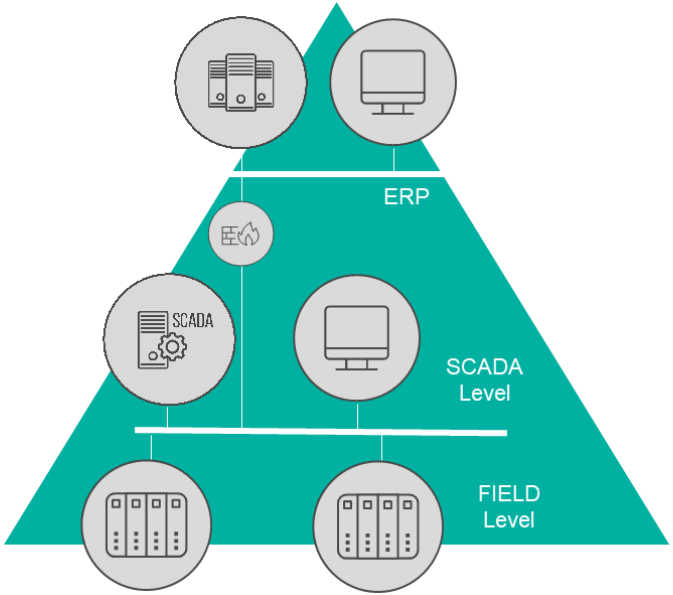
infotecs

Наложенные СЗИ (СКЗИ)

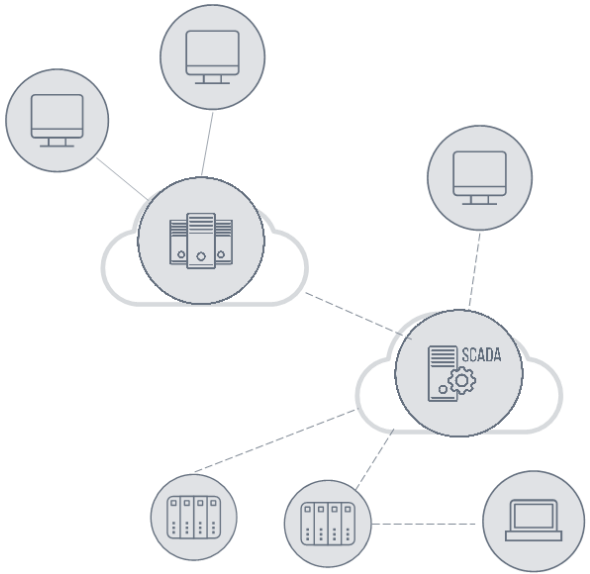
- Защита периметра
- Сегментирование
- Защита каналов связи

Применение встраиваемых средств защиты информации

Отсутствие периметра IIoT-системы



Классическая АСУ



IIoT-система

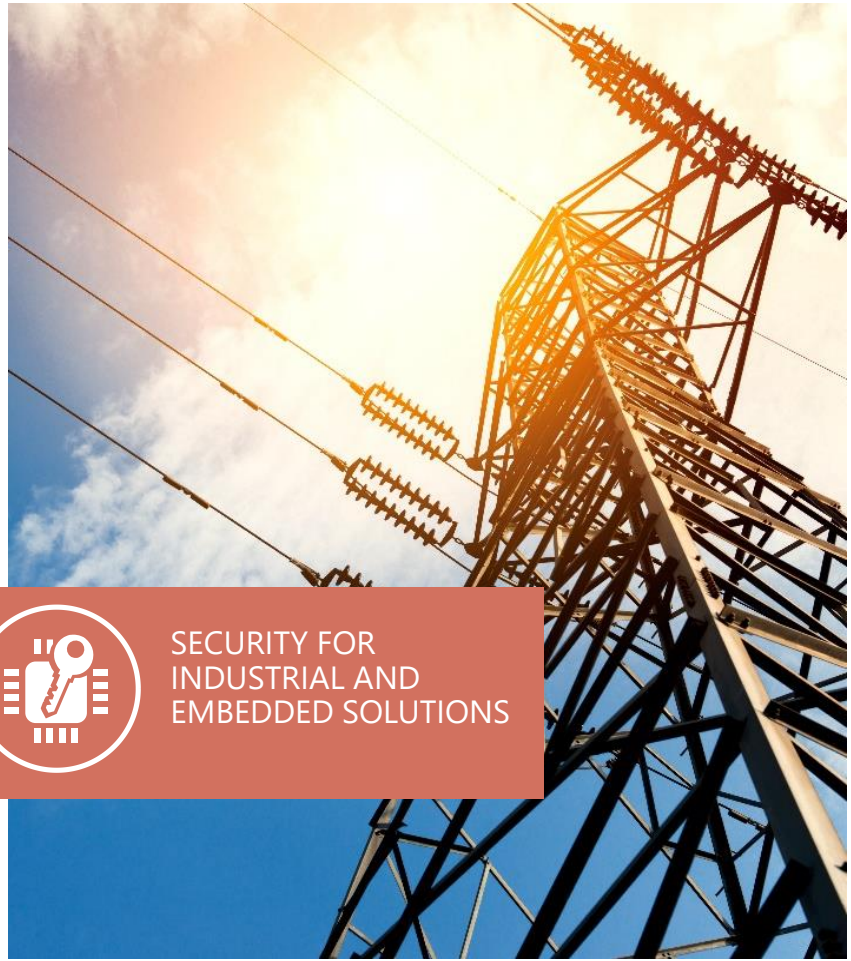
Особенности и ограничения АСУ ТП и IIoT-систем

- Широкий диапазон объемов информационного обмена и допустимых задержек
- Ограниченные вычислительные ресурсы
- Специализированное ПО (прошивка), часто без операционной системы
- Автономное питание
- Многообразие протоколов и каналов связи
- Аппаратные исполнения для работы в сложных климатических условиях
- Малообслуживаемые условия эксплуатации

Особенности и ограничения АСУ ТП и IIoT-систем

- Высокая емкость отдельных сетей
- Продолжительный жизненный цикл устройств
- Разнообразие отраслевых стандартов и условий оценки соответствия
- Неопределенность периметра безопасности
- Строгие требования по стоимости для массовых устройств
- Слабые аппаратные возможности для реализации криптографических механизмов
- Достаточно закрытое сообщество компаний, способных разрабатывать прошивки для защищенных микроконтроллеров

Защита АСУ ТП и IIoT-систем с помощью СКЗИ



Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

- для устройств автоматизации на всех уровнях АСУ
- для IIoT-устройств

ГОСТ Р 34.11-2012
ГОСТ 34.11-2018

ГОСТ 28147-89

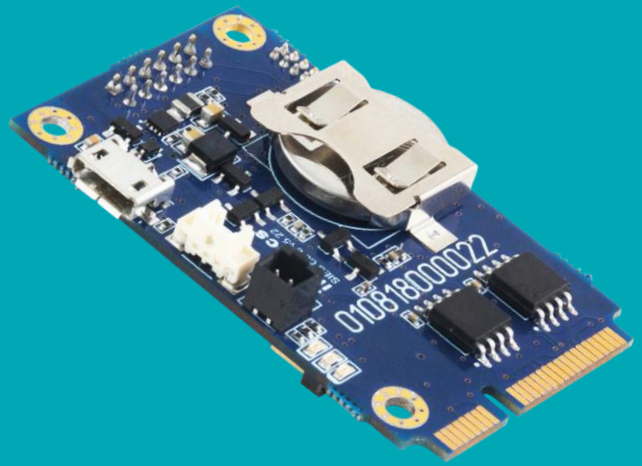
ГОСТ Р 34.12-2015
ГОСТ Р 34.13-2015
ГОСТ 34.12-2018
ГОСТ 34.13-2018

ГОСТ Р 34.10-2012
ГОСТ 34.10-2018

Криптографический сервис для защищаемых устройств

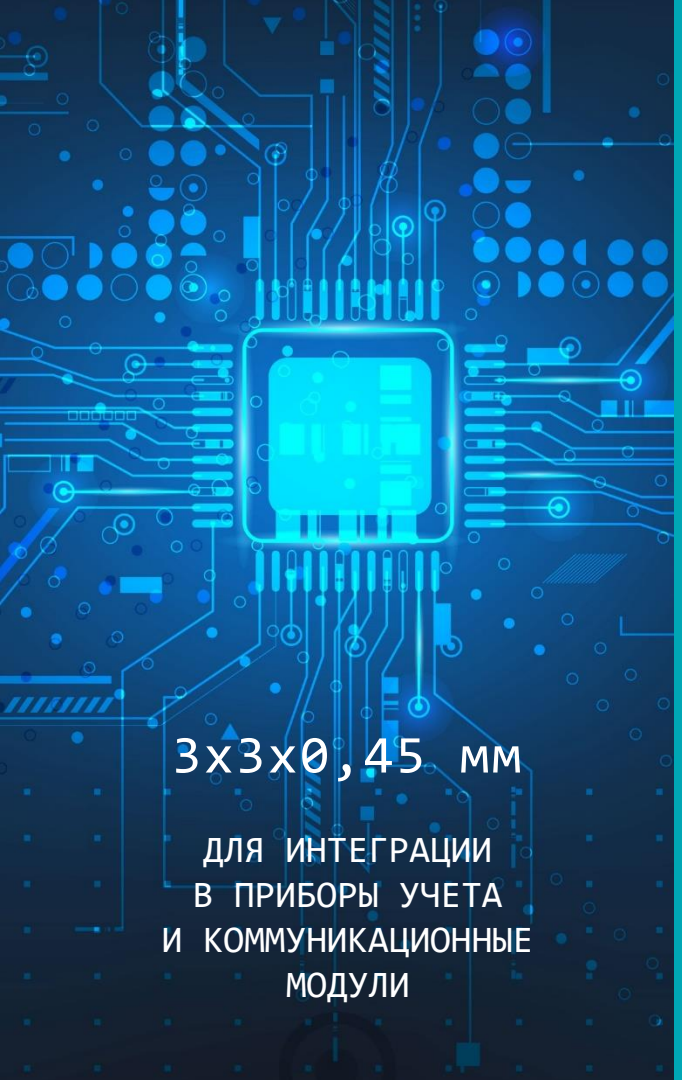
Состав решения ViPNet SIES

- СКЗИ класса КС1 и КС3, соответствующие требованиям ФСБ России
- Применение криптографии на разных по вычислительной мощности устройствах
- Отсутствие зависимости от ОС и архитектуры устройств



- ПАК – System On a Module (SOM)
- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм)
- Интеграция на аппаратном уровне – USB, UART, SPI
- Интеграция на программном уровне – SIES Core API
- Наличие SDK для Linux (ARM, x86),Windows, RTOS
- Возможность использования вне контролируемой зоны при использовании ДНСД
- Рабочий диапазон температур – -40…+70 ^{0}C
- Сертификат СКЗИ класса КС3

СКЗИ ViPNet SIES Core для IIoT-шлюзов и ПЛК



ПАК ViPNet SIES Core Nano

Встраивание:

- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

Криптографический протокол:

- Зашифрование/расшифрование
- Создание имитовставки/ проверка имитовставки

Функциональные особенности:

- 3 резервируемых ключа связи
- Хранение ключевой информации 16 лет
- Рабочий диапазон температур -40…+85 ^{0}C
- Форм-фактор – микросхема 3x3x0,45 мм

Проводится сертификация:

- СКЗИ-НР и СКЗИ класса КС3

ViPNet SIES Core Nano

infotecs

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

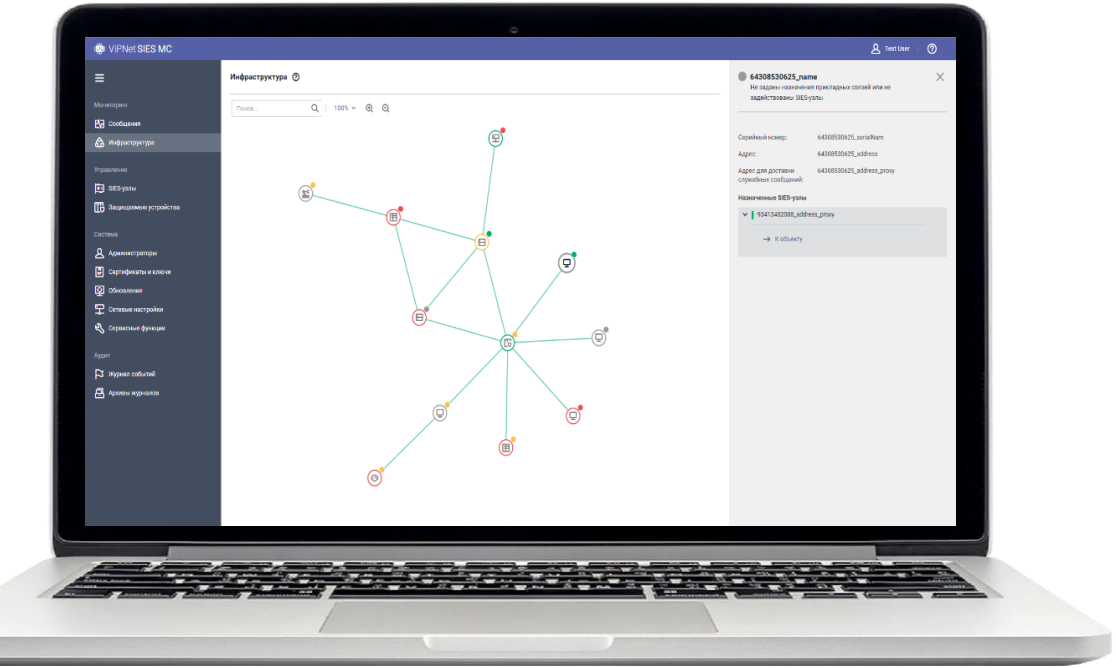
полностью
российская
разработка

ПО ViPNet SIES Unit

ДЛЯ УСТАНОВКИ НА ЗАЩИЩАЕМОЕ УСТРОЙСТВО ИЛИ ВЫДЕЛЕННУЮ ПЛАТФОРМУ

- Интеграция по RESTAPI (HTTP/1.1), gRPC API (HTTP/2) или SDK;
- Поддерживаемые ОС:
  - Windows 8.1/10
  - Windows Server 2012/2012 R2/ 2016
  - Debian 9.8, 10/ Ubuntu 16, Ubuntu 18
  - Astra Linux Special Edition (Смоленск) 1.6
- Поддержка архитектуры процессора x86-32, x86-64, ARM (armhf)
- Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

Центр управления ViPNet SIES MC



- Ключевой и Удостоверяющий центры
- Управление связями в системе
- Дистанционная смена ключевой информации
- Управление активами
- Разграничение прав доступа к решению SIES
- Доступ к интерфейсу по WedUI

Центр управления ViPNet SIES MC

ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Сертификат СКЗИ КС1

ViPNet SIES MC 3000

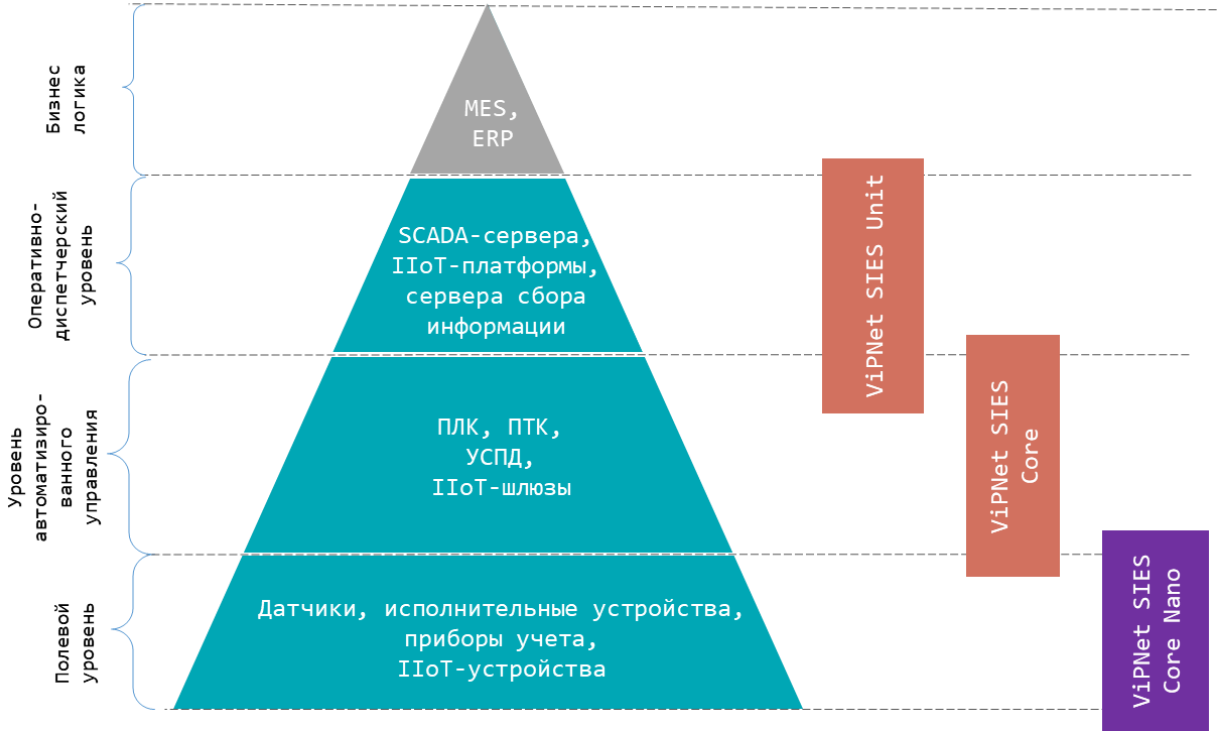
- Max: 3000-узлов
- Max: 300 администраторов безопасности
- Сертификат СКЗИ КС3

ViPNet SIES MC 10000

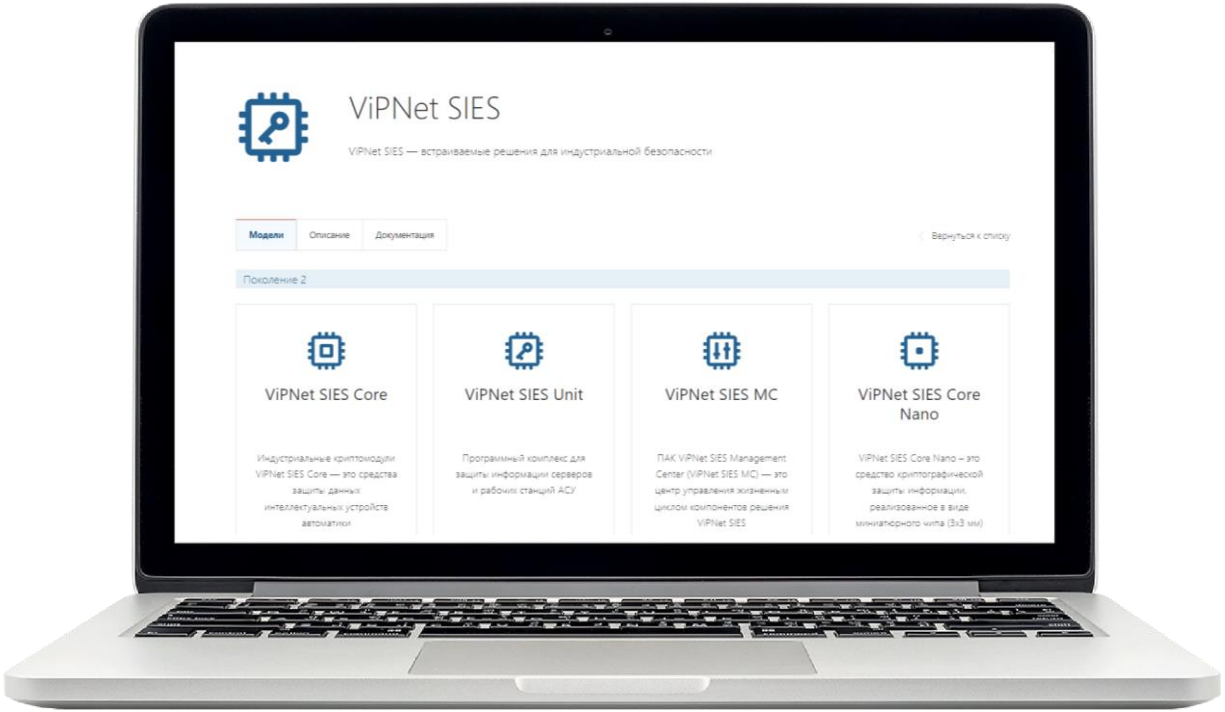
- Max: 1 млн узлов
- Max: 1000 администраторов безопасности
- Сертификат СКЗИ КС3

Встраиваемые продукты ViPNet SIES

Встраиваемые криптографические средства защиты информации для интеграции в устройства автоматизации на всех уровнях АСУ



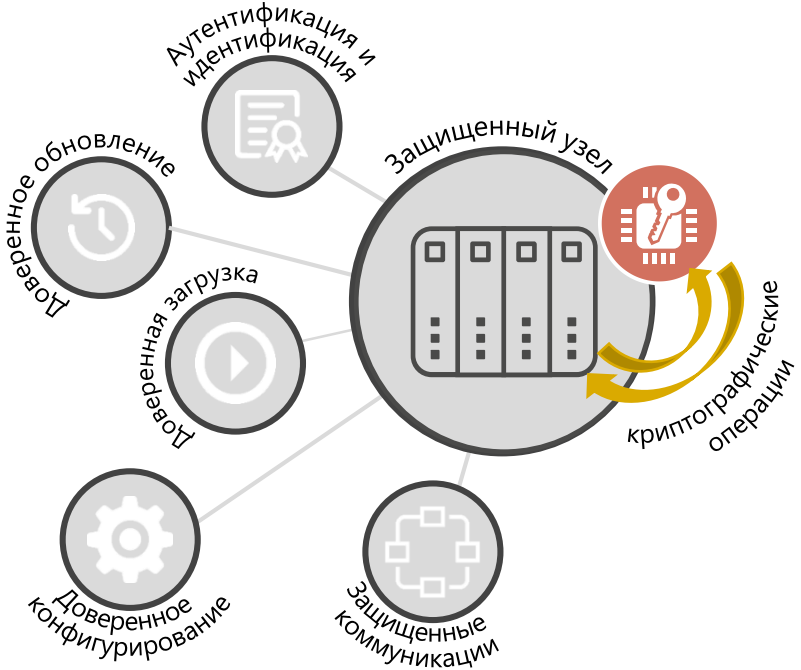
Информация по ViPNet SIES



Вся новая информация доступна на сайте – [ViPNet SIES | ИнфоТеКС (infotecs.ru)]

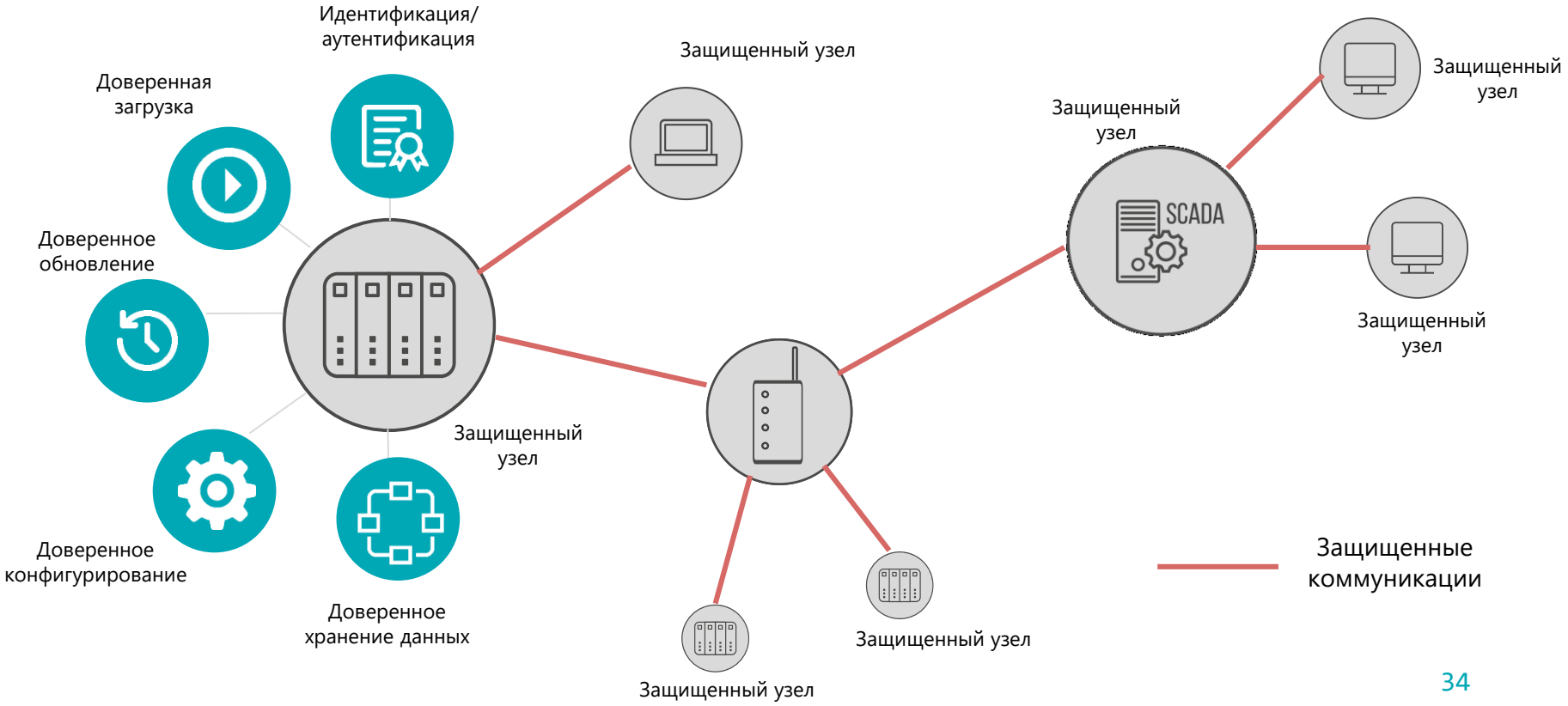
Типовые сценарии применения ViPNet SIES

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
- Стойкая аутентификация на устройстве

Защита на уровне конечных устройств



Протоколы IIoT-систем

Протоколы IIoT-системы, которые можно защищать с помощью решения ViPNet SIES

Встраивание СКЗИ

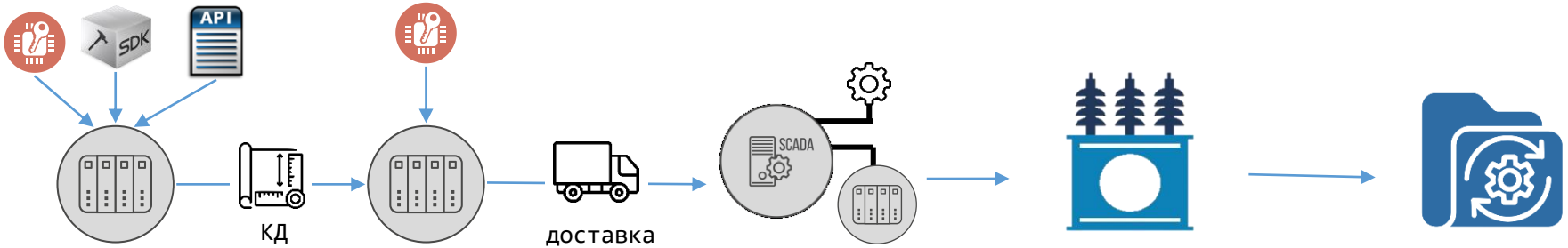
РАЗРАБОТКА УСТРОЙСТВА

ПРОИЗВОДСТВО УСТРОЙСТВА

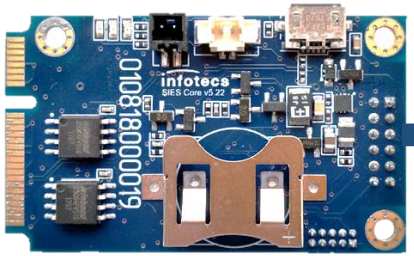
ВВОД В ЭКСПЛУАТАЦИЮ УСТРОЙСТВА

ЭКСПЛУАТАЦИЯ УСТРОЙСТВА

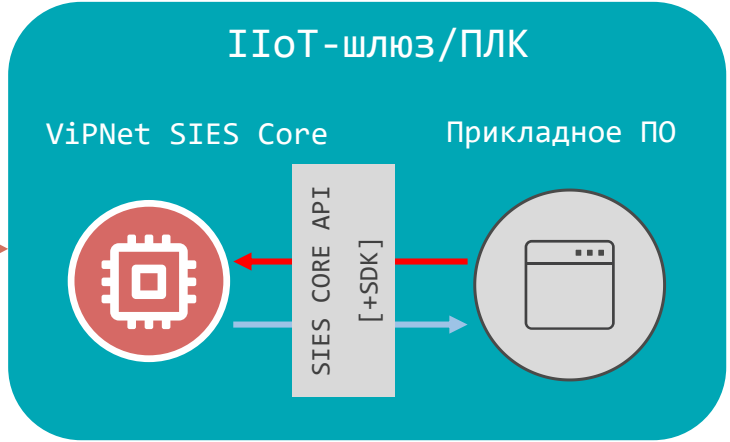
УПРАВЛЕНИЕ ОБНОВЛЕНИЕМ И КОНФИГУРАЦИЕЙ УСТРОЙСТВА



Встраивание ViPNet SIES Core



UART / USB / SPI



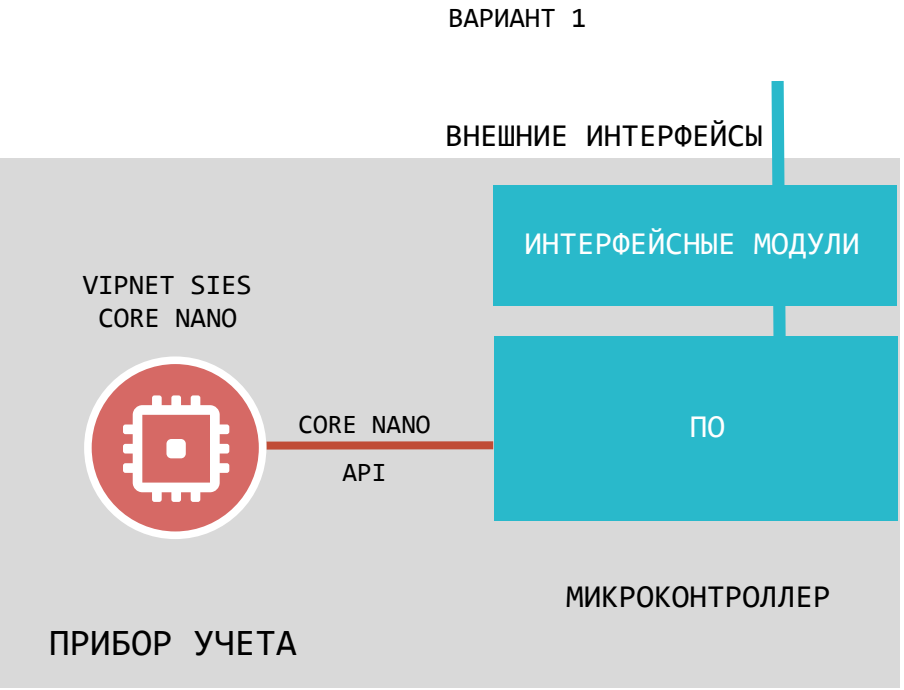
SIES Core SDK:

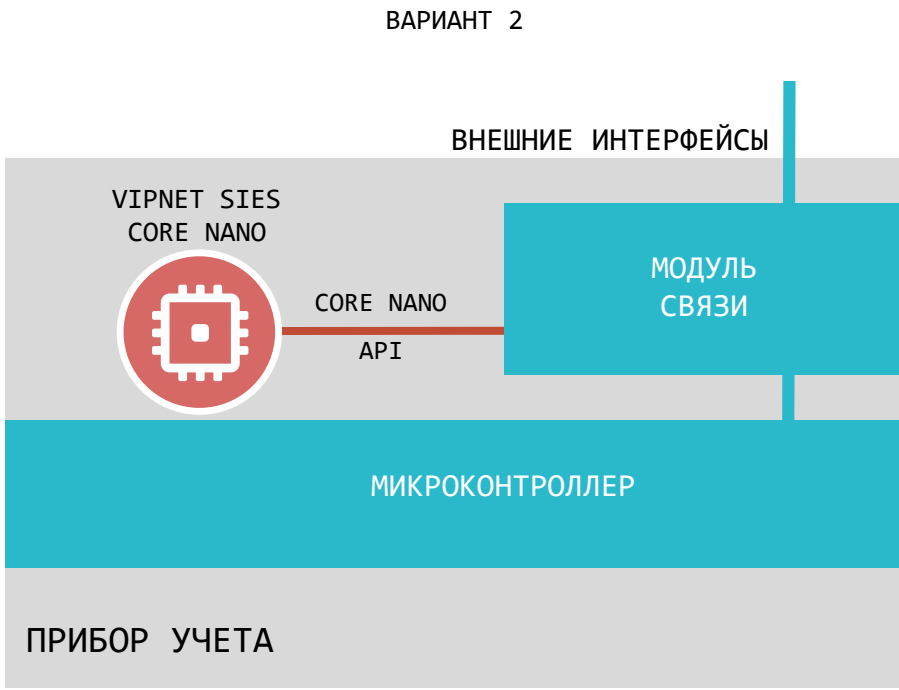
- x86-32/x86-64/ARM
- Windows
- Linux
- Baremetal (для устройств без ОС)

Защищенные данные

Незащищенные данные

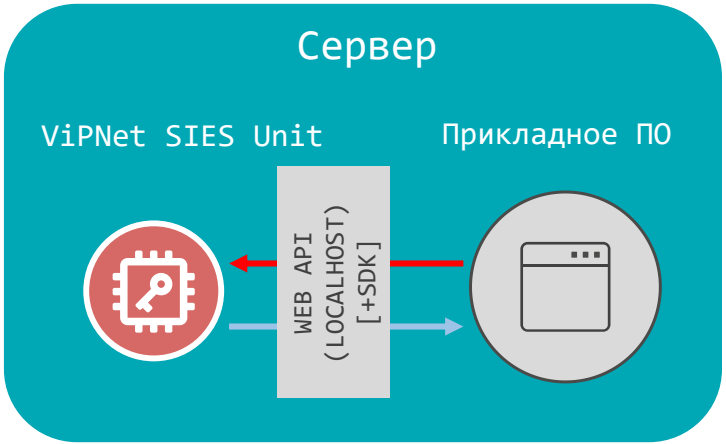
Встраивание ViPNet SIES Core Nano





Интеграция ViPNet SIES Unit

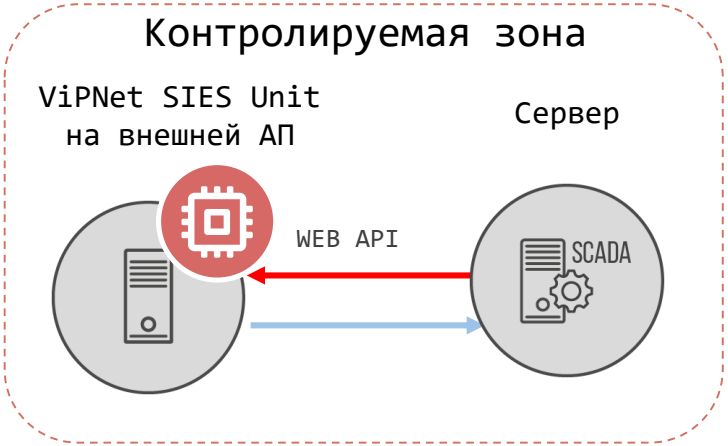
ВАРИАНТ 1



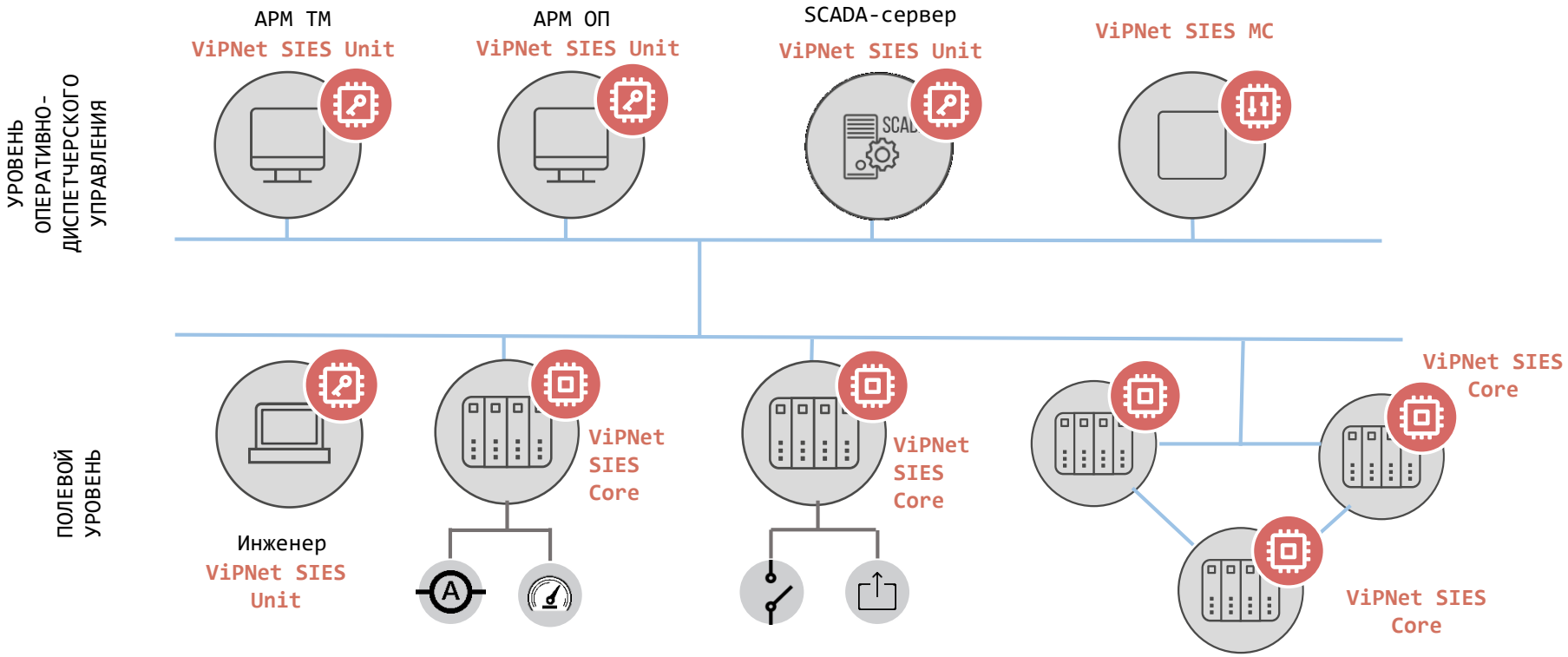
Защищенные данные

Незащищенные данные

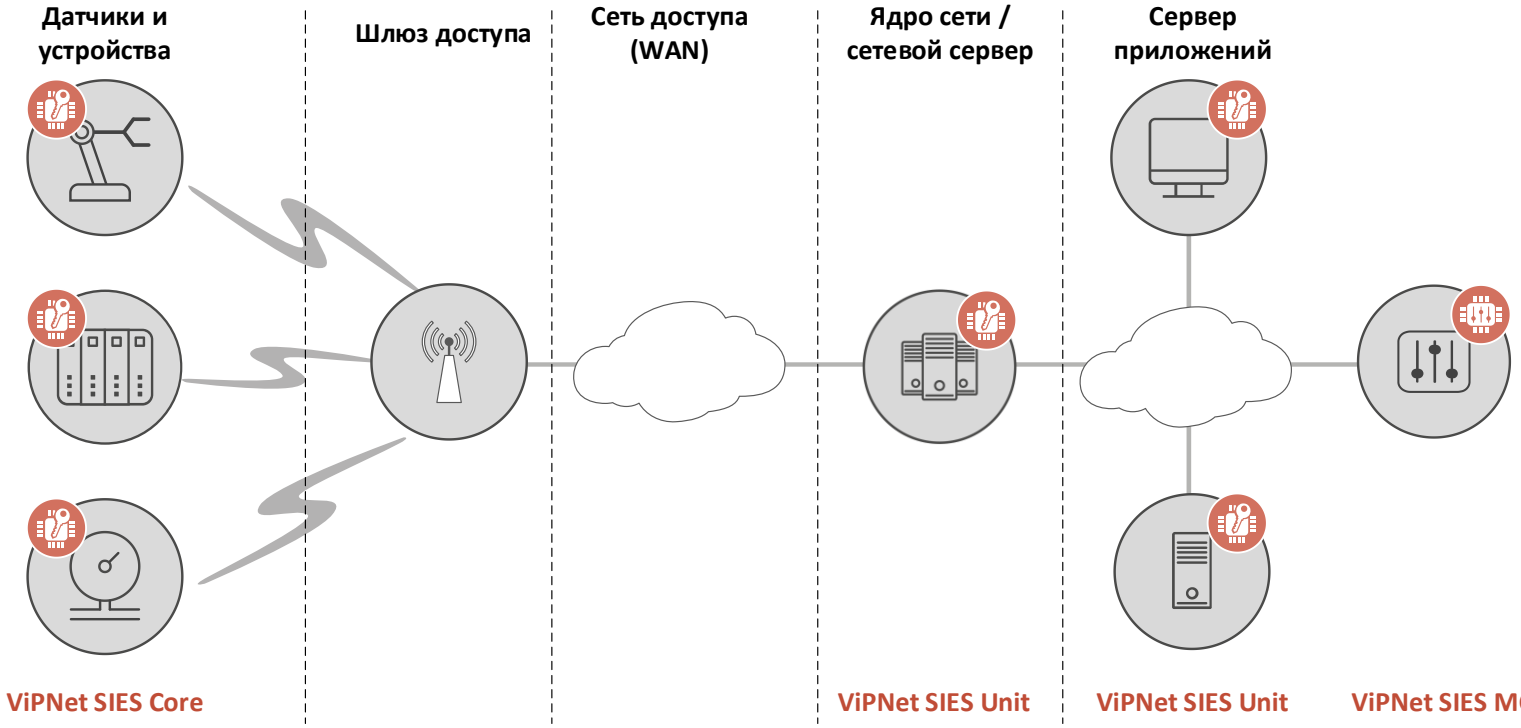
ВАРИАНТ 2



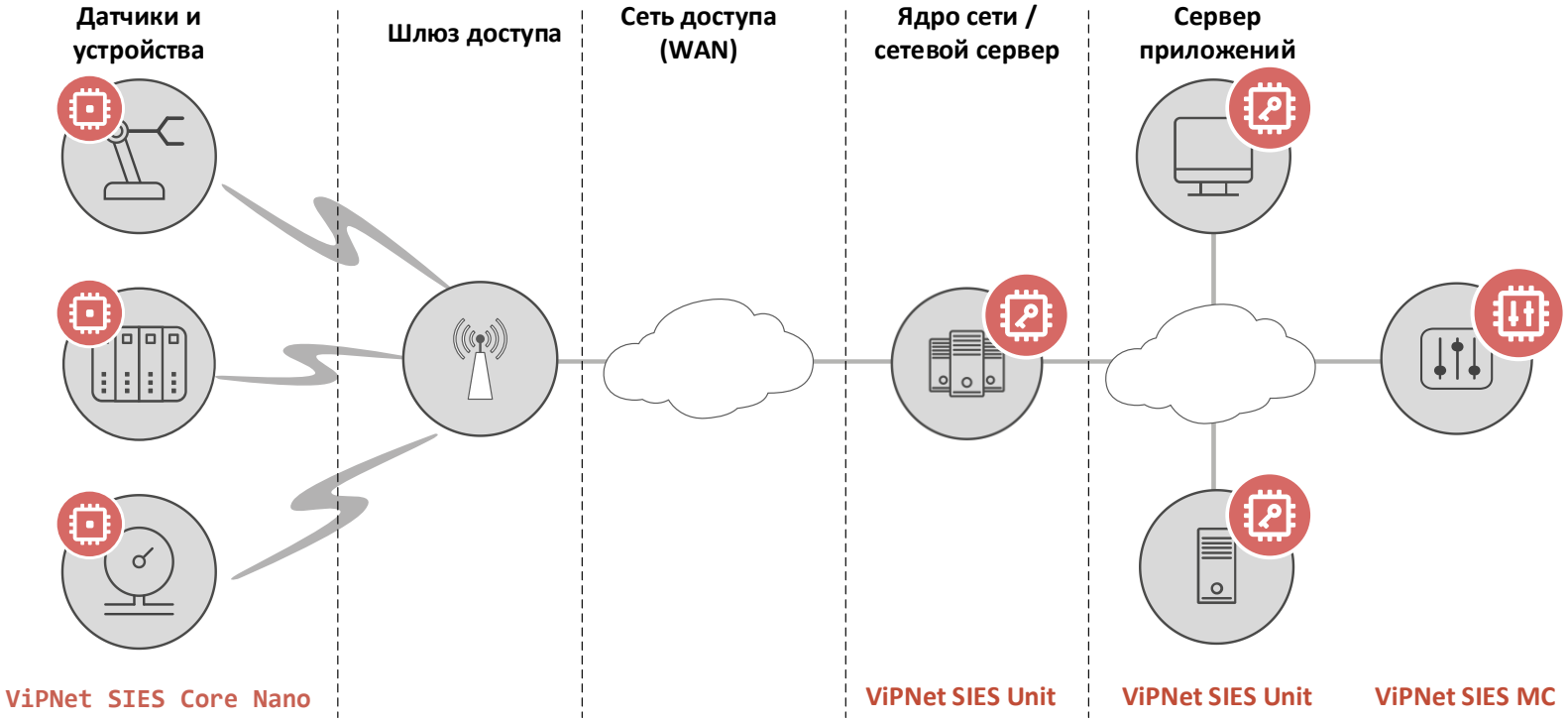
Типовая схема защиты АСУ ТП



Типовая схема защиты информации в IIoT-системе

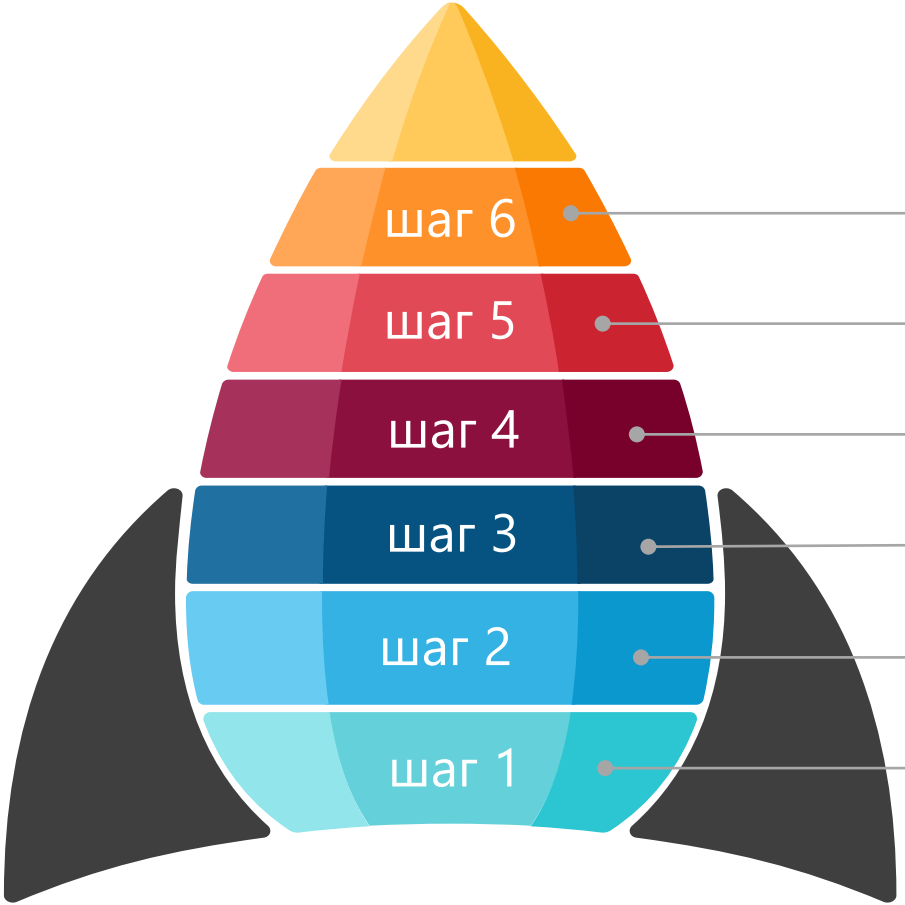


Типовая схема защиты информации в IIoT-системе



Порядок встраивания ViPNet SIES

Этапы встраивания СКЗИ



Производство

Работа с СКЗИ

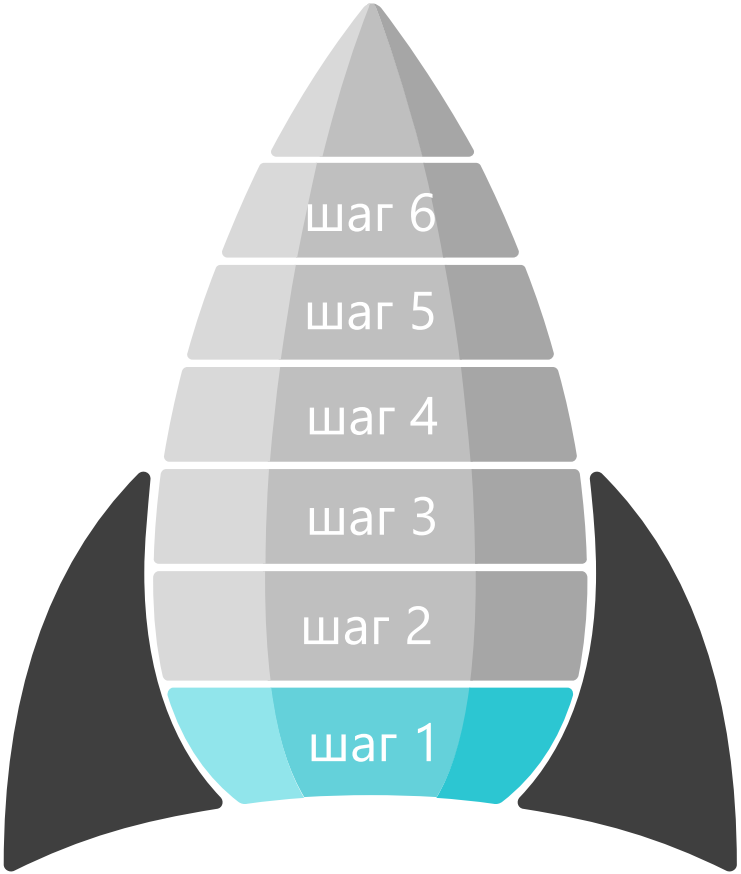
Оценка влияния

Проведение испытаний

Встраивание СКЗИ

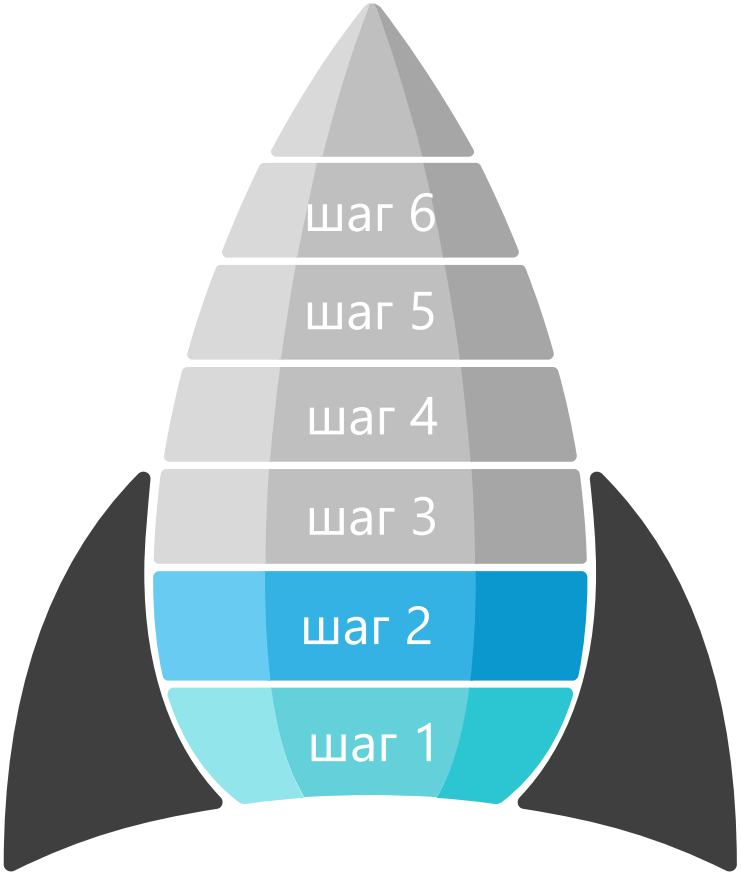
Подготовка к встраиванию СКЗИ

Подготовка к встраиванию СКЗИ



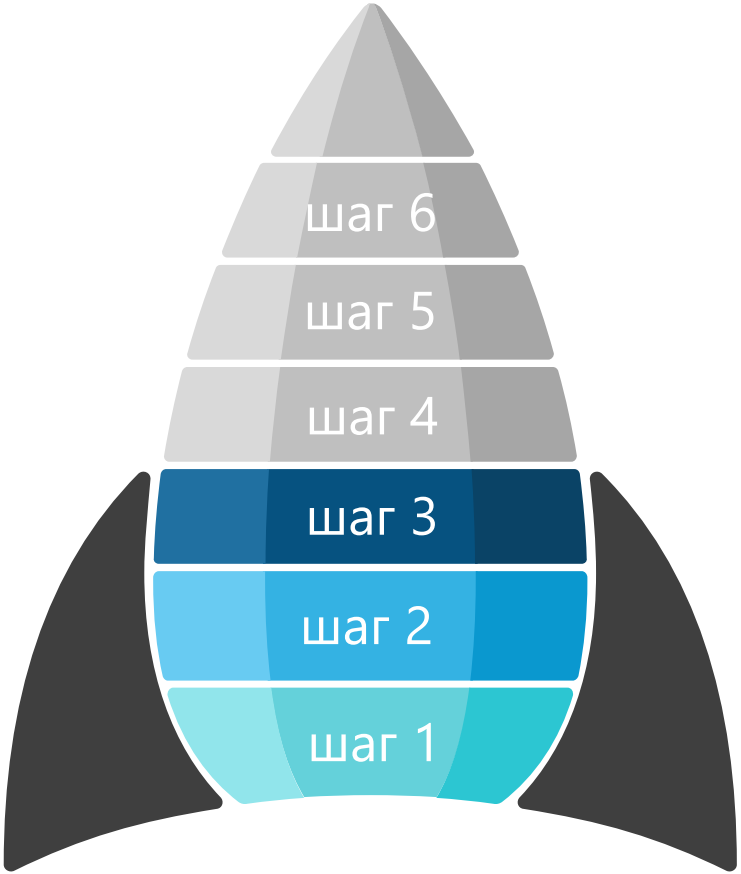
- Определение задач и мер обеспечения ИБ
- Ознакомление с документацией ViPNet SIES
- Разработка структурной схемы защиты с применением ViPNet SIES
- Выбор необходимых сценариев защиты информации
- Получение комплекта разработчика ViPNet SIES Development Kit и лицензий
- Подготовка инфраструктуры для развертывания ViPNet SIES Development Kit

Встраивание СКЗИ



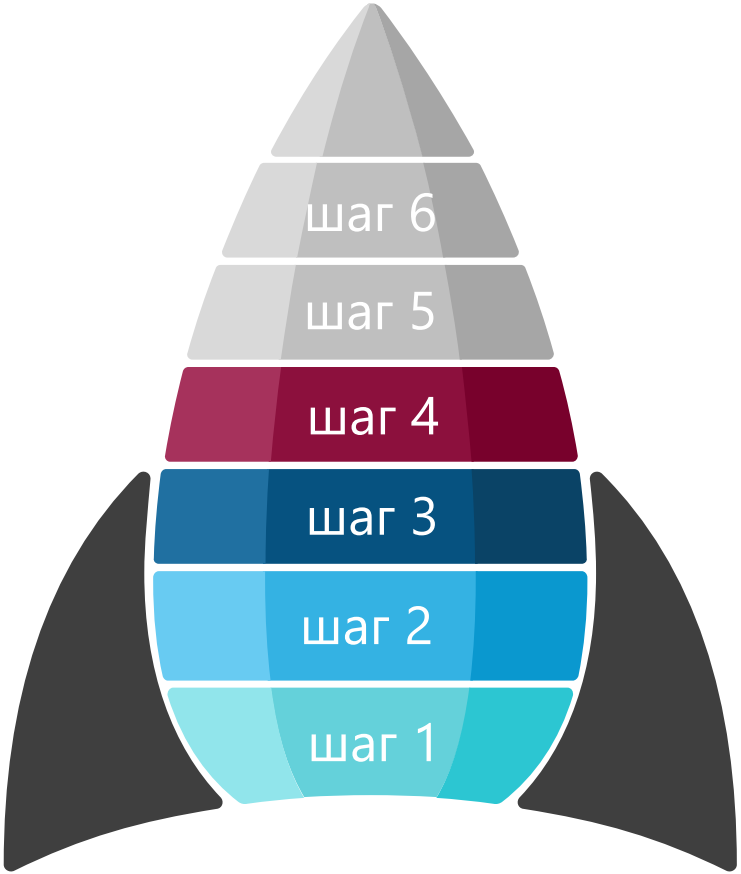
- Ознакомление с документацией и правилами пользования СКЗИ
- Проработка сценариев взаимодействия компонентов и определение необходимых сценариев ИБ
- Выбор способа защиты передачи данных
- Аппаратное встраивание (SIES Core) / программная интеграция (SIES Unit)
- Разработка (доработка) документации для соблюдения правил пользования СКЗИ

Проведение испытаний



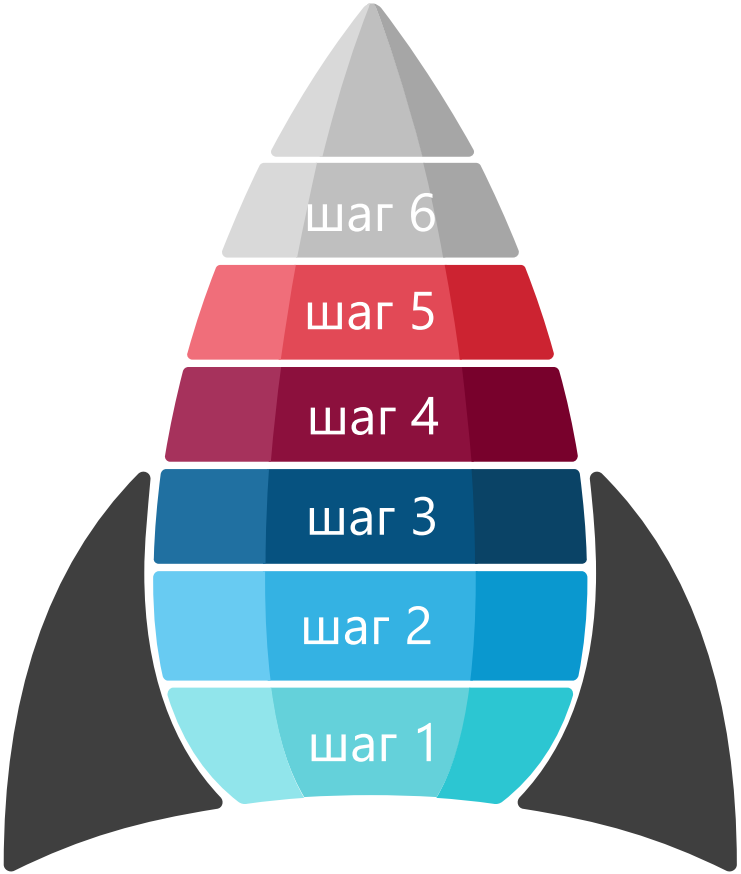
- Разработка программы и методики испытаний
- Разработка стенда для экспериментальных проверок
- Проведение испытаний, подготовка актов и протоколов испытаний

Оценка влияния



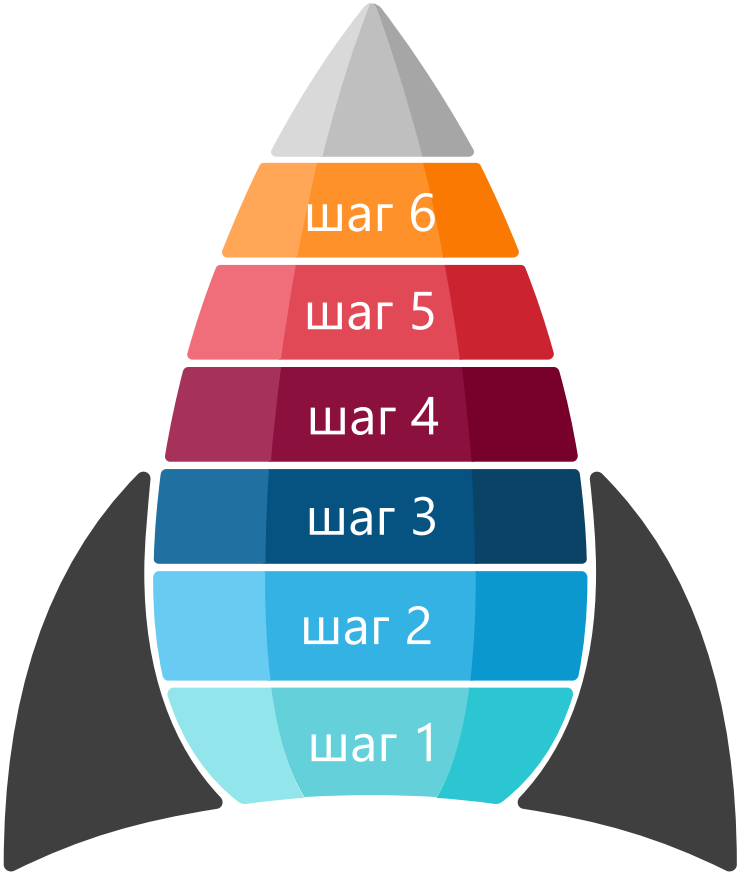
- Подготовка ТЗ на оценку влияния
- Согласование ТЗ на оценку влияния с испытательной лабораторией
- Согласование ТЗ на оценку влияния с ФСБ России
- Передача материалов и стенда в исследовательскую лабораторию для проведения работ по оценке влияния
- Направление исследовательской лабораторией результатов исследований на экспертизу в ФСБ России
- Получение результатов экспертизы в ФСБ России

Работа с СКЗИ



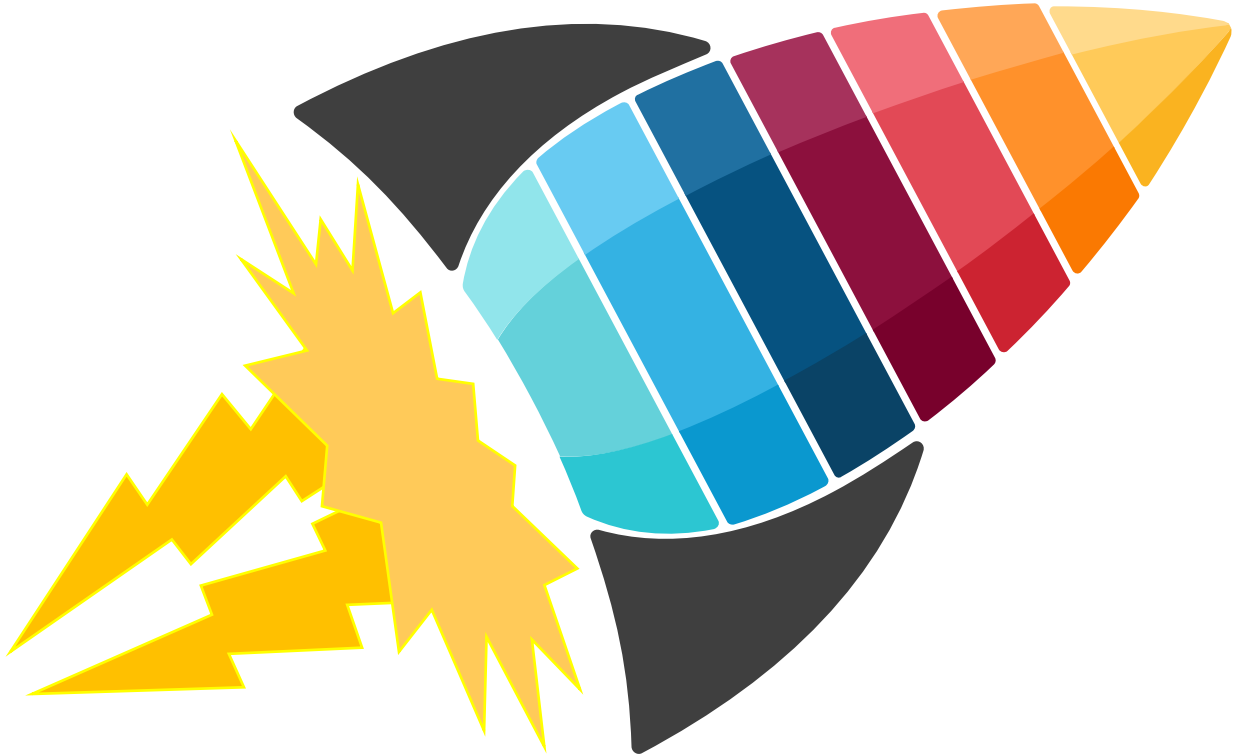
- Подготовка помещения для хранения СКЗИ и документации
- Ознакомление сотрудников с правилами работы с СКЗИ
- Подготовка помещения для инициализации СКЗИ (при необходимости)

Производство



- Учет и регистрация СКЗИ
- Инициализация СКЗИ в случае проведения данной операции при изготовлении
- Активация датчиков несанкционированного доступа SIES Core

Встраивание завершено



Итого

Преимущества решения ViPNet SIES с точки зрения производителей устройств автоматизации

1

Криптографические операции вынесены в отдельный модуль и доступны по простому API или протоколу – разработчику нет необходимости разбираться в криптографии

2

Используются сертифицированные СКЗИ высокого класса – сертификации устройств автоматизации не требуется, получение производителям лицензии на разработку, производство СКЗИ не требуется, достаточно оценки влияния

3

Криптографическими вычислениями занимается отдельный модуль, для устройств автоматизации среднего и нижнего уровня нет необходимости выполнения ресурсоемких операции

4

Ключевая информация хранится в отдельном СКЗИ, к устройствам автоматизации не предъявляются специальные требования

Спасибо за внимание!

Сергей Лыдин

e-mail: sergey.lydin@infotecs.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news