РУТОКЕН

Аутентификация и защита каналов передачи данных в умной инфраструктуре

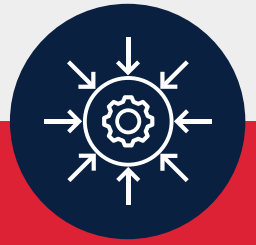
Алексей Лазарев

Руководитель департамента
защиты киберфизических систем,
Компания «Актив»

Проблематика

В IoT злоумышленник обладает большими возможностями физического доступа к целевому объекту атаки, нежели хозяин этого объекта

Новые возможности инфраструктуры порождают новые уязвимости и новые цели для атаки



Атаки могут быть неинвазивными. Атакующему не обязательно нарушать целостность системы

Базовая модель угроз безопасности информации ИСУЭ

Модель угроз содержит исходные данные по угрозам безопасности информации в ИСУЭ, связанным с:

1. Воздействием на метрологические характеристики компонентов ИСУЭ
2. Воздействием на компоненты ИСУЭ в целях управления подачей электрической энергии (мощности) потребителю
3. Воздействие на компоненты ИСУЭ в целях нарушения их функционирования в проектных режимах работы
4. Несанкционированным доступом к компонентам ИСУЭ с целью деструктивного воздействия на обрабатываемые в них персональные данные

Статические цели атак

- Данные, передаваемые по каналам связи
- Информация, хранящаяся на устройствах
- Съемные носители, внешние интерфейсы
- Настройки системы

Нужна аутентификация

Динамические цели атак

Загрузка операционной системы

Запуск процессов в операционной системе устройства

Регистрация нового устройства в системе

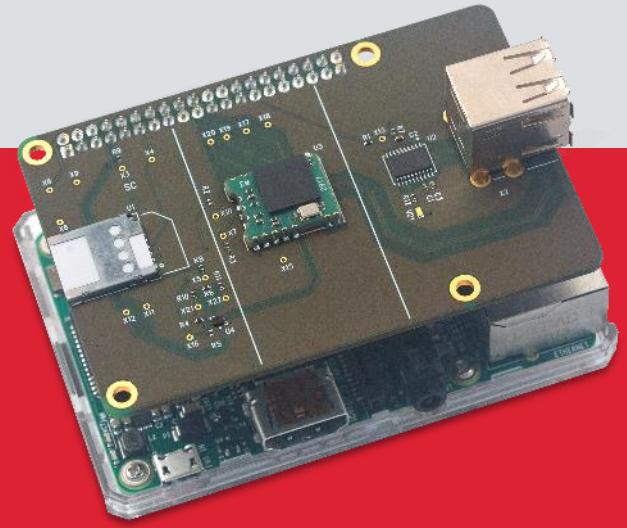
Обновление софтверных компонентов операционной системы

Аутентификация пользователей

Нужна строгая аутентификация

Рутокен Модуль

Набор интегрируемых программно-аппаратных средств защиты межмашинного взаимодействия (M2M), автоматизированных систем управления технологическими процессами (АСУ ТП) и интернета вещей (IoT).



1. Поддержка различных аппаратных интерфейсов взаимодействия
2. Широкий выбор форм-факторов для встраивания
3. Постоянно совершенствующийся SDK

Надежное хранение ключевой информации

Хеширование

- ГОСТ Р 34.11-2012/2018

Электронная подпись

- ГОСТ Р 34.10-2012/2018

Шифрование, имитовставка

- ГОСТ Р 34.12-2015/2018, ГОСТ Р 34.13-2015/2018 (Кузнечик, Магма)

CRISP (ГОСТ Р 71252–2024)

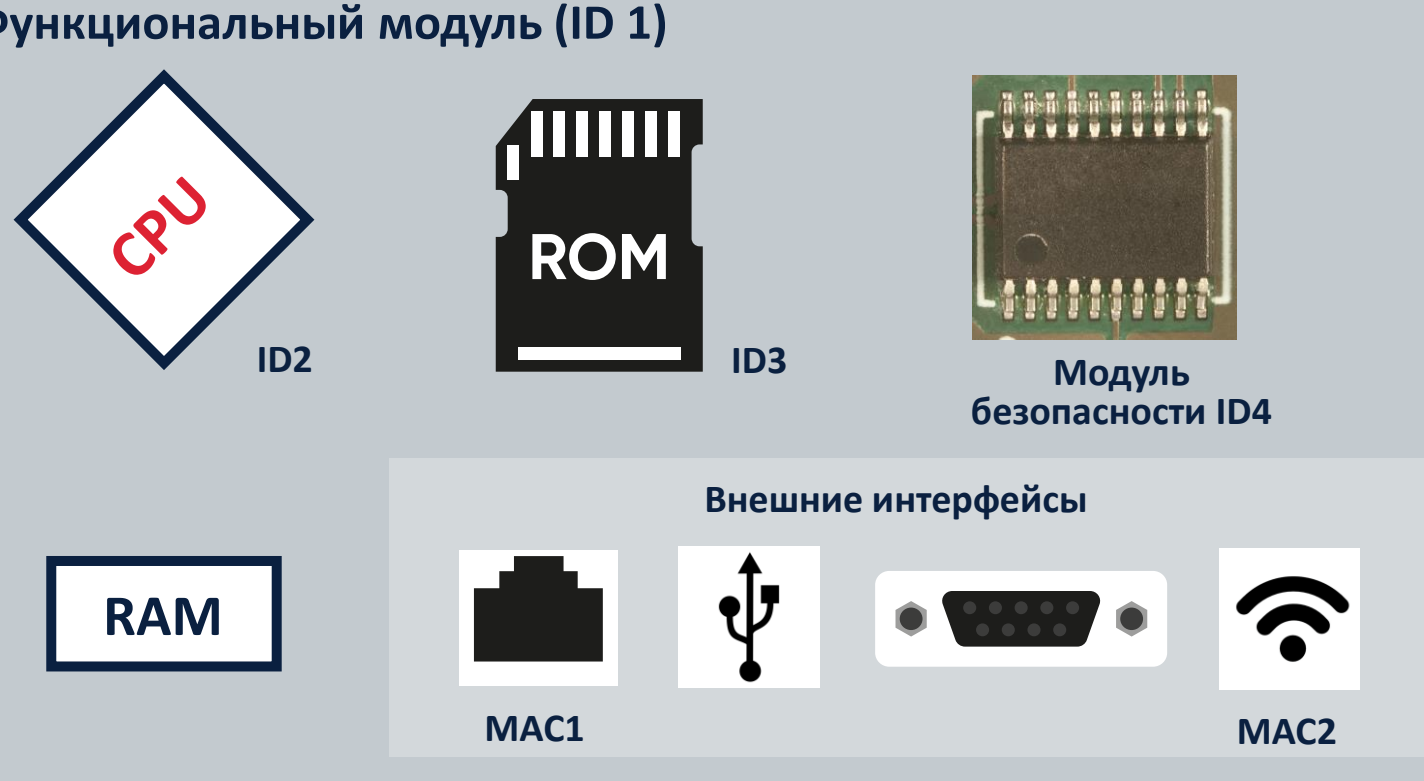
Архитектура защищенного устройства

Функциональный модуль

- Коммуникация
- Обработка данных
- Хранение данных

Модуль безопасности (крипто-модуль)

- Хранение учетных данных
- Генерация и хранение секретов
- Криптографические операции



Identity, Integrity, Incessancy

CRISP

Рутокен Модуль + CRISP

1. Контроль аппаратной целостности устройства
2. Защита обмена информацией от подмены и атак повторения (ЭЦП)
3. Контроль аутентичности передаваемых данных (ЭП)
4. Защита конфиденциальности данных. Шифрование
5. Контроль запуска устройства
6. Аутентификация пользователя
7. Аутентификация процессов и подпроцессов, запускаемых на устройстве
8. Доверенное обновление софта и компонентов операционной системы (ЭЦП)

Аутентификация пользователей и процессов

#1 В M2M пользователем — может быть не физическое лицо, а процесс

#2 В контексте операционной системы нет отличий между живым пользователем и процессом

#3 Аутентификация таких «пользователей», а по сути, процессов — необходимый шаг

Guardant – защита, лицензирование и монетизация

Используется 3 000 вендоров ПО по всему миру

- Защита ПО от реверс-инжиниринга, копирования и модификации
- Лицензирование и контроль использования, распространения
- Защита и шифрование данных
- Система учета продаж, лицензий, обновлений
- Возможность исполнять код внутри ключа

Рутокен Криптомост

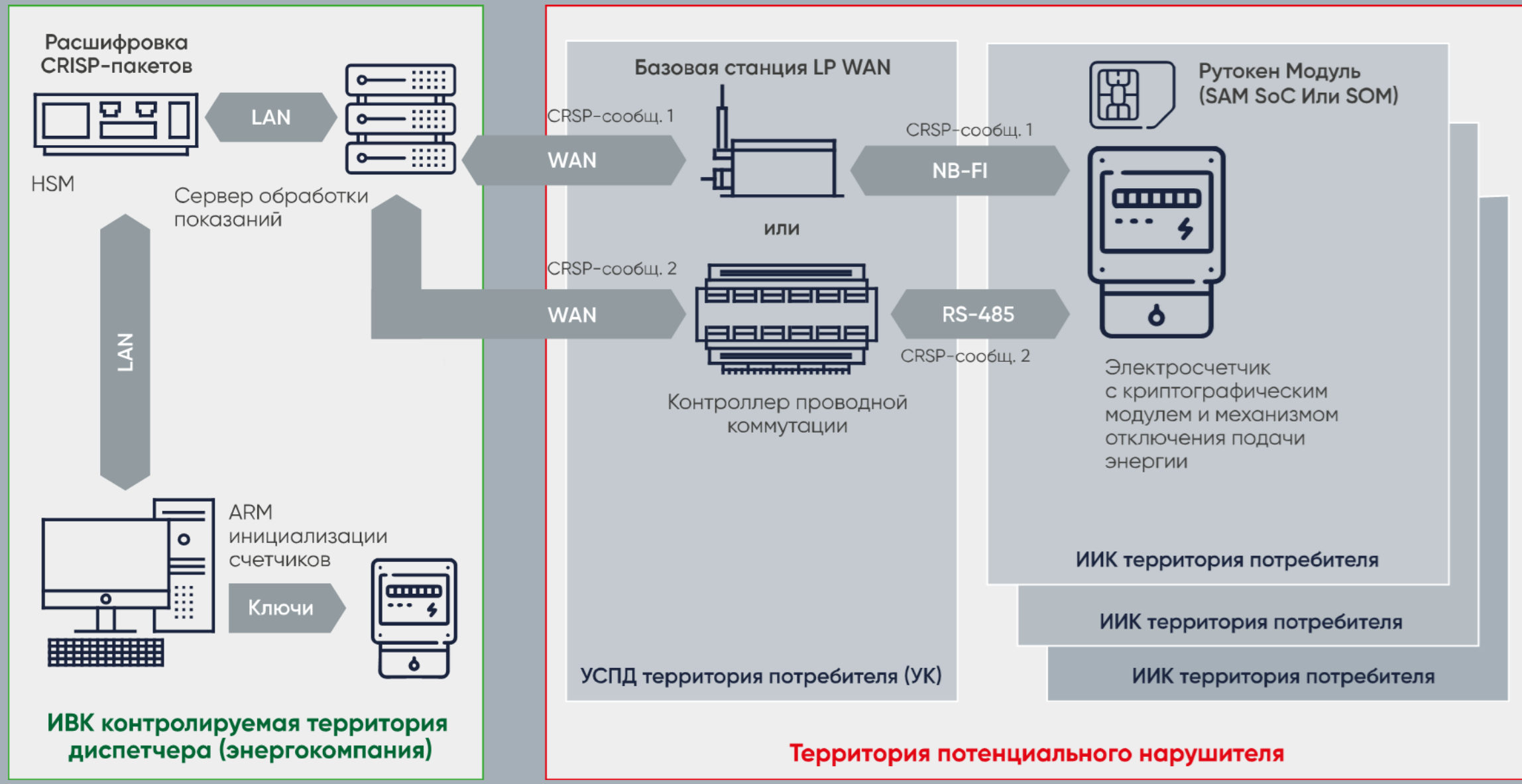
Защита IP-каналов

1. Обеспечивает безопасный высокоскоростной VPN-канал связи между удаленной камерой и системой видеонаблюдения

2. Использует отечественные криптографические стандарты

3. Позволяет выполнить требования российских регуляторов

Пример защищенной SCADA-системы



Контактная информация

Алексей Лазарев

Руководитель департамента
защиты киберфизических систем,
Компания «Актив»

al@rutoken.ru
hotline@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90
+7 905 729-34-26

РУТОКЕН