



# Технологическая основа доверия. Необходимость применения аппаратных элементов для эффективной защиты массовой инфраструктуры

## Алексей Лазарев

Руководитель департамента  
защиты киберфизических систем,  
Компания «Актив»

## Сергей Панасенко

Директор по научной работе,  
Компания «Актив»



# Основа **доверия**



Основанием для доверия к объекту могут быть результаты проведения оценки соответствия.



**Иерархия доверия** - способ установления доверия к системе посредством организации иерархии элементов этой системы, в которой сервисы безопасности элементов, доверие к которым уже установлено, используются для свидетельствования и (или) обеспечения свойств безопасности элементов следующих уровней иерархии необходимых для установлении доверия к последним.



**Цепочка доверия** - частный случай иерархии доверия, в которой на каждом уровне находится один элемент

# Корень доверия и ДКБ. В чем разница?

**Корень доверия** — логический элемент, определяющий набор сервисов, необходимых для проверки свойств целостности и аутентичности других элементов системы.

- Неотъемлемая часть и основа цепочки доверия
- Распространяет доверие на другие части цепочки доверия

**Доверенный компонент безопасности** — неотъемлемый компонент доверенной аппаратно-программной платформы (АПП), представляющий элементарные сервисы корня доверия.

ДКБ может быть аппаратным, программно-аппаратным и чисто программным. Доверие достигается в процессе оценки соответствия, например, в рамках сертификации. Это предоставляет определенную степень уверенности в том, что функции корня доверия реализованы в рамках налагаемых на них требований.

# Значимые характеристики ДКБ



## Функциональная безопасность



Отсутствие негативного влияния на сопряженные компоненты



Переход в безопасное состояние во время непреднамеренного сбоя

## Информационная безопасность



Неизвлекаемость секретов



Невозможность воздействия на выполняемые операции извне



Изоляция реализации функций ДКБ от основной системы



Защищенность модуля от НСД

## Устойчивость



Способность сохранять функциональность и восстанавливать работоспособность



Избыточность



Резервирование

## Надежность



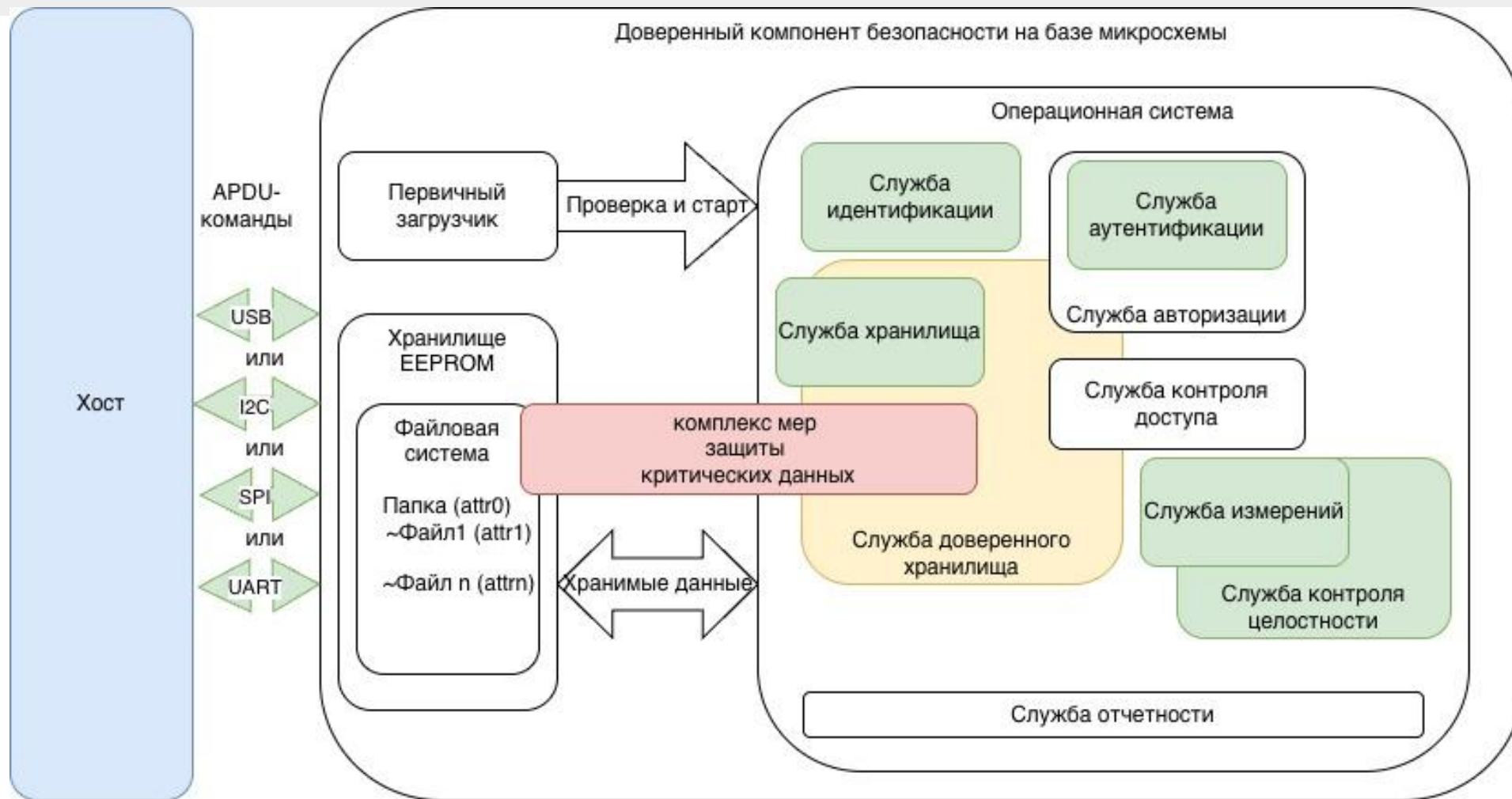
Способность выполнять функции за установленное время



Защита от непреднамеренных сбоев

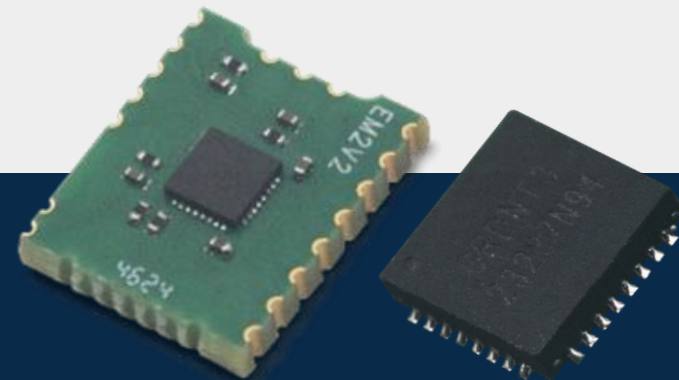
Реализация криптографических преобразований, критичных для безопасности устройств/систем

# Службы корня доверия, реализованные в ДКБ



# Сценарии применения

**Интегрируемый доверенный компонент безопасности, используемый в реализации сценариев защиты**



## В средствах вычислительной техники

- Функциональность TPM
- Электронная подпись документов
- Проверка электронной подписи
- Аутентификация пользователей
- Защищенный сетевой обмен (TLS, VPN)
- Шифрование данных на носителях

## В киберфизических системах

- Защита от атак повтора пакета
- Контроль целостности и аутентичности данных на носителях и данных, передаваемых по каналам связи
- Обеспечение конфиденциальности данных
- Контроль аппаратной целостности устройства

## Общие сценарии

- Контроль целостности ПО
- Доверенное обновление ПО
- Аутентификация запускаемых процессов
- Аттестация АПП
- Организация цепочки доверия для загрузки и исполнения программного кода
- Сценарии защиты на неподменяемых корневых сертификатах
- Генерация случайных последовательностей

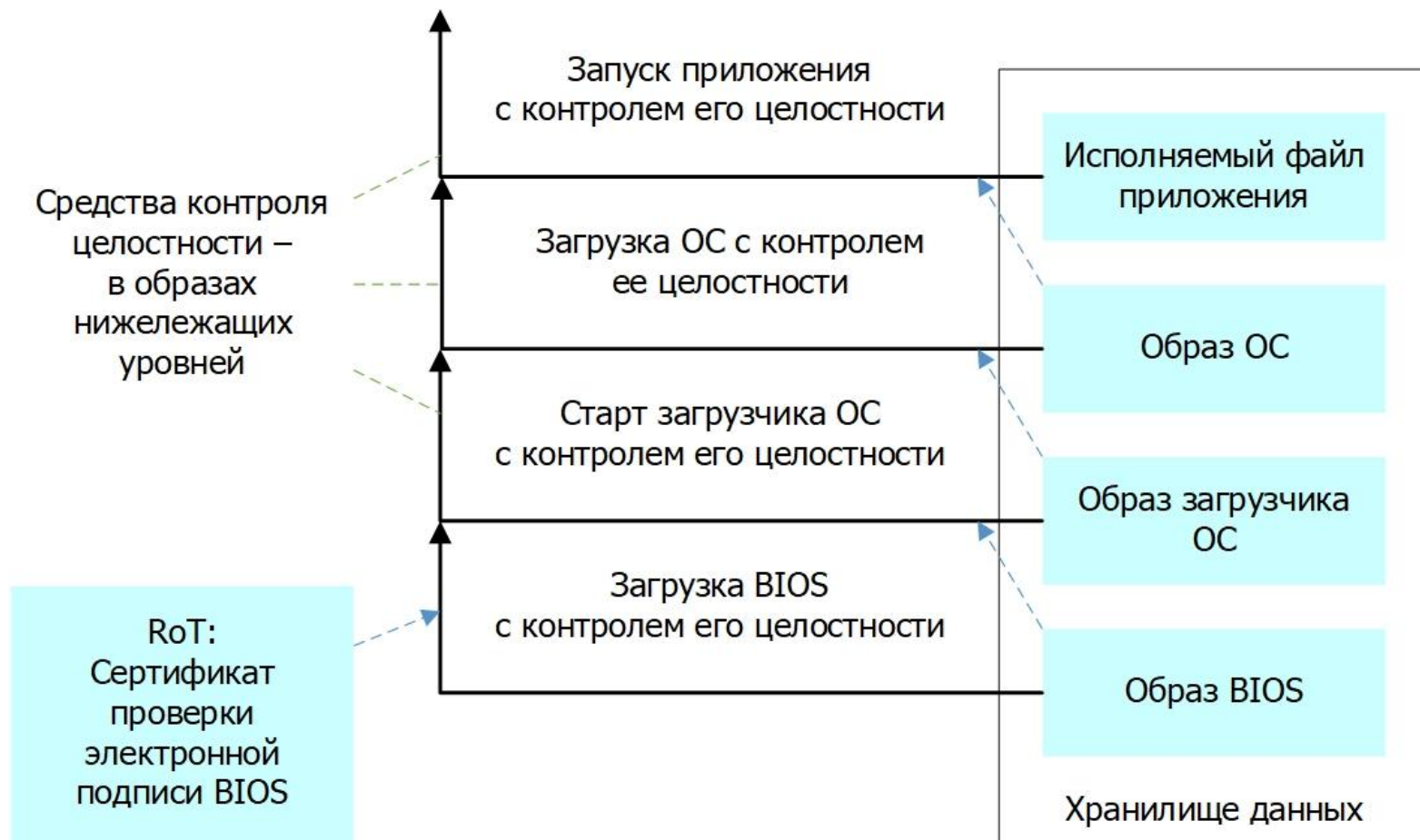
# Примеры использования: доверенная загрузка



Цепочка доверенной загрузки программных компонентов с поочередным контролем целостности на всех этапах.

На нижнем уровне контроль выполняется средствами RoT.

Предотвращение загрузки недоверенных программных компонентов.





# Примеры использования: строгая взаимная аутентификация

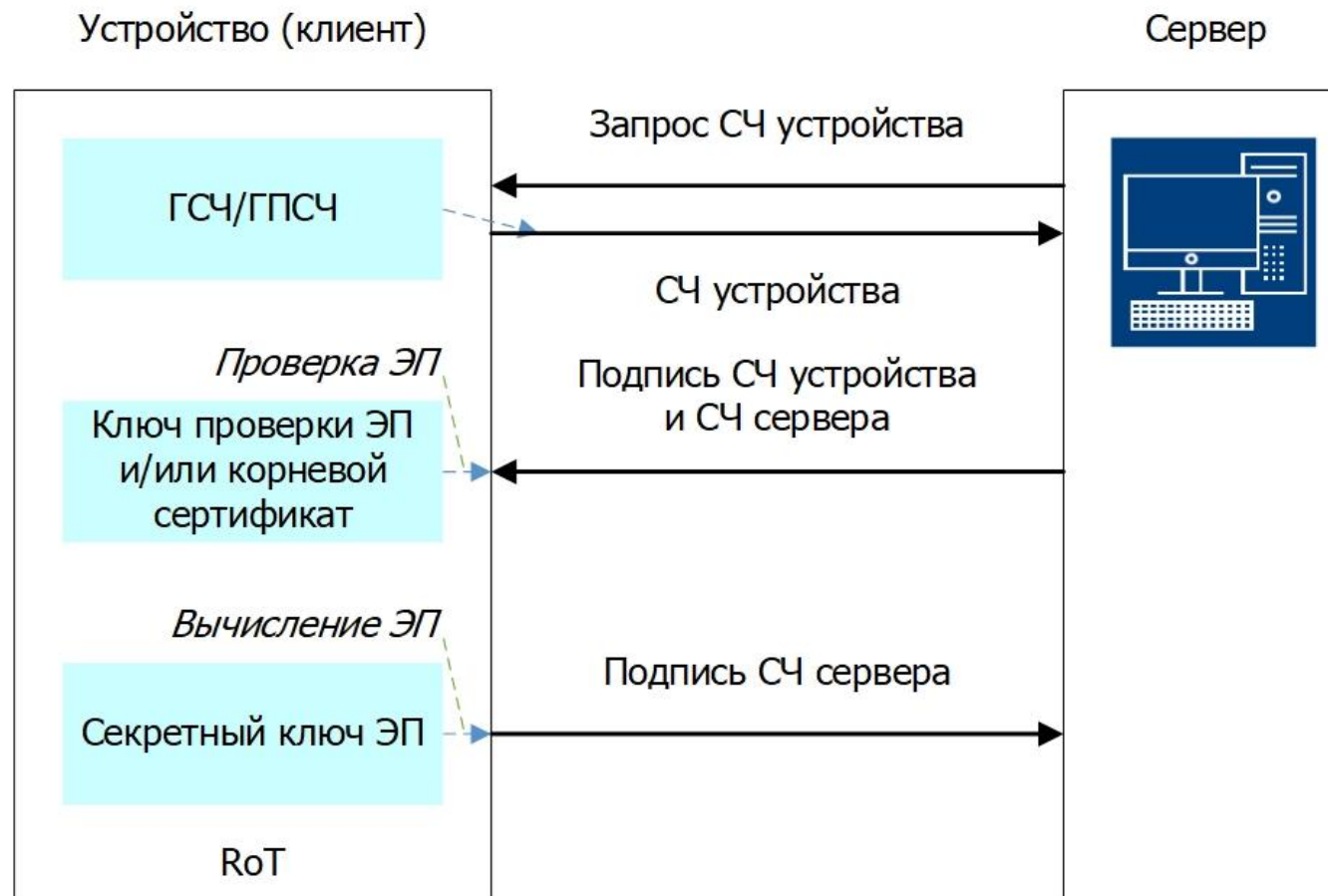


Взаимная аутентификация устройства и сервера на основе электронной подписи.

Может сопровождаться вычислением общего симметричного ключа для защиты канала связи.

## Пример применения:

- клиент – сенсор IoT;
- сервер – пограничный узел.

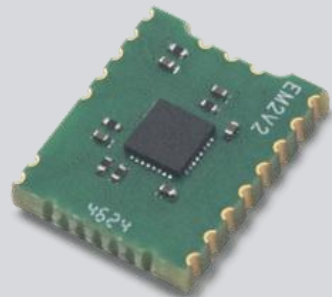




# Форм-факторы и возможности



Встраиваемый модуль



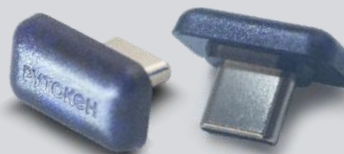
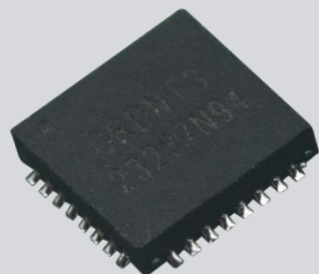
USB-устройства



SAM-модуль



Встраиваемый чип



## 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)

# Способы интеграции

Поддержка стандартов ISO/IEC 7816, PKCS#7, PKCS#11

## В уже разработанных системах

USB-устройство

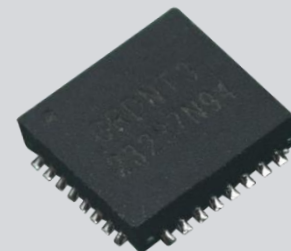


SAM-модуль

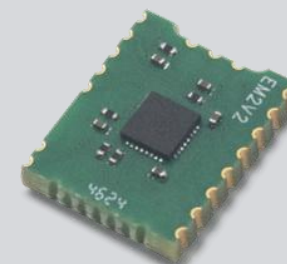


## Во вновь создаваемых системах

Микросхема



Многоинтерфейсный  
интегрируемый модуль



## Прикладное ПО, плагины для браузеров

## Библиотека прикладного уровня PKCS#7 (CMS), PKCS#11

Поддержка CCID на уровне операционной системы

Кроссплатформенный драйвер уровня CCID

## Работа на аппаратном уровне (APDU, ISO/IEC 7816 ч.4)

USB-драйвер операционной системы

Интерфейсы USB, SPI, I2C, UART

# Пример защищенной системы **СКУД** >>>



OSDP  
(CRISP)



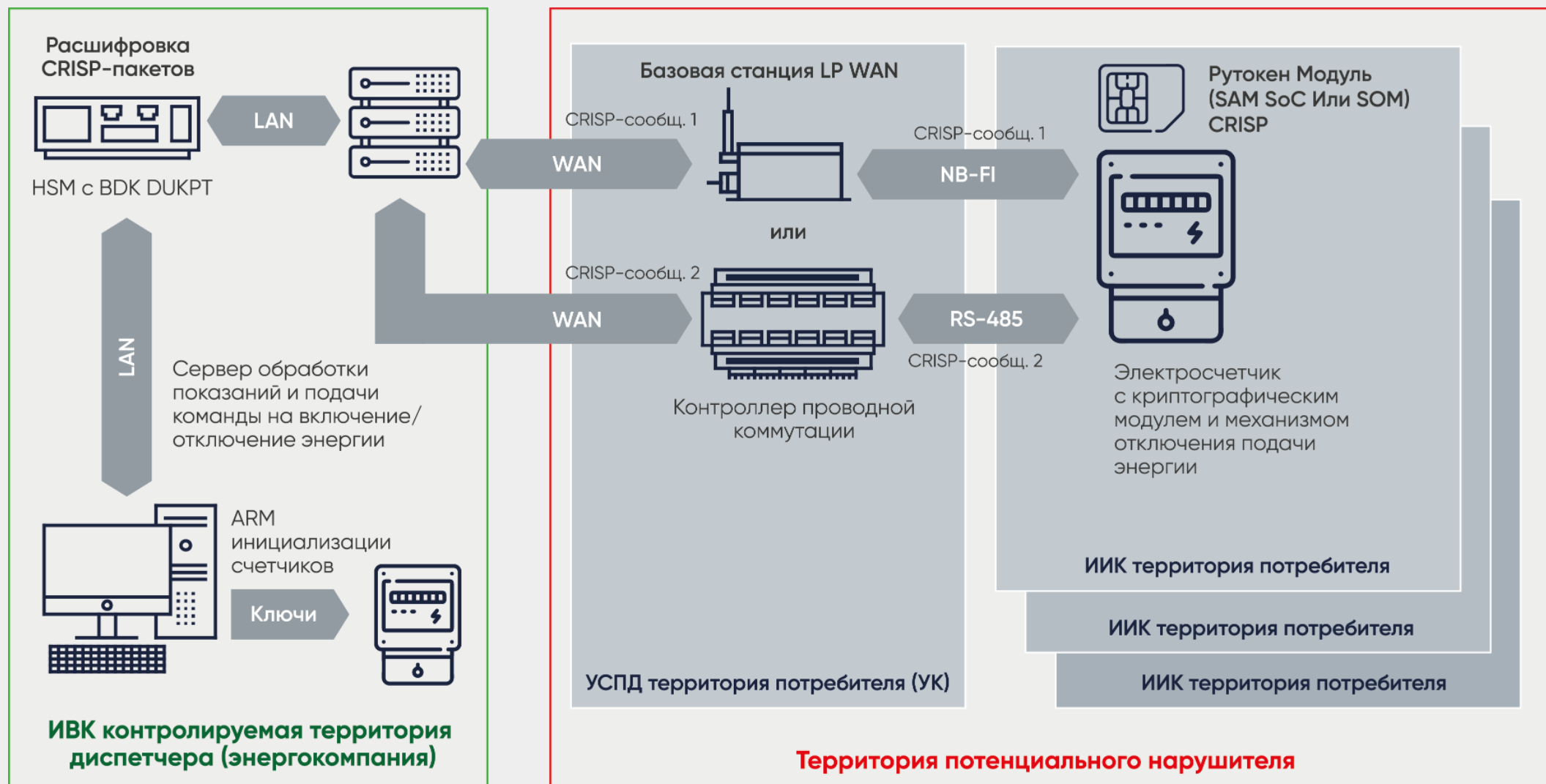
ISO 14443  
(Challenge-response)



IP-Канал  
(VPN)



# Пример защищенной SCADA-системы



# Защита IP-каналов

## Рутокен криптомост



Обеспечивает **закрытый высокоскоростной VPN-канал связи** между удаленным устройством и центральным сервером



**Не требует глобальной переделки** существующей системы



Позволяет выполнить требования **российских регуляторов**

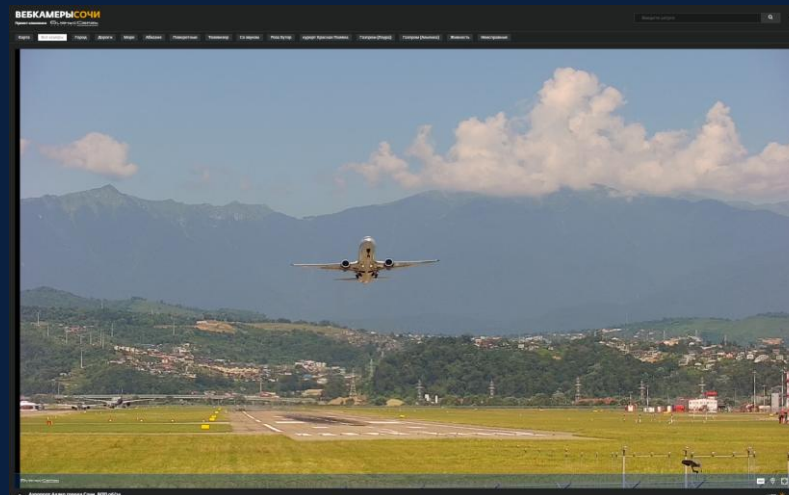
# Уязвимости систем видеонаблюдения

Перехват и подмена видеопотока

## OSINT!

Перехват управления фокусом и углами обзора

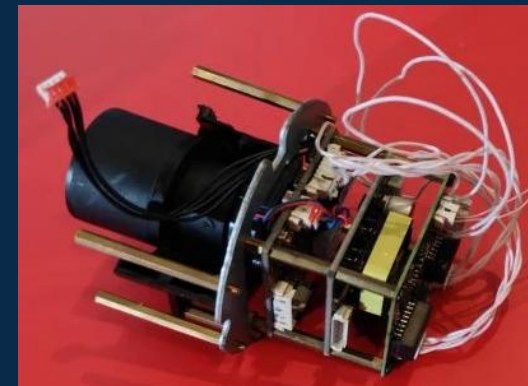
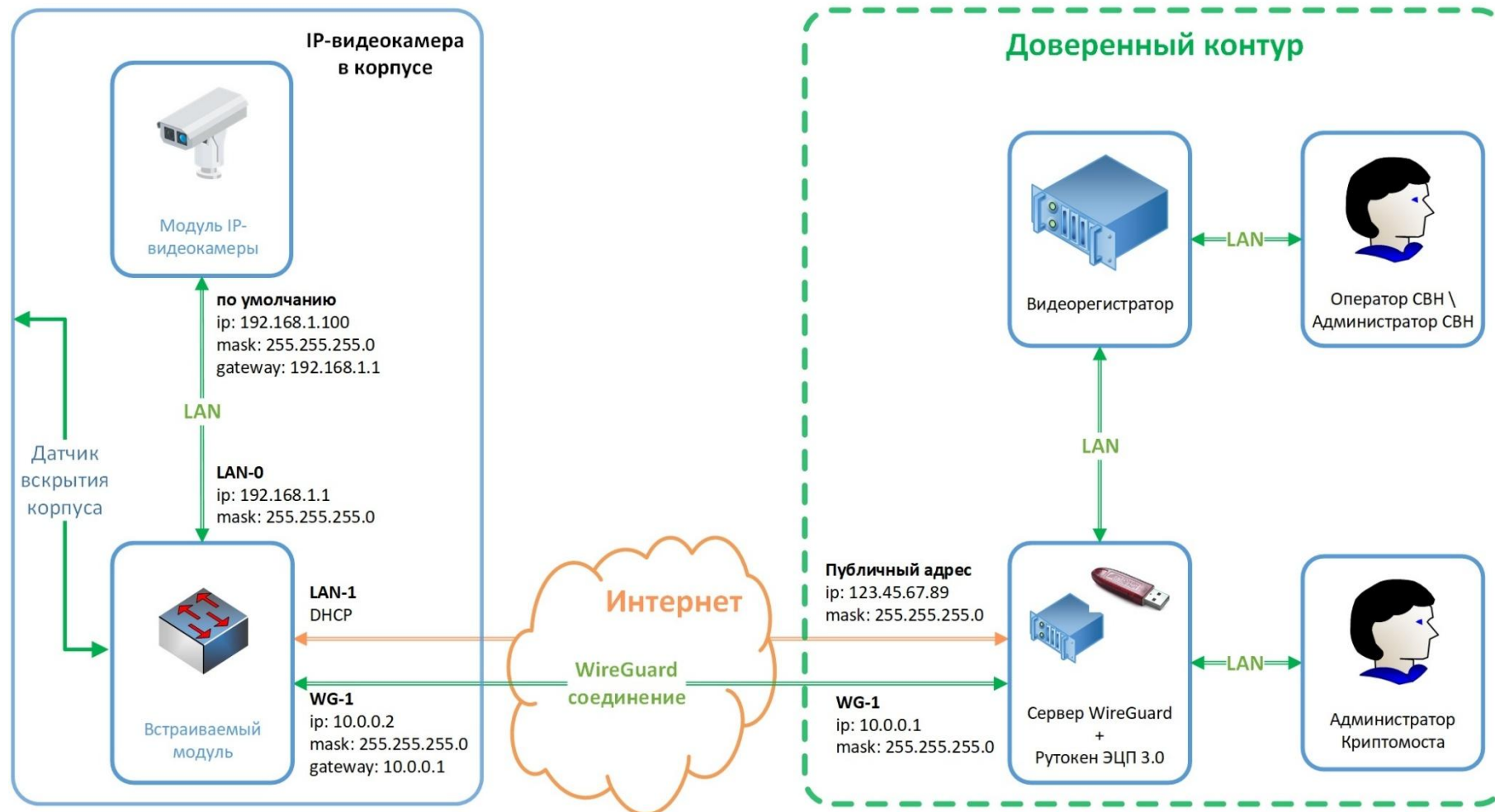
Несанкционированный сбор ПД по отслеживаемым лицам





# Решение для защиты СВН

Схема эксплуатации на объекте





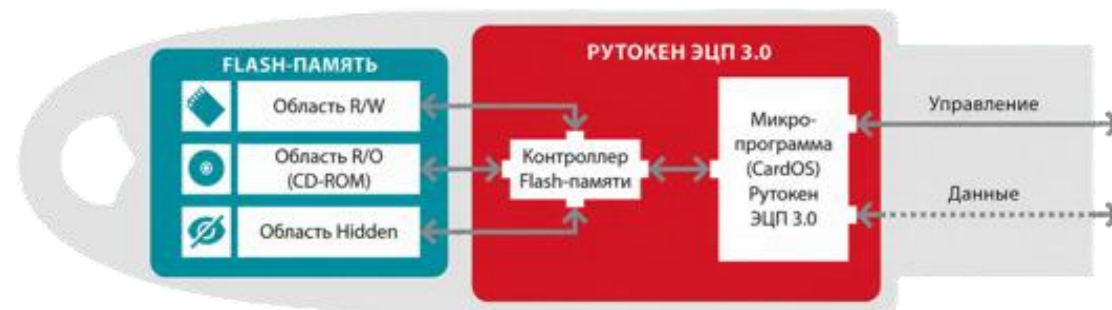
# Решение для защиты данных на СМН



**Рутокен ЭЦП 3.0 5100 Flash** - объединение возможностей криптографического токена Рутокен ЭЦП 3.0 и flash-накопителя

- безопасное удаленное рабочее место
- защищенное хранение информации ограниченного доступа

- работа на авторизованном компьютере
- аудит действий пользователей и администраторов



Выход на рынок

2Q 2026