КОМПАНИЯ АКТИВ

Аппаратный корень доверия для обеспечения защиты данных: варианты реализации

Сергей Панасенко
Директор по научной работе,
Компания «Актив»

Алексей Лазарев
Руководитель департамента
защиты киберфизических систем,
Компания «Актив»

Компания «Актив»

guardant

Комплексная система для защиты, лицензирования и управления продажами ПО

РУТОКЕН

Аппаратные и программные решения в области аутентификации, защиты информации и электронной подписи

AKTIV. CONSULTING

Консалтинг и аудит в области ИБ

Что такое аппаратный корень доверия?

Аппаратный корень доверия (Hardware Root of Trust, далее — RoT) — это аппаратный модуль, на котором основывается обеспечение безопасности функционирования устройства или вычислительной системы.

Для выполнения предусмотренных функций RoT содержит:

- основные/корневые секретные криптографические ключи
- реализации криптографических преобразований, критичных для безопасности устройств/систем

Что такое аппаратный корень доверия?

Для качественного обеспечения безопасности RoT должен обладать основными свойствами:

#1 Высокий уровень надежности

#2 Защищенность модуля от НСД, его соответствие высоким уровням требований по обеспечению безопасности

#3 Неизвлекаемость криптографических ключей

#4 Обеспечение невозможности воздействия на выполняемые операции извне

Концепция
и сферы применения

Сферы применения:

- Банки
- Телеком
- АСУ (включая АСУ ТП) и их компоненты
- IoT

Основное содержимое RoT

Примеры хранимых криптографических ключей:

- Корневые сертификаты
- Неизвлекаемые секретные ключи для электронной подписи и обмена ключами
- Секретные ключи симметричного шифрования
- Мастер-ключи для диверсификации ключей или генерации псевдослучайных чисел
- Ключи для аутентификации

Основное содержимое RoT

Примеры реализуемых криптографических функций:

#1 Вычисление электронной подписи на неизвлекаемом ключе

#2 Проверка электронной подписи / цепочки сертификатов

#3 Вычисление общего ключа на неизвлекаемом ключе

#4 Симметричное шифрование данных

#5 Диверсификация ключей

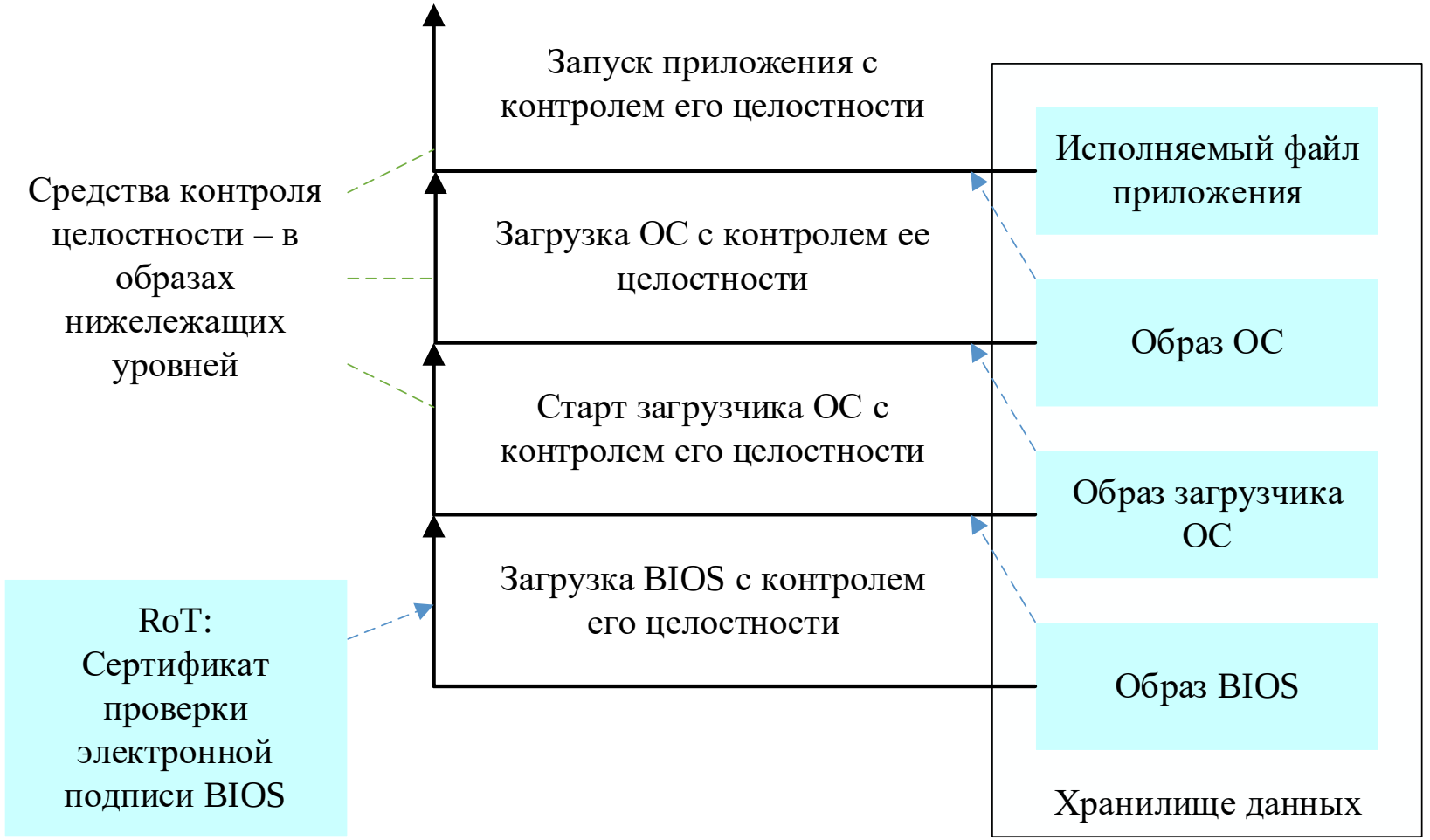
#6 Генерация псевдослучайных чисел

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.



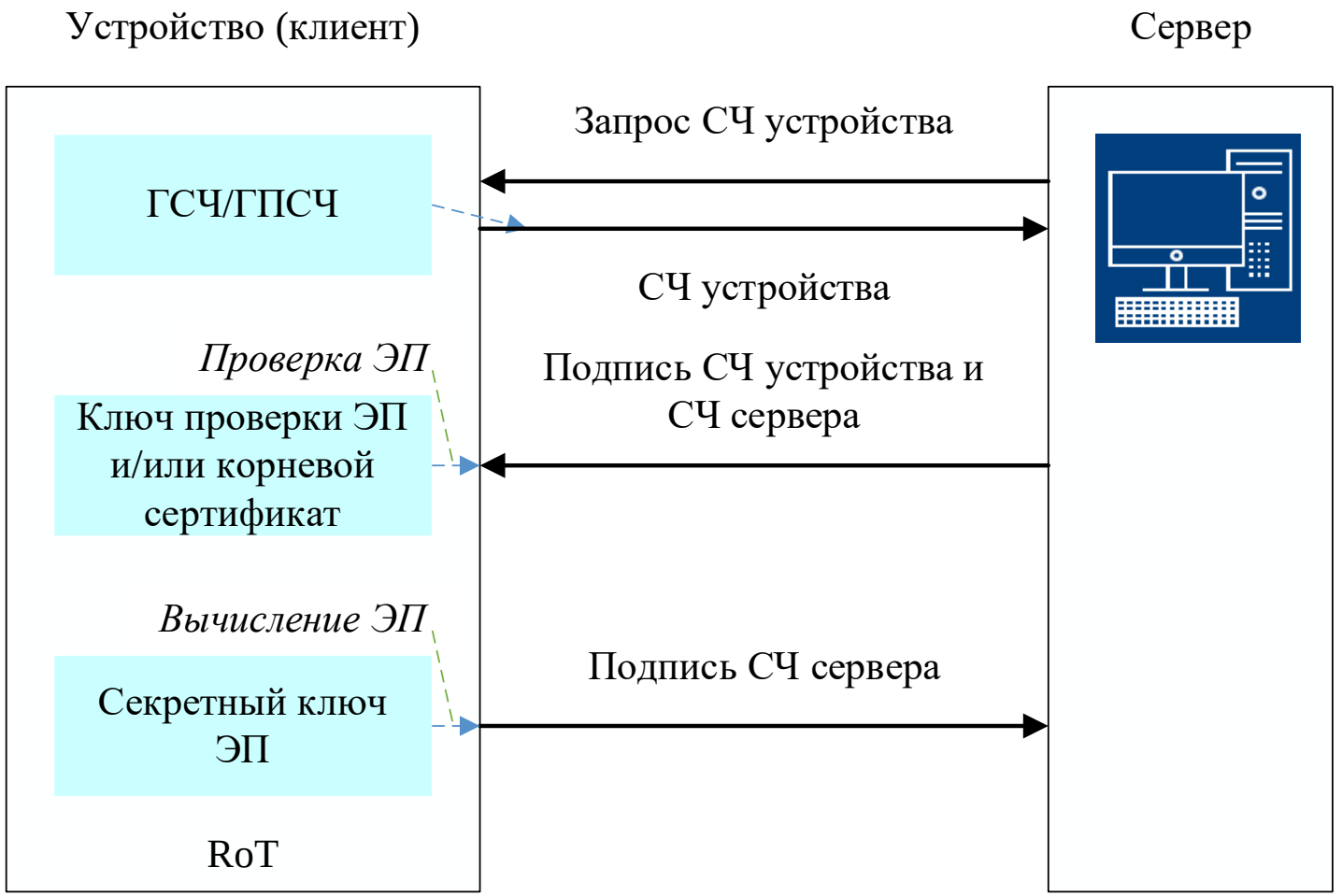
Примеры использования:
строгая взаимная аутентификация

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.



РУТОКЕН
КОМПАНИЯ АКТИВ

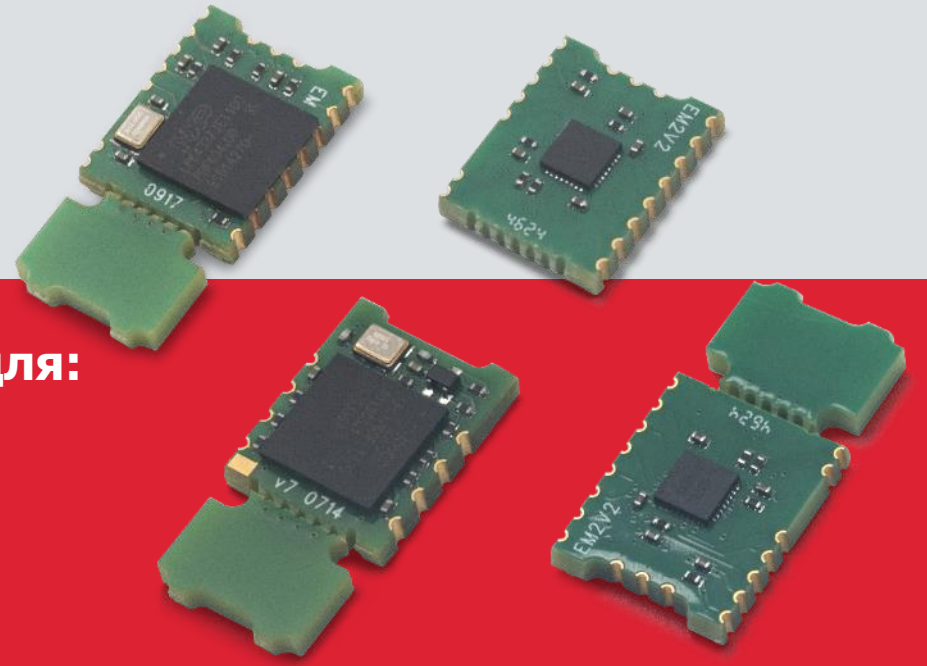
Статические цели атак

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

Динамические цели атак

- Загрузка операционной системы
- Запуск процессов в операционной системе устройства
- Обновление софтверных компонентов операционной системы
- Регистрация нового устройства в системе
- Аутентификация пользователей

Рутокен Модуль



Набор интегрируемых программно-аппаратных средств для:

- защиты межмашинного взаимодействия (M2M)
- автоматизированных систем управления технологическими процессами (АСУ ТП)
- 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

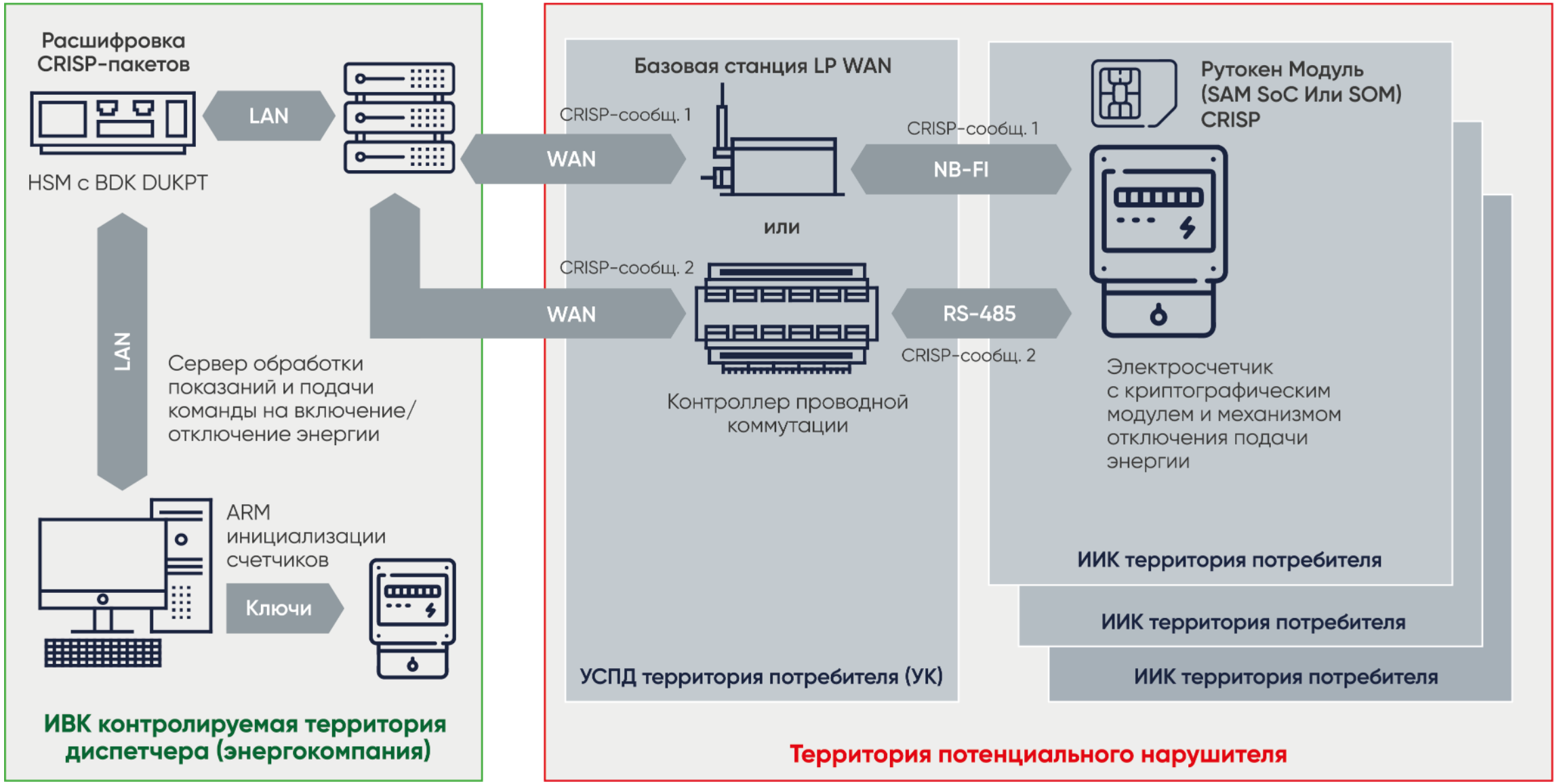
Identity, Integrity, Incessancy

CRISP

Рутокен Модуль + CRISP

1. Контроль аппаратной целостности устройства
2. Защита обмена информацией от подмены и атак повторения
3. Контроль аутентичности передаваемых данных
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

Пример защищенной SCADA-системы



Заключение

1

Аппаратный корень доверия является центральным узлом обеспечения информационной безопасности устройств и систем за счет содержащихся в нем основных криптографических ключей и реализаций криптографических функций, критичных для обеспечения безопасности.

2

Примером реализации аппаратного корня доверия является устройство Рутокен Модуль. Различные форм-факторы и интерфейсы взаимодействия позволяют встраивать Рутокен Модуль в SCADA-системы, АСУ ТП, СКУД и другие информационные системы различного назначения.

Спасибо за внимание!

КОМПАНИЯ АКТИВ

info@rutoken.ru

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

+7 495 925-77-90

Сергей Панасенко

panasenko@aktiv-company.ru

Алексей Лазарев

lazarev@aktiv-company.ru