

Три кита информационной безопасности

Андрей Соломатин

Руководитель по развитию проектов
в государственном секторе,
Компания «Актив»



Компания «Актив»



Комплексная система для защиты,
лицензирования и управления
продажами ПО

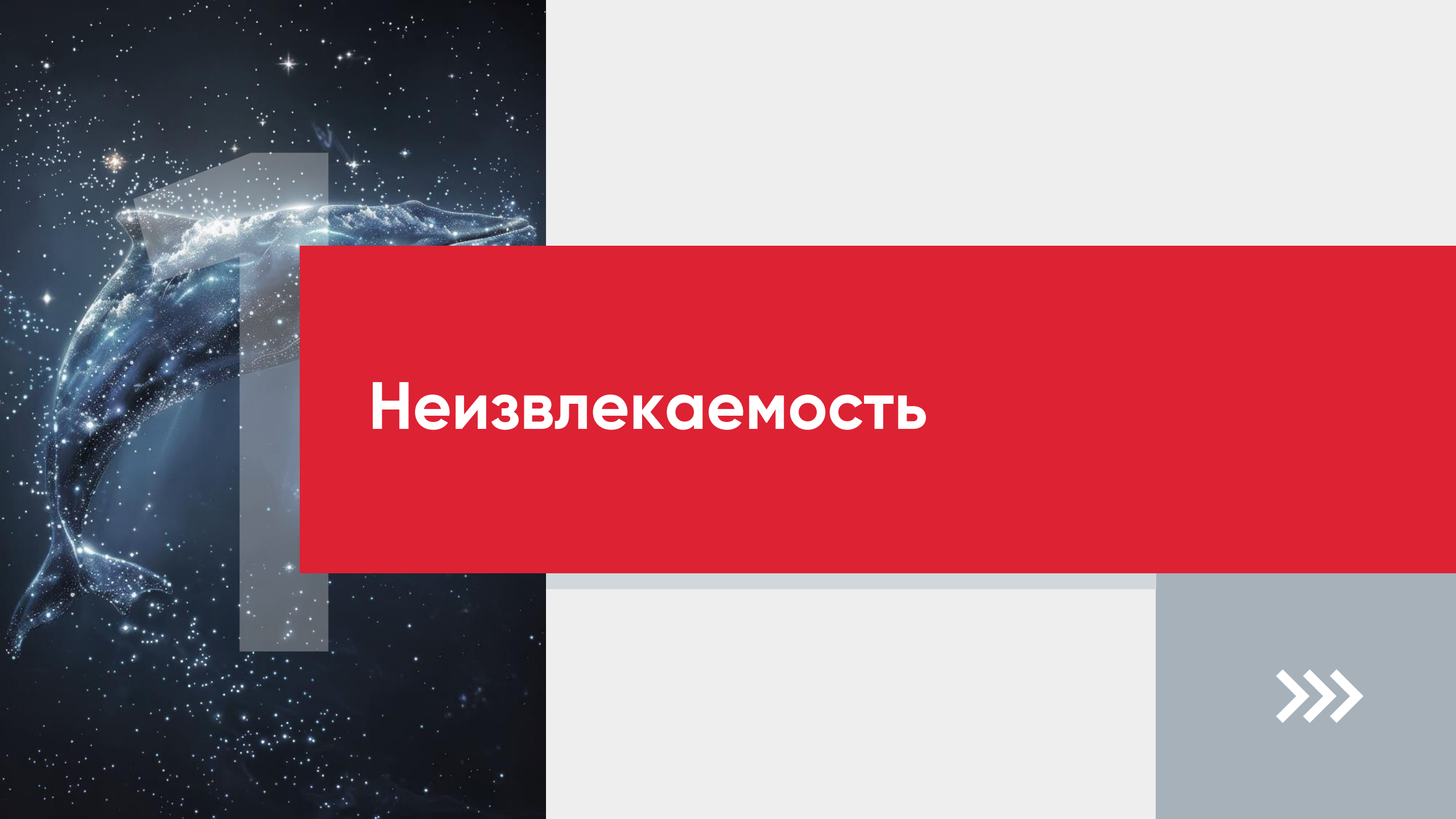
РУТОКЕН

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

AKTIV.
CONSULTING

Консалтинг и аудит в области ИБ





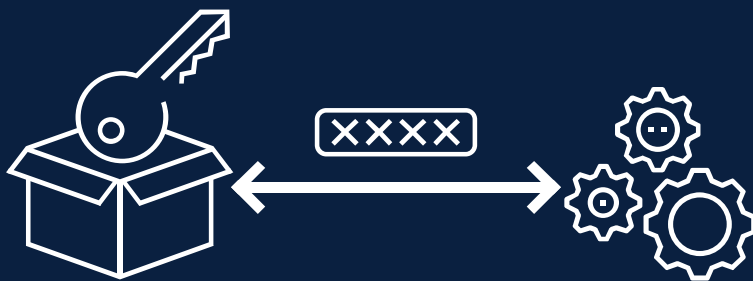
Неизвлекаемость



Какие ключи могут храниться **на токене**?



Извлекаемые ключи



Неизвлекаемые ключи



Виды неизвлекаемых ключей

Стандарт PKCS#11

Генерация ключей и работа с ними производится **с помощью аппаратного СКЗИ внутри активного носителя Рутокен.**

При использовании стандарта PKCS#11 программы работают напрямую с аппаратной реализацией электронной подписи и шифрования внутри токена



ФКН

Генерация ключей и работа с ними производится с помощью двух компонентов:

- **аппаратные возможности устройства Рутокен**
- **программные возможности СКЗИ «КриптоПро CSP»**



Защита канала с помощью протокола SESPake*

* PIN-код пользователя не передается в открытом виде: для обмена сообщениями между криптопровайдером и носителем устанавливается зашифрованный канал

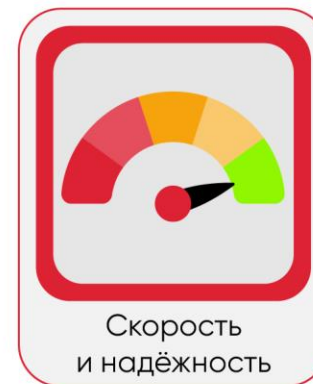
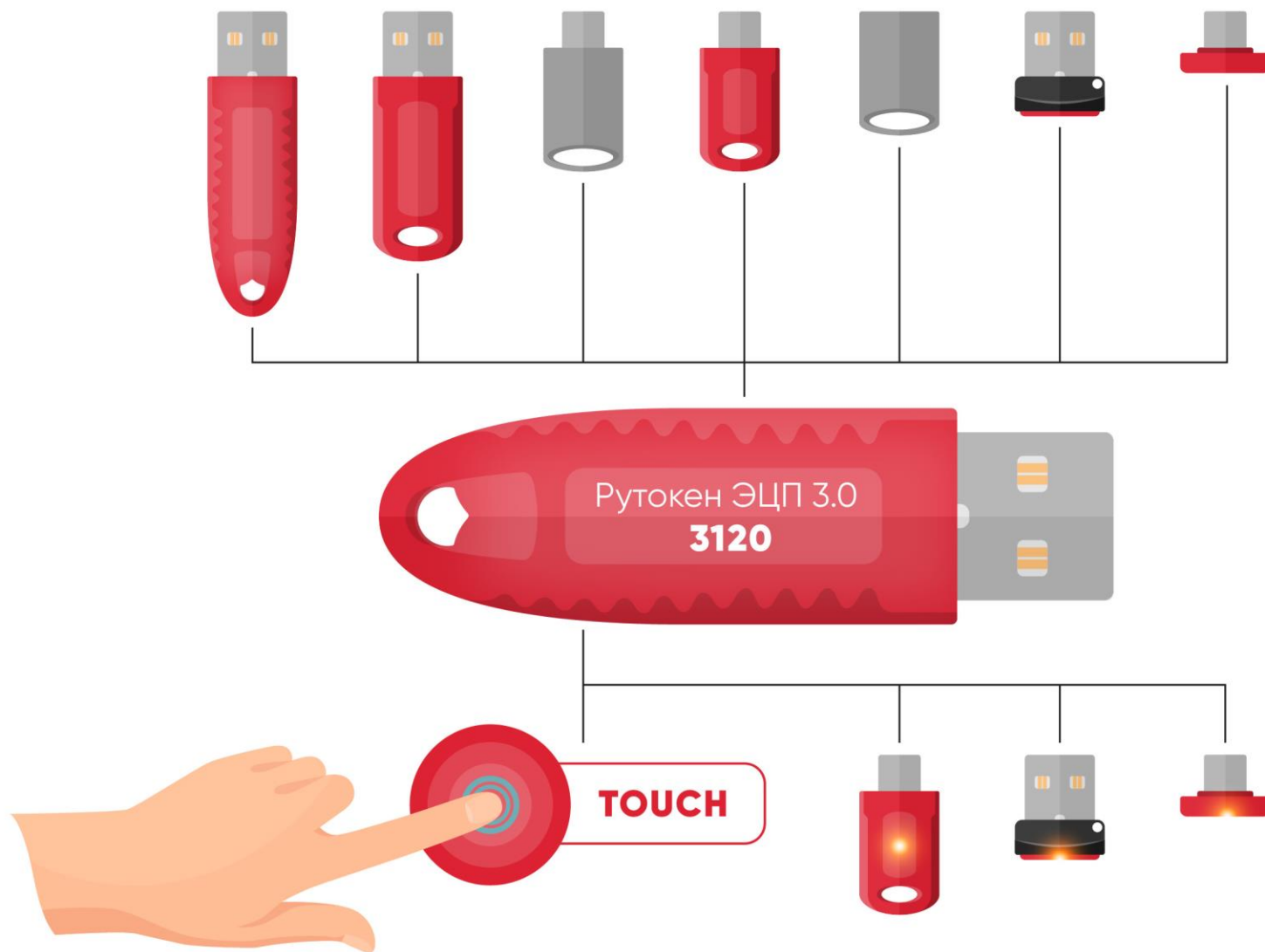


Окончание сертификата ФСБ Рутокен ЭЦП 2.0

После 1.09.2025г Рутокен ЭЦП 2.0
использовать для КЭП больше
не разрешено!



Семейство Рутокен ЭЦП 3.0 3120



Рутокен ЭЦП 3.0 3120

новая функциональность:

журнал событий



Поможет при разборе инцидентов с клиентами, которые:

- ✓ По неосторожности удалили ключи
- ✓ Отформатировали устройство Рутокен
- ✓ Сменили PIN-код и забыли об этом



Что в журнале:

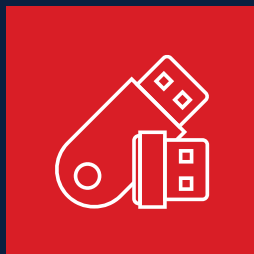
- ✓ Операции форматирования
- ✓ Удаление/генерация любых неизвлекаемых ключей, созданных API Рутокен (PKCS#11, Aktiv ruTokenCSP, minidriver), а также ФКН-контейнеры КриптоПро CSP 5.0+
- ✓ Смена PIN-кодов Пользователя/Администратора



~~Двух~~Трехфакторная аутентификация

Рутокен ЭЦП 3.0 3250.

Трехфакторная аутентификация



Фактор владения

Защищенное сертифицированное устройство для хранения сертификата аутентификации



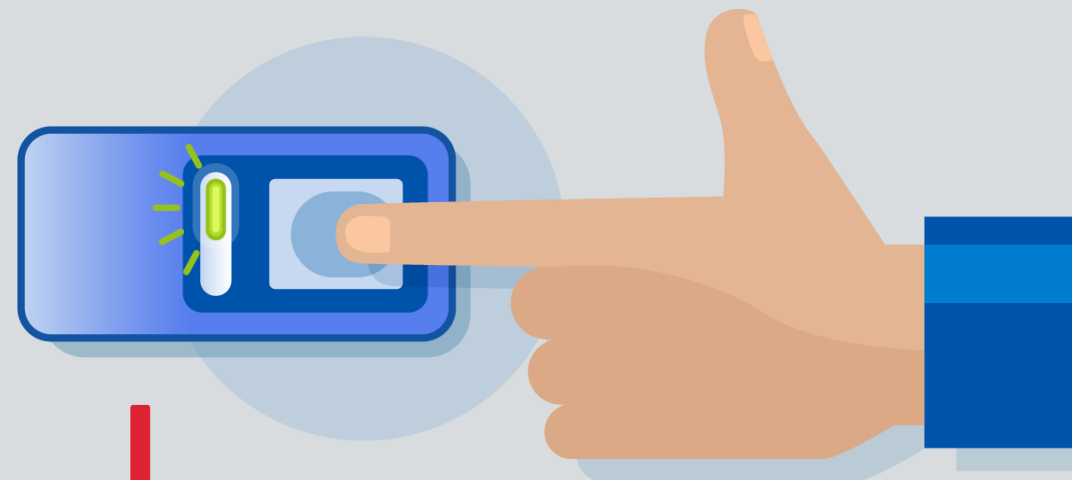
Фактор знания

Персональный PIN-код для доступа к устройству с политикой качества



Фактор свойства

Отпечаток пальца — уникальное свойство владельца устройства



Предъявление отпечатка одного из зарегистрированных пальцев



Ввод PIN-кода
и успешный вход
в систему

Рутокен ЭЦП 3.0 3250.

Принцип работы



Формирование дескрипторов

При занесении отпечатков происходит их анализ и математическая обработка

```
1110101101
1010100101
0110001011
1010101101
1110101101
1010100101
```

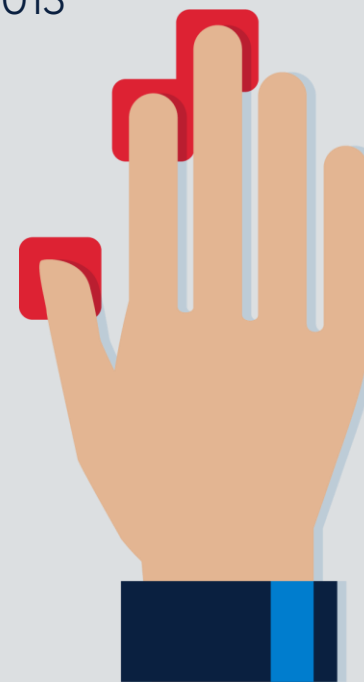
Инициализация устройства

На финальном этапе в устройство записываются дескрипторы пальцев в формате ГОСТ Р ИСО/МЭК 19794-2-2013



Сбор биометрических данных

Для записи в токен собираются данные трех разных пальцев, по четыре отпечатка в каждом



Программный продукт для 2ФА

Рутокен Логон для Linux

Поддерживаемые ОС:

Astra Linux, Альт, РЕД ОС

Поддерживаемые домены:

Active Directory, ALD Pro,
FreeIPA, SambaDC

Поддерживаемые смарт-карты и токены:

Рутокен ЭЦП 2.0/3.0,
Jacarta-2 PKI/ГОСТ

Методы аутентификации:

сложный пароль на токене
или сертификат x509 (PKI)

Параметры входа

Логин и пароль

Рутокен ЭЦП 2.0
5985-333-333

Рутокен ЭЦП 2.0
5985-333-333

РУТОКЕН

Рутокен ЭЦП 2.0 5985-333-333

admin-test

PIN-код

Продолжить

Запросить демо





Ключевые задачи Рутокен Логон для Linux

Инструмент для настройки
многофакторной аутентификации

Позволяет:

- ✓ **Реализовать многофакторную аутентификацию** во всех отечественных ОС и доменах
- ✓ **Сократить затраты на внедрение аутентификации**
- ✓ **Закрыть потребности** Enterprise заказчиков в настройке аутентификации



Автоматизация учета СКЗИ



СКЗИ, они повсюду



- Ключевые носители с сертификатом ФСБ
- Ключевые документы для ЭП
- Программные криптопровайдеры
- Клиенты и серверы VPN
- Средства доверенной загрузки
- Удостоверяющие центры
- ...



Проблемы учета СКЗИ



- ✓ Использование СКЗИ стало действительно массовым
- ✓ Тяжело отслеживать актуальность информации и инвентаризировать
- ✓ Большое количество действий по учету СКЗИ выполняется и обрабатывается вручную
- ✓ Внезапное завершение сроков действий ключей и сертификатов ЭП нарушает бизнес-процессы

Что необходимо при учете СКЗИ, СЗИ, ключевых документов и сертификатов?



Обнаруживать

Ключевые носители, программные СКЗИ, ключи и сертификаты



Вести учет

СКЗИ, СЗИ, ключевых документов и сертификатов согласно приказу ФАПСИ № 152, формировать отчеты



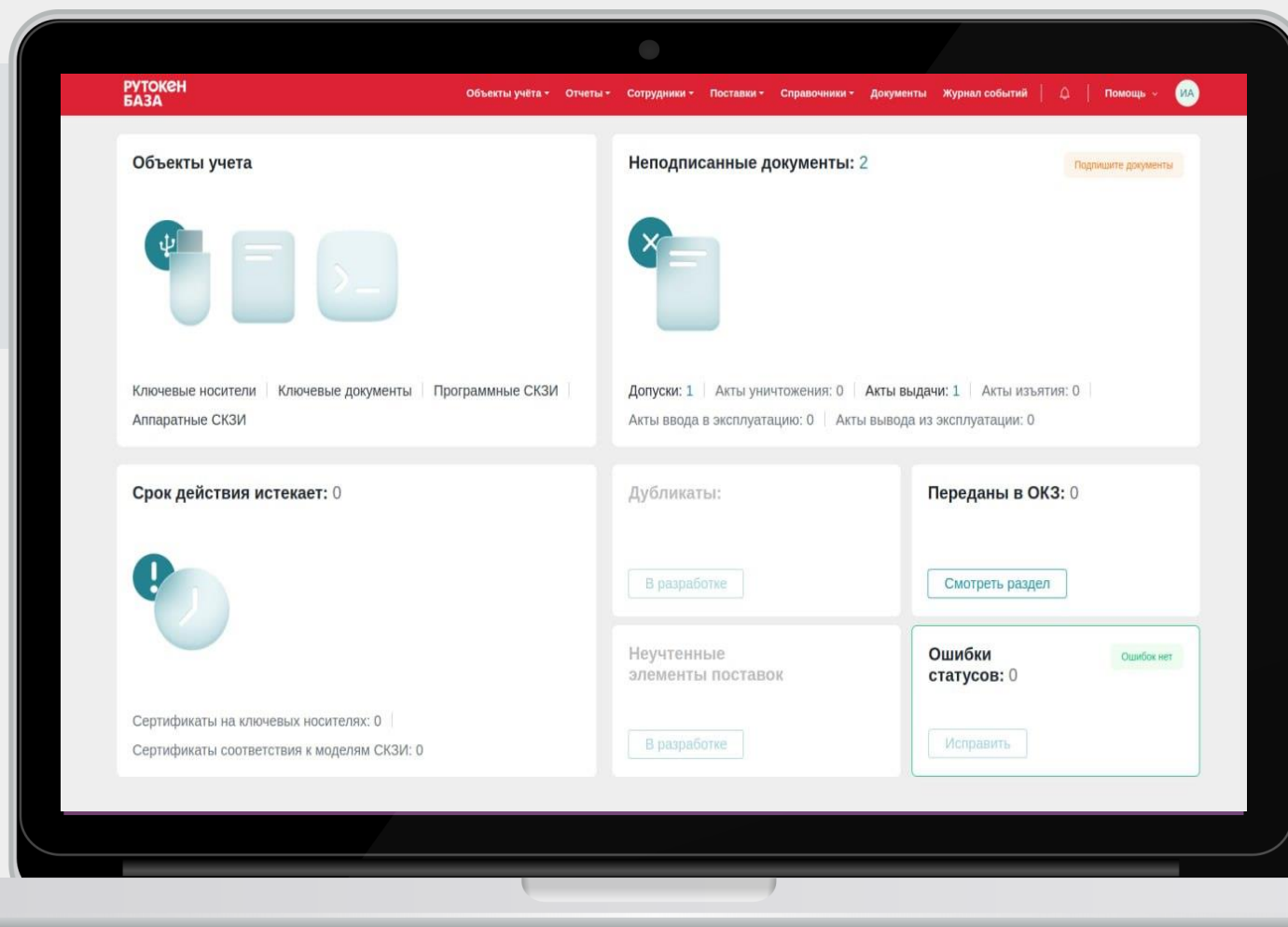
Контролировать

действие сертификатов ЭП и криптографических ключей, сертификатов соответствия, гарантийных сроков и пр.

Решение – Рутокен База



Находится в Реестре
отечественного ПО



Что умеет РутOKEN База



Обнаружение
СКЗИ / СЗИ



Операции с СКЗИ
согласно приказу 152
ФАПСИ



Контроль
за возникновением
событий



Формирование
отчетов и ведение
журналов

Запросить демо
РутOKEN База





**Совместимость
с отечественными
разработками**

Рутокен — центральный элемент безопасности



Отечественные операционные системы

Устройство Рутокен используется как средство электронной подписи и двухфакторной аутентификации для входа в локальные и доменные учетные записи



- ГосЛинукс (РЕД-СОФТ)
- Роса (НТЦ ИТ РОСА)
- AlterOS (ГК «АЛМИ»)

- Мобильная ОС «Аврора» (ОМП)
- Роса Мобайл
- РЕД ОС М



Криптопровайдер

КриптоПро CSP / JCP

Код Безопасности CSP



**ViPNet CSP
ViPNet OSSl**



Signal-COM CSP, JCP



Валидата CSP



Библиотека PKCS#11

Поддержка отечественных ПК и мобильных устройств



kraftway[®]
РОССИЙСКИЕ ТЕХНОЛОГИИ



Fplus ✨



AQUARIUS



Контактная информация



Андрей Соломатин

Руководитель по развитию проектов
в государственном секторе,
Компания «Актив»



andrey_solomatin@rutoken.ru
info@rutoken.ru



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



+7 495 925-77-90
+7 926 275-76-24

РУТОКЕН

