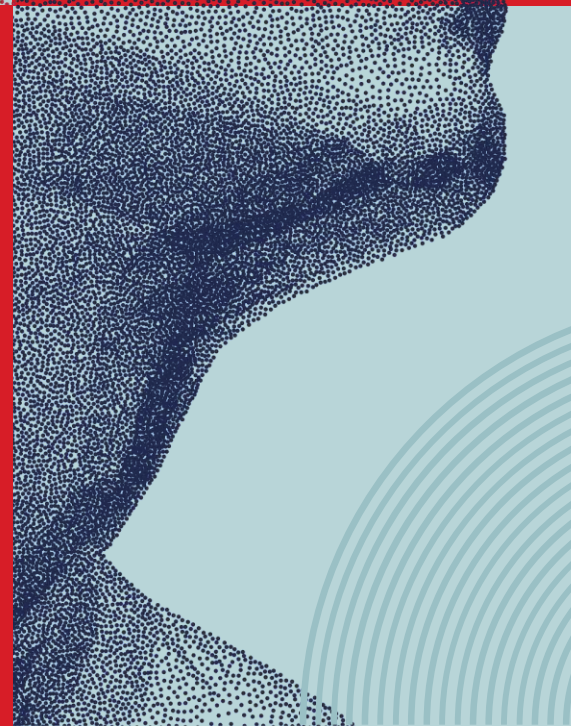
ТЕХНОЛОГИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН DAY

ТЕХНОЛОГИИ ДОВЕРИЯ

КОМПАНИЯ АКТИВ

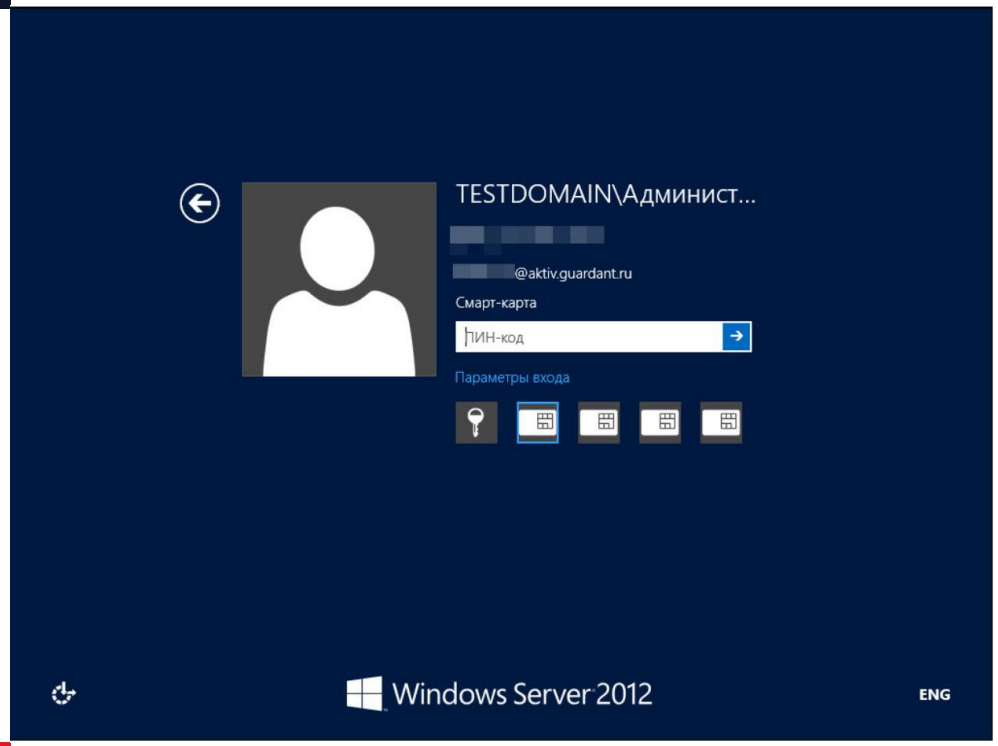


Как настраивать многофакторную аутентификацию в Linux в 8 раз быстрее

Кирилл Аверченко

Руководитель отдела технического пресейла, Компания «Актив»

Давным давно
в далекой галактике...



Аутентификация в домен Active Directory (AD) на Windows

- Токены и смарт-карты – нативный компонент AD
- Распространение – средствами групповых политик
- Не требовались драйвера Рутокен

А потом пришло импортозамещение...

Динамика объема российского рынка ОС для ПК и серверов, млн руб.*

Наличие параллельного импорта, бессрочных лицензий и пиратского ПО обуславливает плавное замещение иностранных решений до 2030 г.

*Tadviser.ru
**Softline

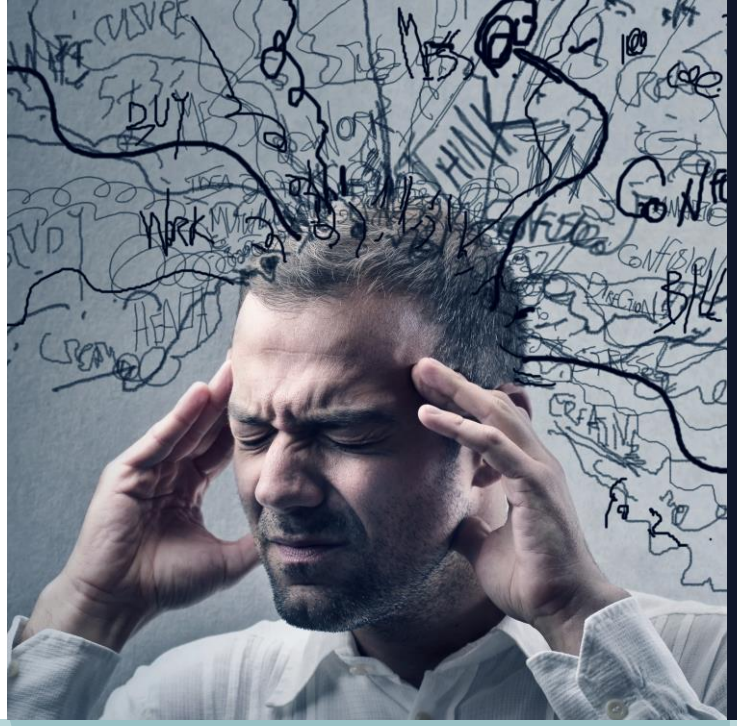
На 78%

упали продажи Windows в РФ за 1-й квартал 2023**

Кто у нас теперь?

- Astra Linux (~ 78% рынка)
- ОС Альт (~11% рынка)
- РЕД ОС (~ 8% рынка)

В чем проблема аутентификации в отечественных ОС?



- Нет нативных инструментов для токенов и смарт-карт
- Поддержка добавляется различными open-source библиотеками
- Многообразие разных вариантов доменов и гетерогенных сред (AD, FreeIPA, SambaDC, ALD PRO, РЕД АДМ, Альт Домен…)
- Нет единых возможностей и UX
- Каждый АРМ настраивается вручную (нужно > 10 действий)

В 10 раз

возрастают трудозатраты на внедрение 2FA

В чем проблемы паролей

Легко подсмотреть
и украсть

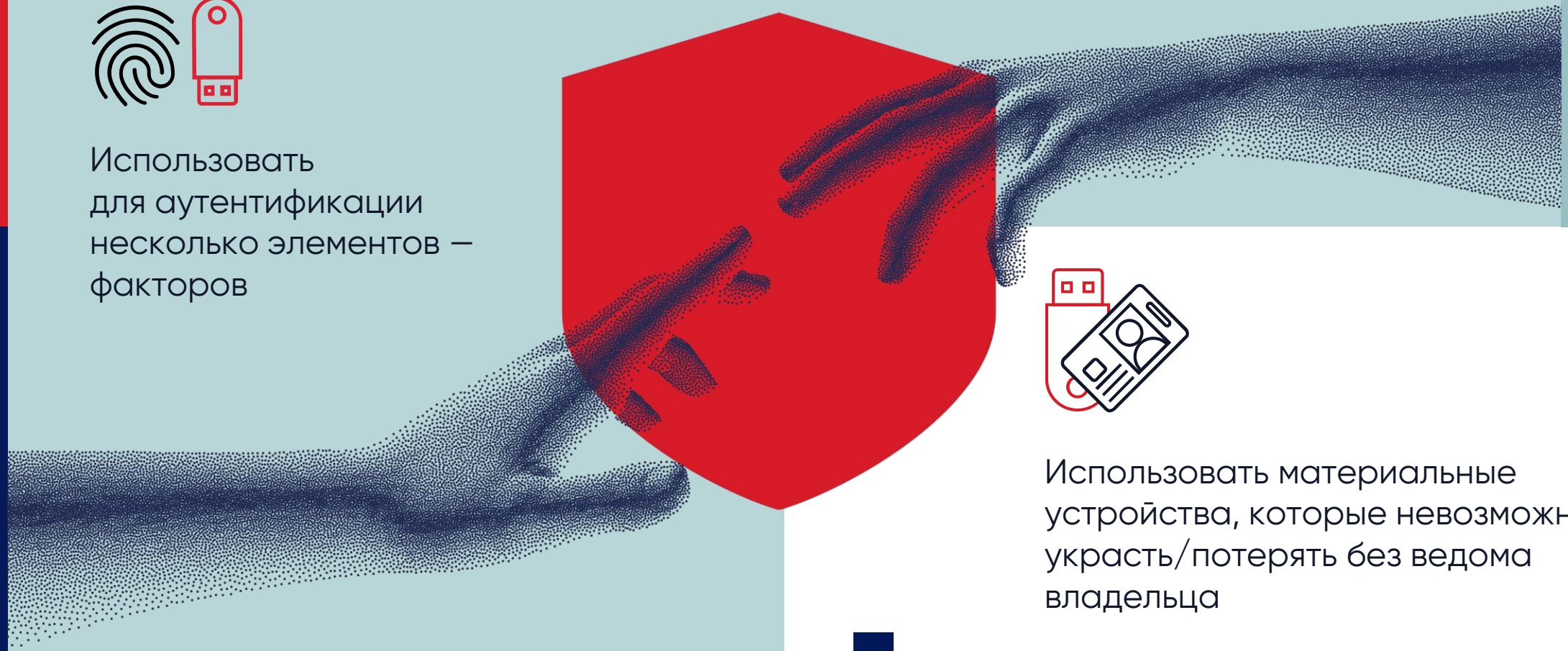
Можно неограниченно
долго использовать вместе
с владельцем

Невозможно понять,
что пароль украден

Сложно доказать, что вред
причинил злоумышленник,
а не владелец пароля

Как защититься

Использовать
для аутентификации
несколько элементов –
факторов



Использовать материальные
устройства, которые невозможно
украсть/потерять без ведома
владельца

Реализация 2ФА на основе Рутокен

#1 Первый фактор — владение физическим токеном семейства Рутокен ЭЦП, который нужно подключить к ПК

#2 Второй фактор — знание PIN-кода токена

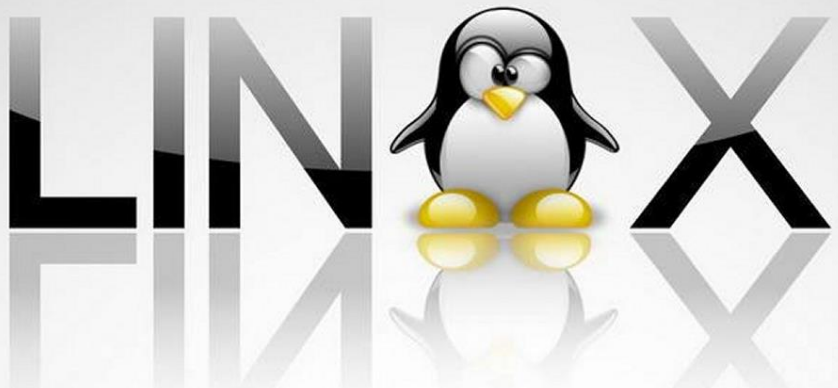
Если подсмотрен PIN-код, то аутентификация без токена невозможна

Если токен украден, то аутентификация невозможна:

- PIN-код не известен
- При переборе PIN-кода токен блокируется
- Владелец уведомляет администратора

Механизм аутентификации в Linux

- Pluggable Authentication Module – компонент ОС для выполнения аутентификации
- Базовый PAM реализует аутентификацию с паролями, хранящимися в локальном файле
- Можно создавать свои PAM
- Есть много готовых PAM для разных вариантов 2ФА

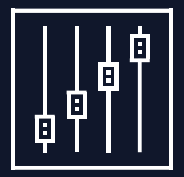


Варианты реализации 2ФА

С использованием инфраструктуры открытых ключей (PKI)

С хранением пароля в защищенной памяти токена

2ФА без PKI



При настройке:

- Генерируется длинный и сложный пароль
- Пароль устанавливается для пользователя в ОС
- Пароль сохраняется на токене

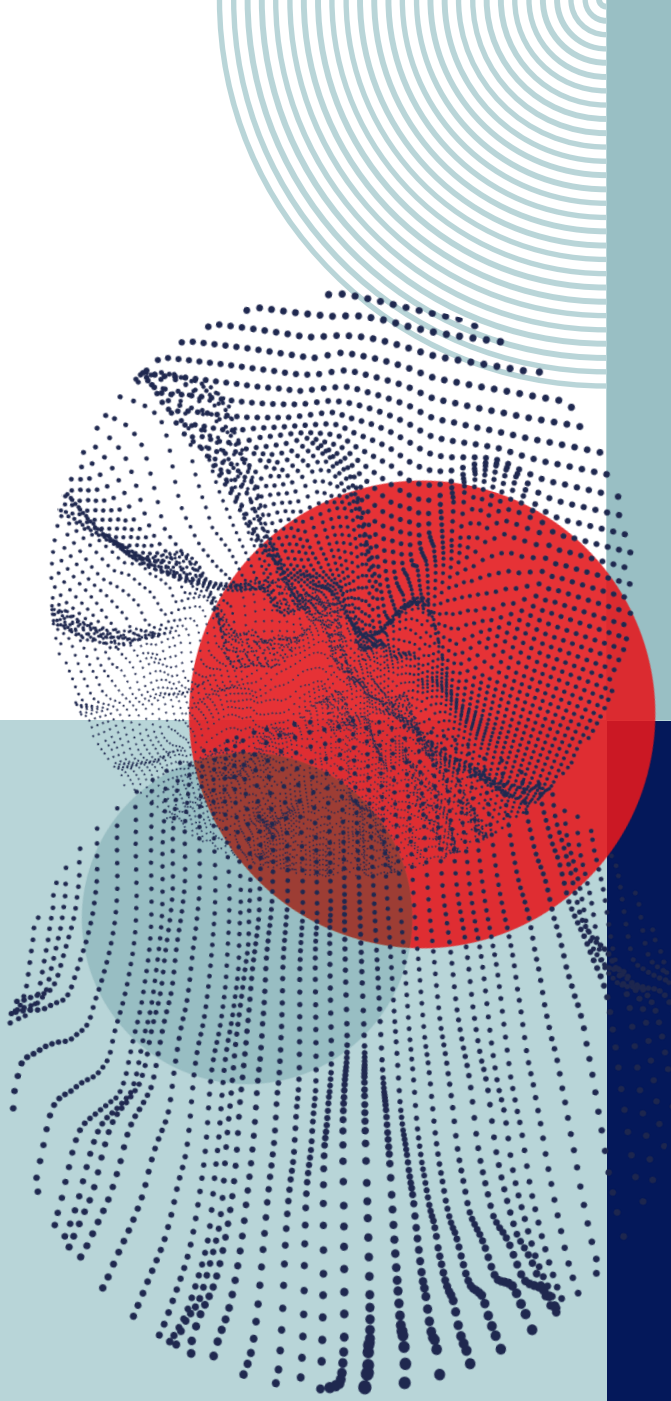
При аутентификации:

- Токен подключается к ПК
- Пользователь вводит PIN-код и разблокирует токен
- PAM извлекает пароль из памяти токена и выполняет аутентификацию

Ключевые задачи
Рутокен Логон для Linux

Инструмент для настройки многофакторной аутентификации

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



Функциональные возможности продукта: устройства

- Поддерживаемые смарт-карты и токены – Рутокен ЭЦП 2.0/3.0, Jacarta-2 PKI/ГОСТ

Функциональные возможности продукта: методы

- Методы аутентификации — сложный пароль на токене или сертификат x509 (PKI)
- Проверка сертификата: CRL или OCSP-сервер

Функциональные возможности продукта: операционные системы

Поддерживаемые ОС:

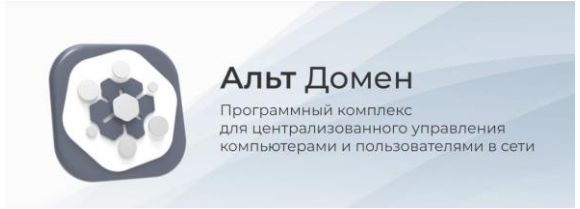
- Astra Linux 1.7.2+, 1.8.1+, 4.7+
- ОС Альт 10, СП релиз 10, 8 СП
- РЕД ОС 7.3, 8

Архитектуры ОС -x86 и ARM

Функциональные возможности продукта: домены

Поддерживаемые домены:

- Active Directory
- ALD Pro
- РЕД АДМ*
- Альт Домен*
- FreeIPA
- SambaDC



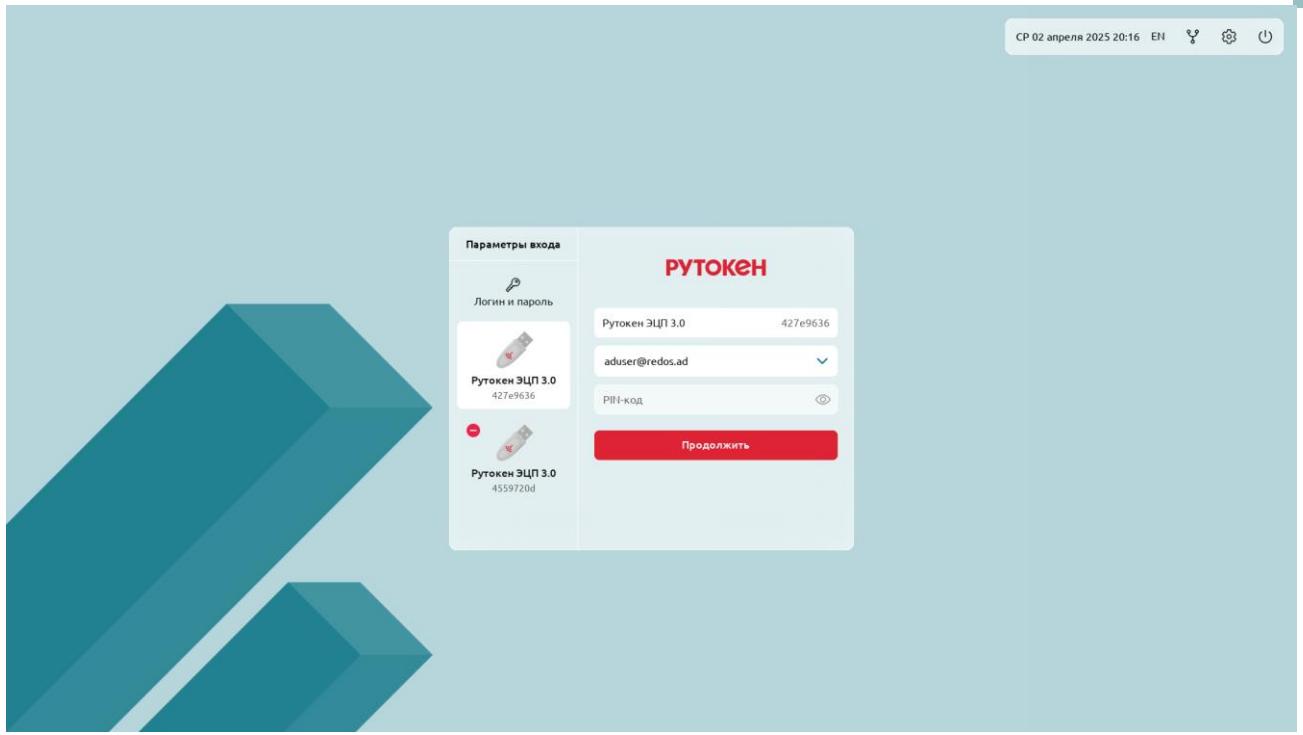
* Поддержка будет в следующих версиях

Функциональные возможности продукта: автоматизация

- Командно-строчный интерфейс (CLI). Сокращение времени на настройку ~ 10 раз относительно «ручного» способа
- Скрипты для быстрого ввода пользователя в различные домены (AD, ALD Pro, FreeIPA)
- Скрипты для развертывания и настройки продукта на рабочих местах
- Интеграция с Рутокен KeyBox

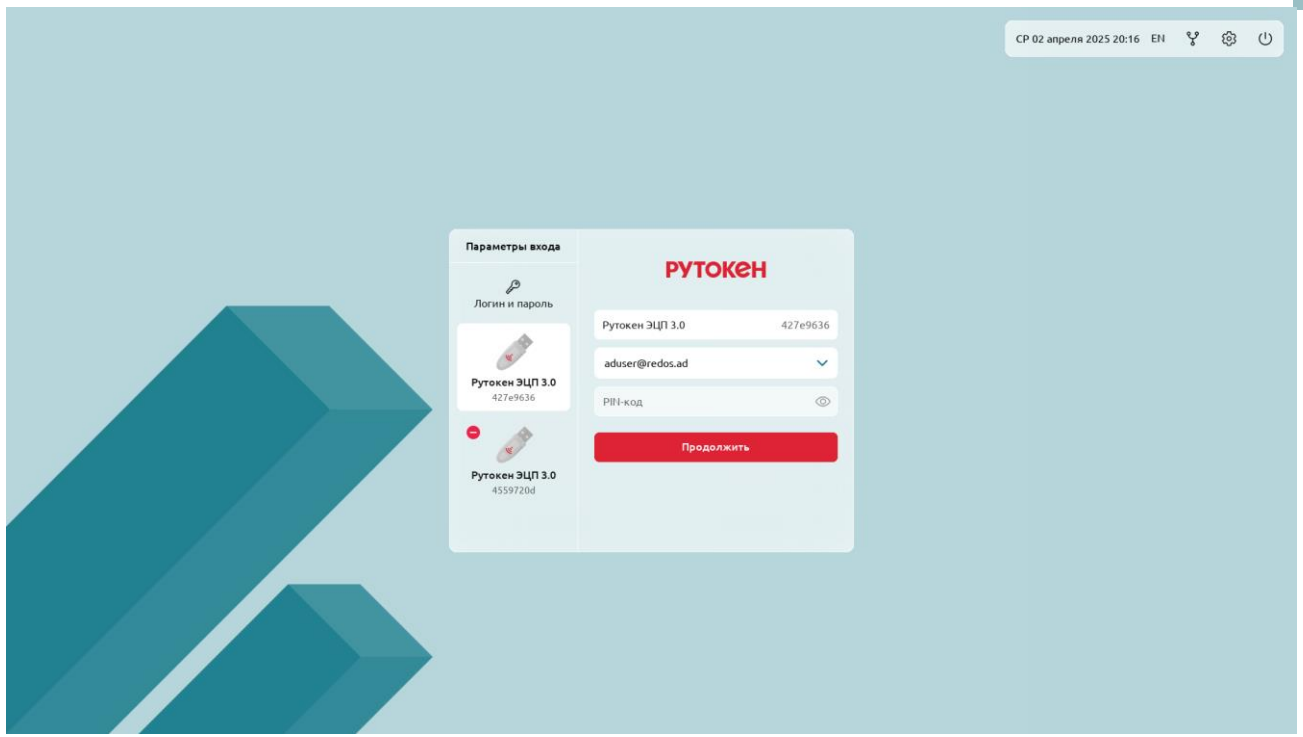
Функциональные возможности продукта: интерфейс

- Собственный экран приветствия и блокировки пользователя
- Обеспечивает единообразный пользовательский опыт



Функциональные возможности продукта: политики

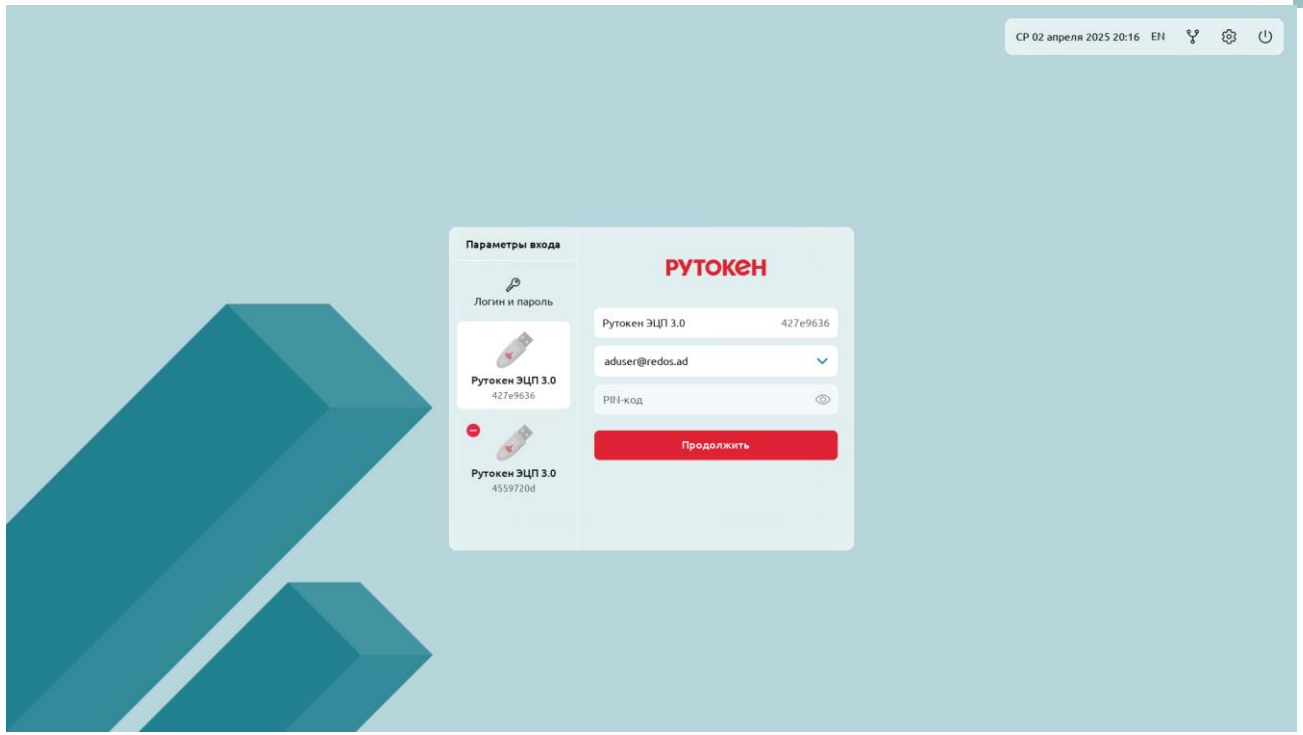
- Политики входа – логин+пароль или PIN-код / только PIN-код
- Действие при отключении токена – блокировка компьютера



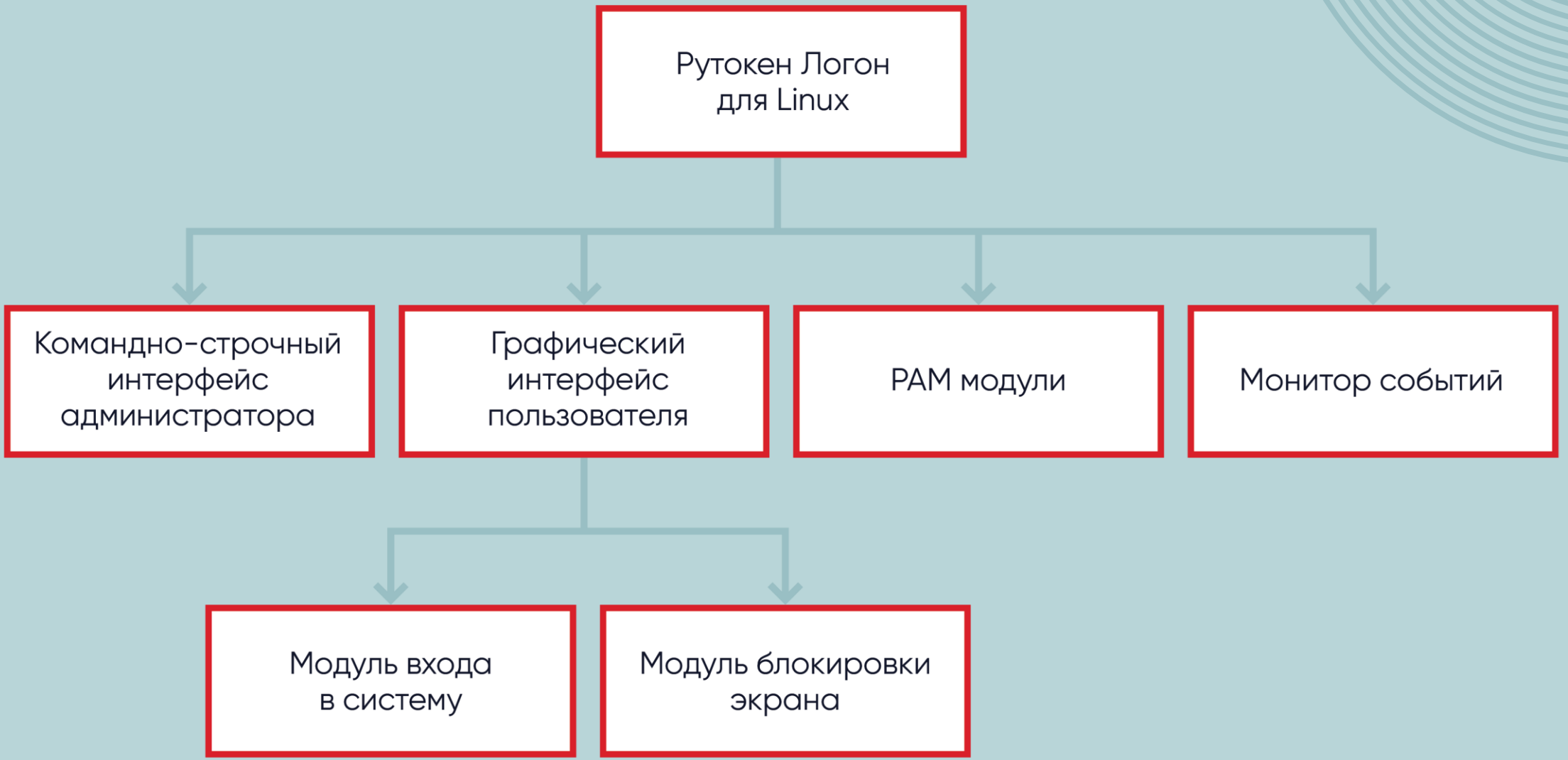
Функциональные возможности продукта: безопасность

Функции безопасности:

- Смена дефолтного PIN-кода токена
- Смена сложного пароля через заданный период
- Журналирование событий



Архитектура продукта



Типовая корпоративная инфраструктура

КОМПАНИЯ АКТИВ

Контактная информация

РУТОКЕН DAY

Кирилл Аверченко

Руководитель отдела технического пресейла, Компания «Актив»

Averchenko@rutoken.ru
info@rutoken.ru

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

+7 495 925-77-90
+7 926 368-11-32