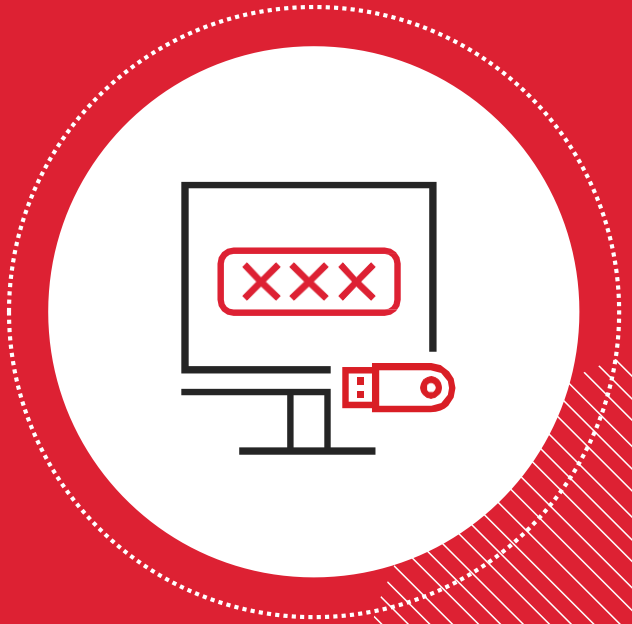
РУТОКЕН

Современные методы аутентификации, как средства обеспечения информационной безопасности



Владимир Иванов

Директор по развитию
Компания «Актив»

Компания «Актив»

guardant

РУТОКЕН

AKTIV. CONSULTING

30 лет
на рынке информационной безопасности

Имеем все необходимые лицензии на разработку СКЗИ и СЗИл

Являемся членом АЗИ, РОСЭУ, ТК26, РусКрипто, ISDEF

Все токены и смарт-карты в реестре РЭП Минпромторга

ПО, драйверы и карточная система Рутокен ОС в едином реестре Минцифры

О чем поговорим?

#1 Насколько надежны традиционные пароли и с какими основными уязвимостями можно столкнуться при однофакторной аутентификации?

#2 Как надо защищать учетные записи?

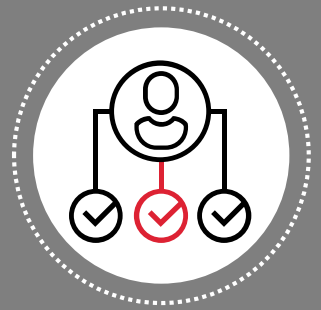
#3 Какие технологии и продукты Рутокен можно использовать для многофакторной аутентификации и какова их роль для бизнеса?

#4 Какие готовые сценарии использования уже есть и какие из них проверены на практике?

Немного ликбеза

Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

Аутентификация — процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.



Авторизация — предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

Виды аутентификации

Критерии:

- **По этапам (шагам):**
  - одноэтапная
  - многоэтапная (два и более этапа
- **По факторам:**
  - однофакторная
  - многофакторная (два и более фактора)
- **По сторонам:**
  - односторонняя
  - взаимная

Какие могут быть факторы?

- Нечто, чем мы **обладаем**
- Нечто, что нам **известно**
- Нечто, что является неотъемлемой **частью нас** самих

Статические пароли — самый популярный метод аутентификации

+

- **Привычно и просто** для пользователей
- **Широко распространены** у разработчиков ПО
- **Не требуют** дополнительных **технических средств**

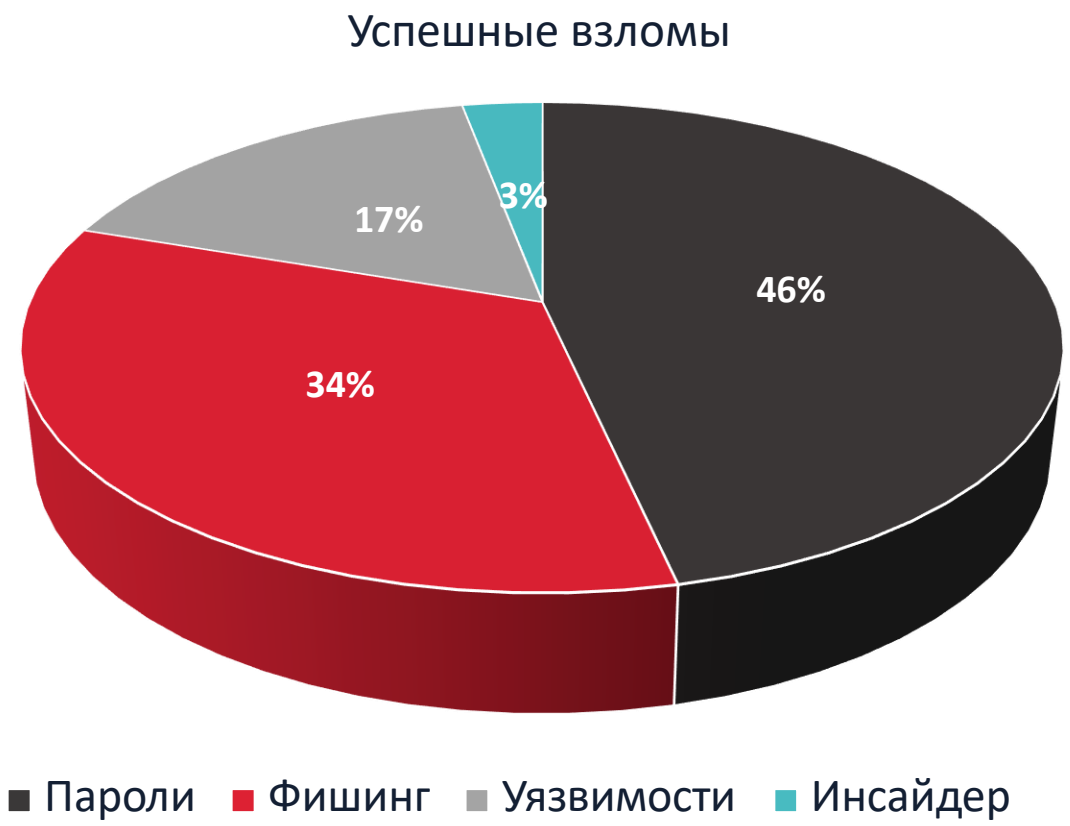
40En5N8*6=goG4A26v

Хороший пароль — пользователь не использует

−

- **Трудно придумать (и запомнить)** хороший пароль
- **Невозможно** установить факт компрометации
- Пользователи используют **одинаковые** пароли в разные сервисы
- На пароли возможно **множество векторов атак**

Статистика успешных взломов в ИС*



46% Подбор паролей от аккаунтов

34% Фишинговые письма

17% Уязвимости в ПО и сервисах

3% Инсайдеры

* согласно исследованию Bi.Zone за 2020-21 г.

Критические уязвимости в ИС*

Во внешних периметрах

59% проектов используют слабые пароли

47% проектов имеют недостаток контроля доступа

Во внутренних периметрах

71% проектов используют слабые пароли

64% проектов используют одинаковые пароли

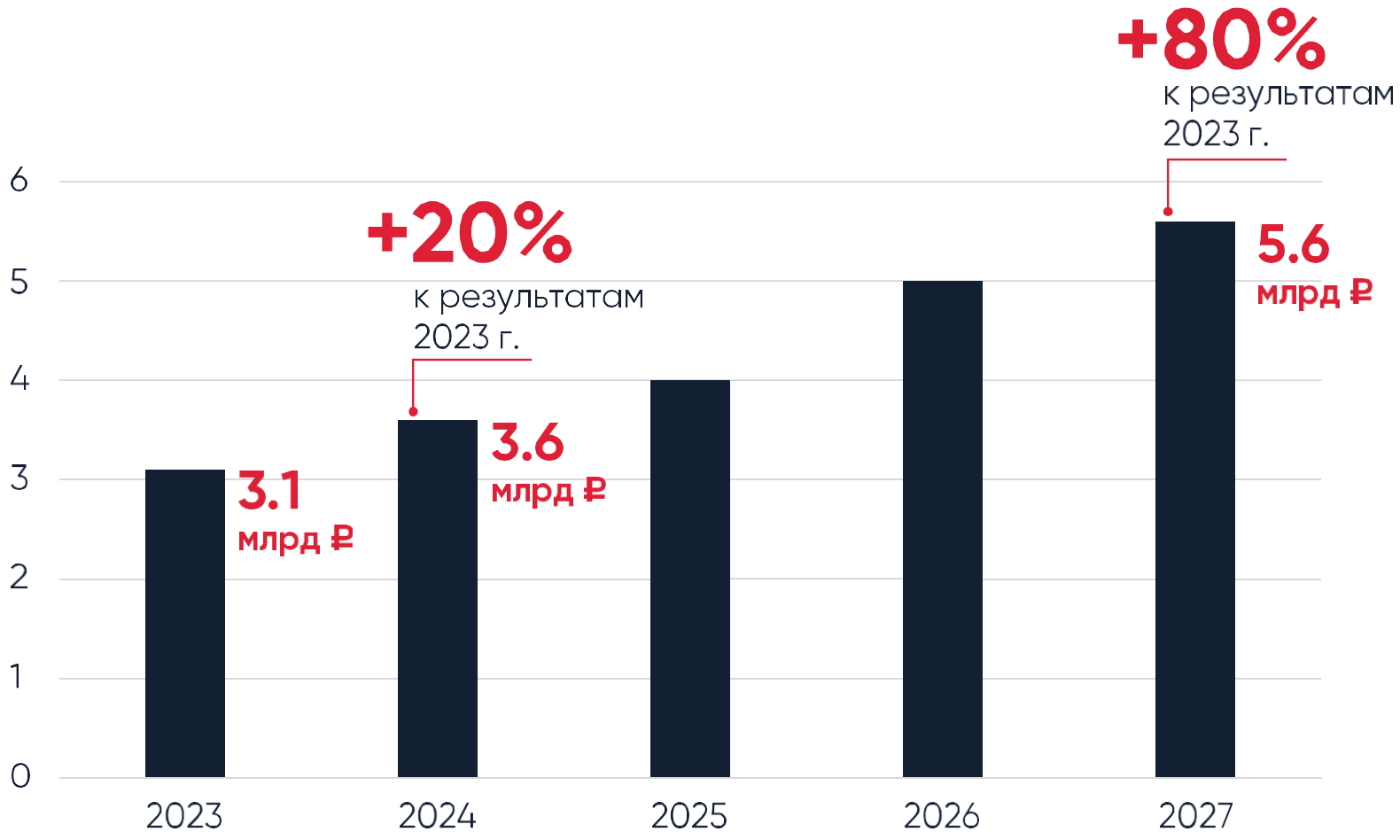
* согласно отчету Ростелеком-Солар за 2022–23 г.

Методы аутентификации
в информационные системы

Методы:	Классы по ГОСТ Р 58833-2020:
Статические пароли	Простая аутентификация
Биометрия (палец\лицо)	Доп. фактор аутентификации
Одноразовые пароли (SMS, Push, OATH HOTP/TOTP)	Усиленная аутентификация
PKI (Инфраструктура открытых ключей)	Строгая
Веб-аутентификация на основе технологий U2F/FIDO	Строгая

Более качественная аутентификация обеспечивает более высокий уровень доверия

Рост отечественного рынка MFA



* согласно аналитике MTS RED от 02.02.2024

Три продукта, три технологии

Рутокен ЭЦП 3.0
(Технология PKI)

Рутокен OTP
(Технология TOTP)

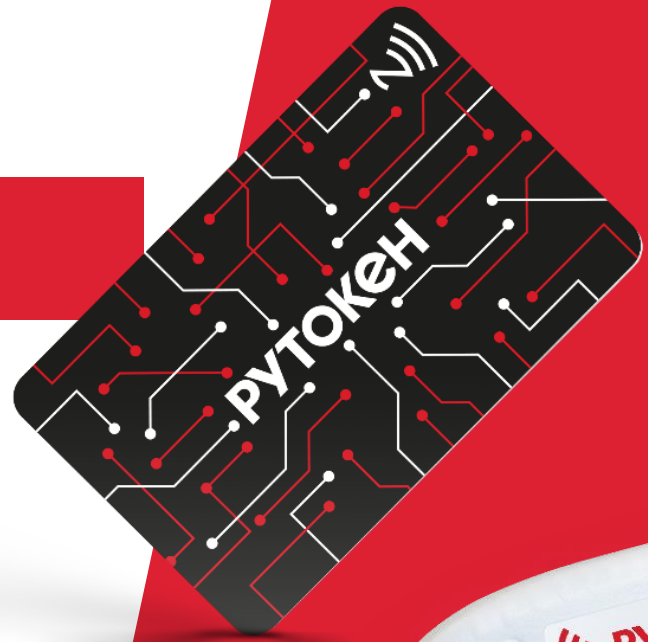
Рутокен MFA
(Технология FIDO2)

Пользовательские аутентификаторы Рутокен

Рутокен ЭЦП (токен или смарт-карта)

- Основан на PKI (инфраструктура открытых ключей)
- Подходит и для ЭП, и для аутентификации
- Создает неизвлекаемые ключи
- Поддерживает NFC
- Разные исполнения (USB-A, USB-A micro, USB-C)
- Работа на всех стационарных и мобильных ОС с любой архитектурой)

Смарт-карта



NFC-токен

Micro

Type-C

Сценарии:
вход в операционные системы

Рутокен ЭЦП используется вместо логина-пароля в ОС

- Поддерживаются все основные ОС — Windows, Linux, MacOs
- Полная поддержка российских ОС — Astra Linux, ОС Альт, РЕД ОС, Роса, Аврора
- Возможность хранения длинного (14-64 символа) пароля на токене при использовании дополнительного ПО (Рутокен Логон для Windows\Linux*)

Преимущества для заказчика:

- Строгая аутентификация (с применением криптографии)
- Защита от внутреннего нарушителя
- Блокировка компьютера при отключении токена

МФЦ Нижнего Новгорода

70
отделений
по городу
и области

2
системы ЭДО

5 000
пользователей

ЮЭДО
внедрение

2ФА
на основе PKI

Рутокен KeyBox
внедрена

Итоги:

- Повышена ответственность пользователей
- Решение парольной проблемы
- Соответствие нормативным требованиям

Сценарии: аутентификация в МДЗ и СЗИ от НСД

Рутокен ЭЦП выступает аутентификатором пользователя\администратора в модули доверенной загрузки и средства защиты от НСД

- Рекомендованный вариант при использовании аппаратных МДЗ: Соболь, Аккорд, Dallas-Lock, Блокхост-Сеть
- Обязательный вариант для программных МДЗ: VipNet SafeBoot
- Используется вместе с СЗИ от НСД: SecretNet, VipNet SafePoint

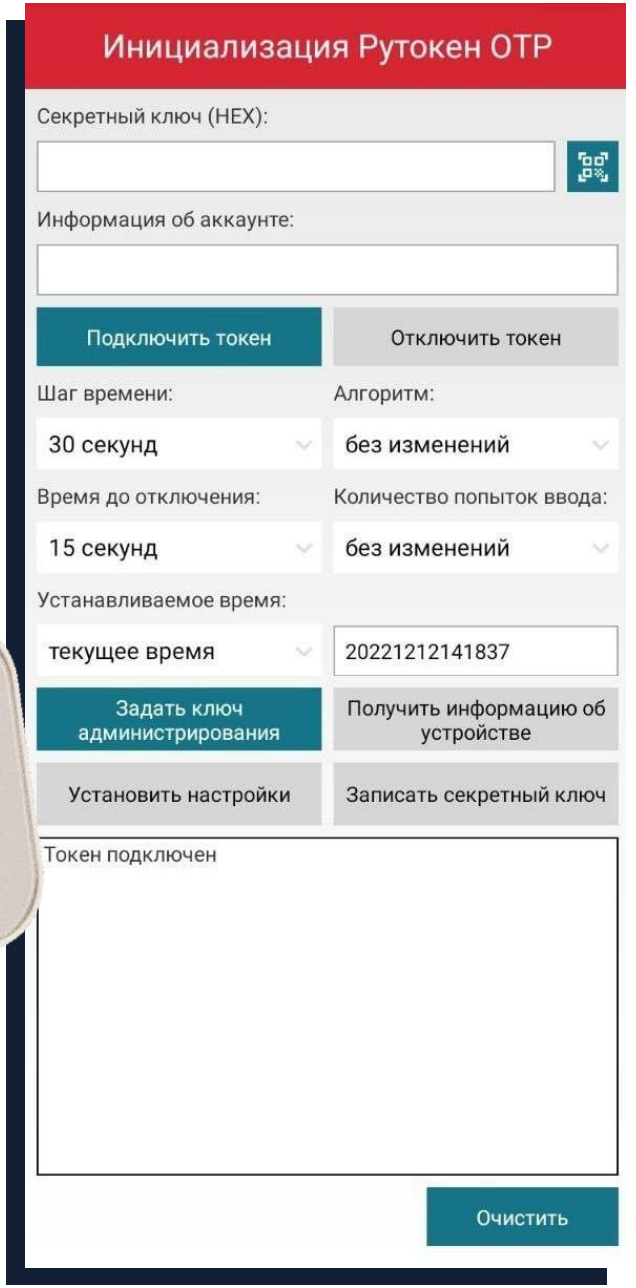
Преимущества для заказчика

- Двухфакторная аутентификация пользователя при загрузке АРМ-а
- Аутентификация администратора при конфигурировании средства защиты от НСД
- Защита от внутреннего нарушителя

Пользовательские аутентификаторы Рутокен

Рутокен OTP (новая версия)

- Вычисляет одноразовый пароль по времени (алгоритм OATH TOTP)
- Персональное устройство с экраном
- Аппаратный таймер подсчета времени (безопаснее программных генераторов)
- Не требует связи с ПК для работы
- Поддерживает NFC для импорта секретного ключа и настройки (есть ПО для Android и Windows)



Почему лучше аппаратный аутентификатор

Рутокен OTP (новая версия)

- Не уязвим для атак на системное время
- Нельзя занести вредонос на устройство
- Возможность массовой поставки предустановленных устройств заказчику и интеграция вектора настройки в систему аутентификаци

Софт или железо?

Решение для Веб-аутентификации

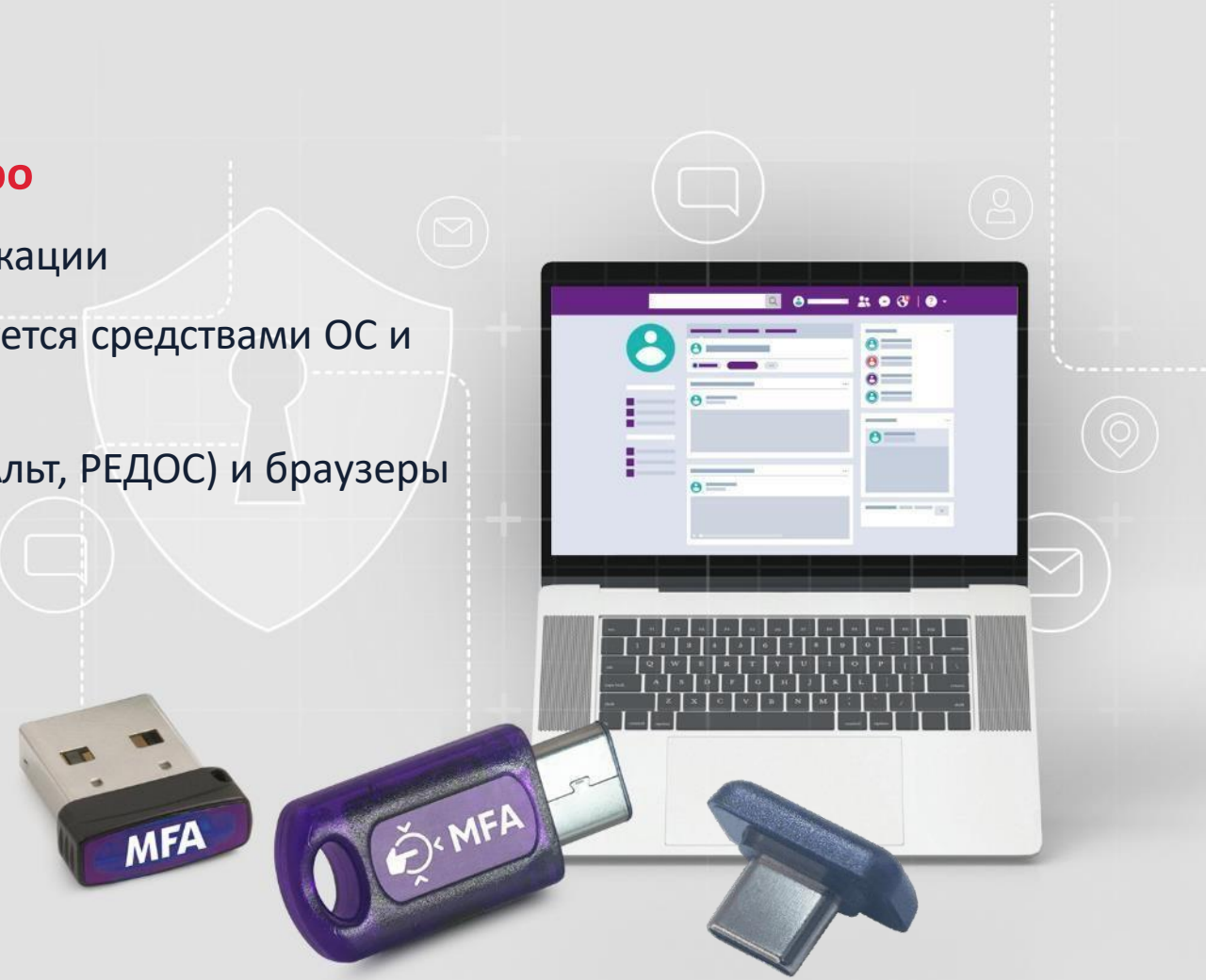
Рутокен MFA

Линейка устройств в формате USB-C и USB-A микро

- Поддержка технологий U2F, FIDO2 для веб-аутентификации
- Не требует установки драйверов (поддержка реализуется средствами ОС и браузеров)
- Поддерживаются отечественные ОС (Astra Linux, ОС Альт, РЕДОС) и браузеры (Яндекс Браузер и Атом)
- Поддержка беспарольной аутентификации (passwordless) для 16-ти аккаунтов
- Возможность обновления прошивки

Планы:

- поддержка NFC и сертификация во ФСТЭК по УД4



Ключевые интеграции

Поддержка в российских idP (VK ID и Яндекс ID)

Доступ в учетные записи отечественных ОС

Поддержка в популярных сервисах и платформах

Сценарии: простая аутентификация в web-приложениях

Рутокен MFA позволяет быстро и просто обеспечить двухфакторную аутентификацию в web-приложения

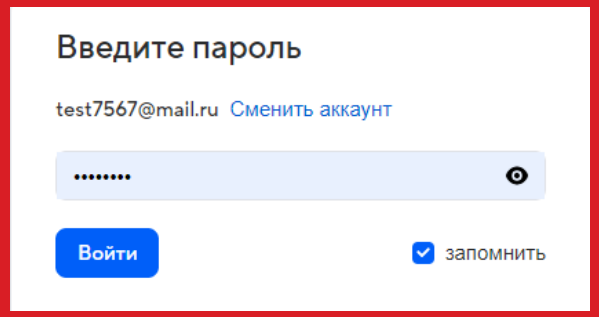
- Любые сервисы, поддерживающие спецификацию WebAuthn.
  В том числе — VK ID, Mail.ru, Облачная платформа NextCloud, GitHub, Google Account, DropBox, Microsoft, Apple ID и другие
- Пользователь управляет своей аутентификацией

Преимущества для заказчика:

- Возможность использования беспарольной аутентификации (не нужно вводить логин\пароль, нужен только токен)
- Работает из коробки на стационарных и мобильных устройствах
- Максимально просто для пользователя

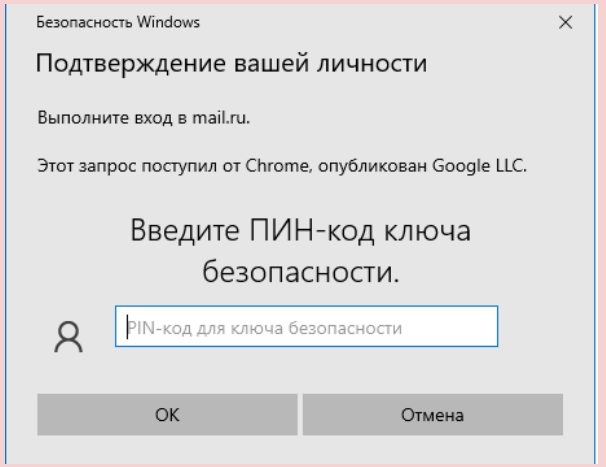
(на примере Mail.ru)

1 Вводим логин\ пароль

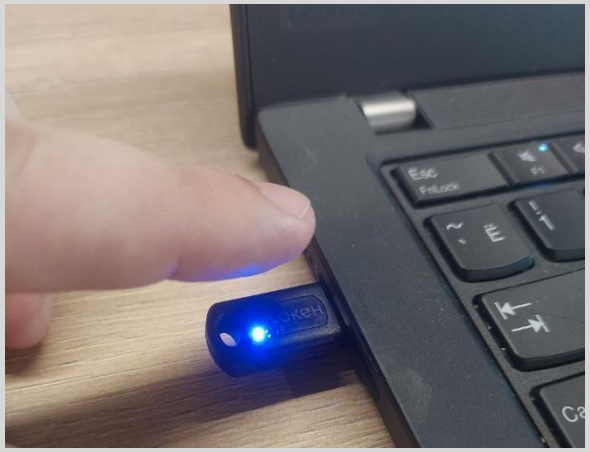


2 Вставляем/ прикладывем ключ

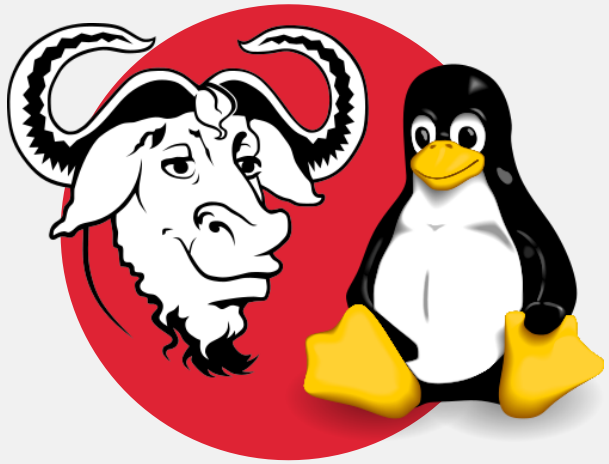
3 Вводим PIN- токена



4 Касаемся устройства



Возможности аутентификации с Рутокен MFA в операционных системах GNU/Linux



- Локальная аутентификация пользователя в ОС с использованием Рутокен MFA с нажатием кнопки в качестве второго фактора
- Локальная аутентификация пользователя в ОС с использованием Рутокен MFA с вводом PIN-кода и нажатием кнопки
- Доступ к хостам по SSH с использованием Рутокен MFA с нажатием кнопки в качестве второго фактора.

Расширение сценариев аутентификации (IAM, IDM, AS)

Позволяют добавить 2FA к сервисам и ПО

- В операционные системы (pam\credential provider)
- В приложения через штатные механизмы аутентификации (SALM, OpenID Connect+ Oath, ADFS)
- В приложения без поддержки аутентификации (Reverse-Proxy)
- К оборудованию (Radius)
- Single-Sign-On (SSO)
- **Используют Рутокен ЭЦП, OTP или MFA в качестве аутентификатора пользователя**

RooX

MFASOFT

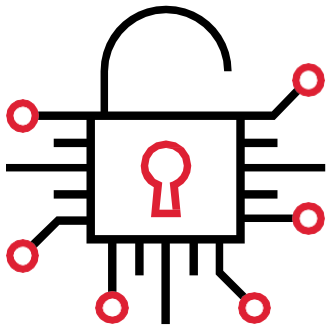
INDEED ID

Avanpost

РУТОКЕН

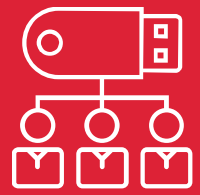
РУТОКЕН БАЗА

Система учета СКЗИ, СЗИ, ключевых пар и сертификатов

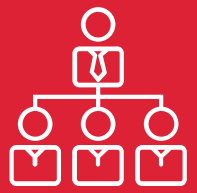


Кому необходим Рутокен База?

Государственная организация,
компания с госучастием,
или коммерческая компания



Большой процент сотрудников,
использующих квалифицированная
электронная подпись

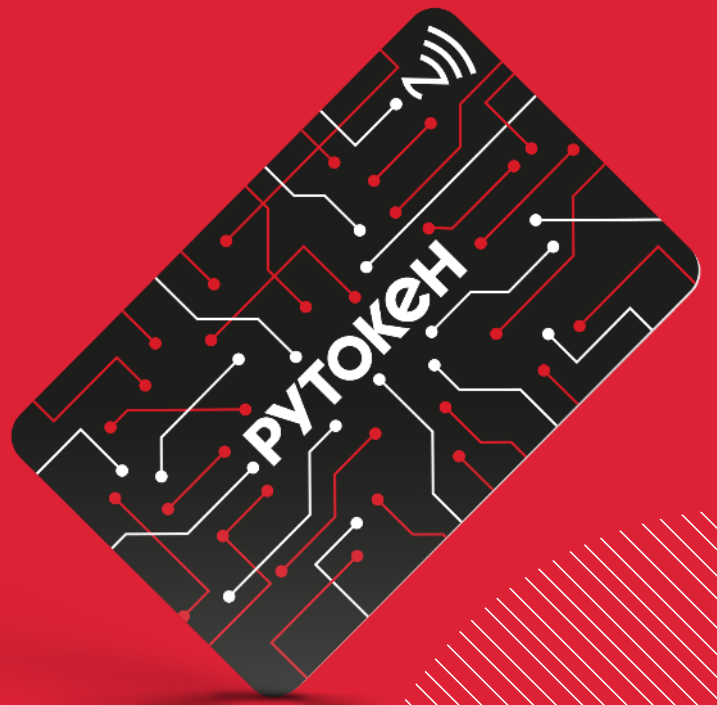


Численность сотрудников —
от 100 человек

Идет процесс импортозамещения —
на серверах и рабочих станциях Linux,
а в продукте должны использоваться
компоненты входящие в реестр
российского ПО

Рутокен База предназначен для ведения учета и управления:

- Защищенными ключевыми носителями от различных производителей
- Прочими ключевыми носителями (реестр, файловая система, usb-flash и т. д.)
- Программными криптопровайдерами, установленными на ПК сотрудников
- Ключевыми документами и сертификатами электронной подписи



Контактная информация

Владимир Иванов

Директор по развитию
Компания «Актив»

info@rutoken.ru

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

+7 495 925-77-90