РУТОКЕН

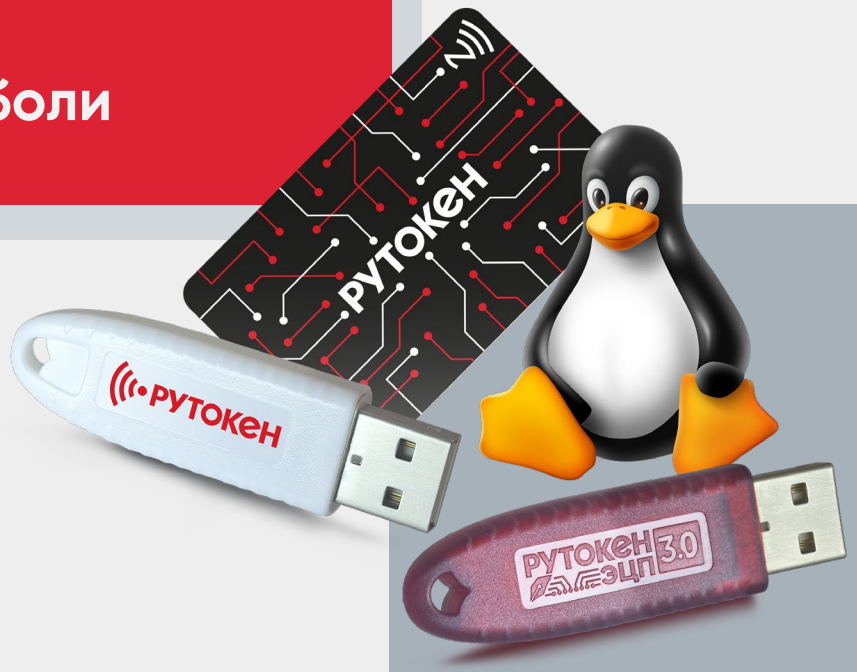
КОМПАНИЯ АКТИВ

Рутокен Логон для Linux

МФА в эпоху ИИ, кибератак и роста требований регуляторов: как перейти на отечественную инфраструктуру без боли

Кирилл Аверченко — Руководитель технического пресейла

Михаил Моисеев — Эксперт по аутентификации



Компания «Актив»

guardant

РУТОКЕН

AKTIV. CONSULTING

30 лет
на рынке ИБ

Лицензии
на разработку
СКЗИ и СЗИ

Член
АЗИ, РОСЭУ, ТК26,
ТК362, РусКрипто,
АПКИТ, АБИСС

Собственная
испытательная
лаборатория

Если вы сегодня на вебинаре, то скорее всего:

- понимаете, что одного пароля уже недостаточно
- знаете MFA на Windows, но не на Linux
- ищете быстрые инструменты внедрения
- хотите перенести MFA на Linux без сбоев
- готовите аргументы по MFA для руководства
- ждете, когда жесткие требования к MFA начнут касаться и вас

Итак, вот почему MFA актуален сейчас

Нормативно-правовая база
MFA

Прямое указание

- **Приказы ФСТЭК №117**
  ГИС класса К1
- **ГОСТ 57580.1-2017**
  Набор мер РД
- **СТО БР БФБО-1.8-2024**
- **PCI DSS**
  Раздел 8.3

Косвенное указание

- **Приказы ФСТЭК №239, №17, №21, №31**
  Набор мер ИАФ
- **Указ Президента №250**
  Усиление мер ИБ

PCI DSS Certified

Банк России

Приказ ФСТЭК №117

- Муниципальные информационные системы (МИС)
- Государственные органы
- Государственные унитарные предприятия и учреждения

Что добавилось в требованиях:

> Применять строгую аутентификацию для осуществления привилегированного доступа к ИС.
> В случае технической невозможности ее применения – использовать многофакторную аутентификацию.

Проблемы с надежностью паролей

45% паролей взламывают меньше минуты

14% паролей взламывают меньше часа

>57% содержат словарное слово

Алгоритмы брутфорса учитывают замену символов *(«е» на «3», «1» на «!», «а» на «@»)*, и знают популярные комбинации *(qwerty, 12345, asdfg)*

*Исследование «Лаборатории Касперского»: анализ 193 млн паролей, обнаруженных в публичном доступе

«ИИ в кибератаках — это тренд»

1

Снижение порога входа

Хакеров-новичков больше:
есть ИИ — необязательно быть экспертом в программировании

2

Автоматизация

Ускоряется сканирование и эксплуатация известных уязвимостей
+ 40% эффективности атак в фишинге и обходе защиты

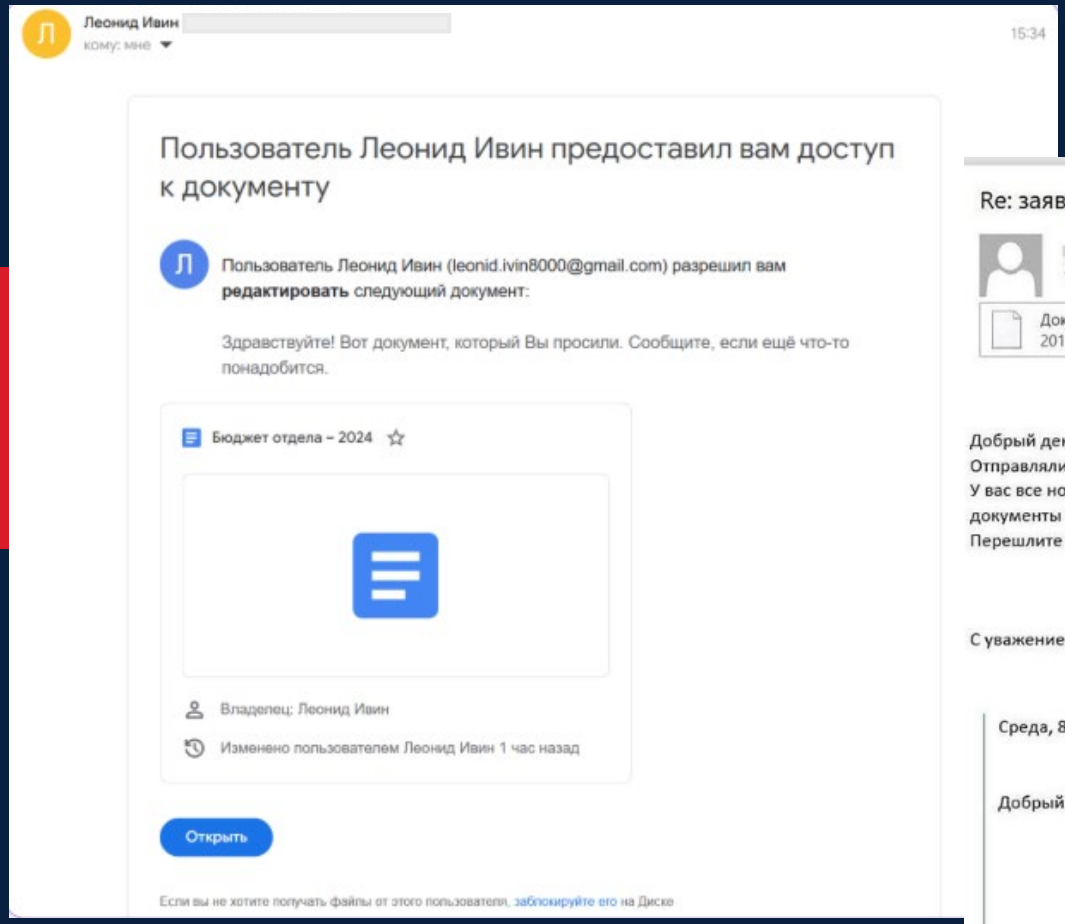
3

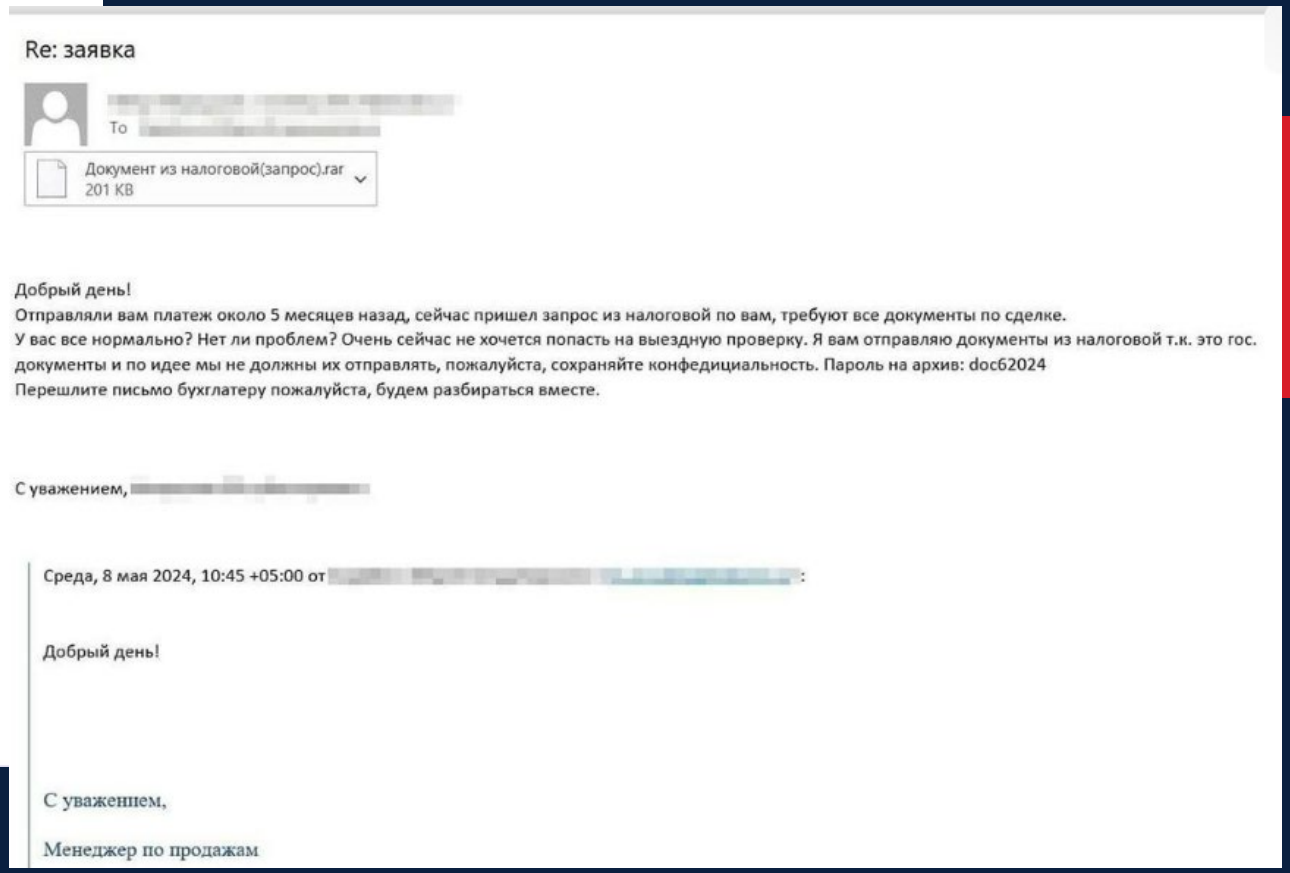
Улучшенный фишинг и социальная инженерия

Данные утечек для таргетированных ИИ-атак

* Forbes

Варианты фишинговых писем





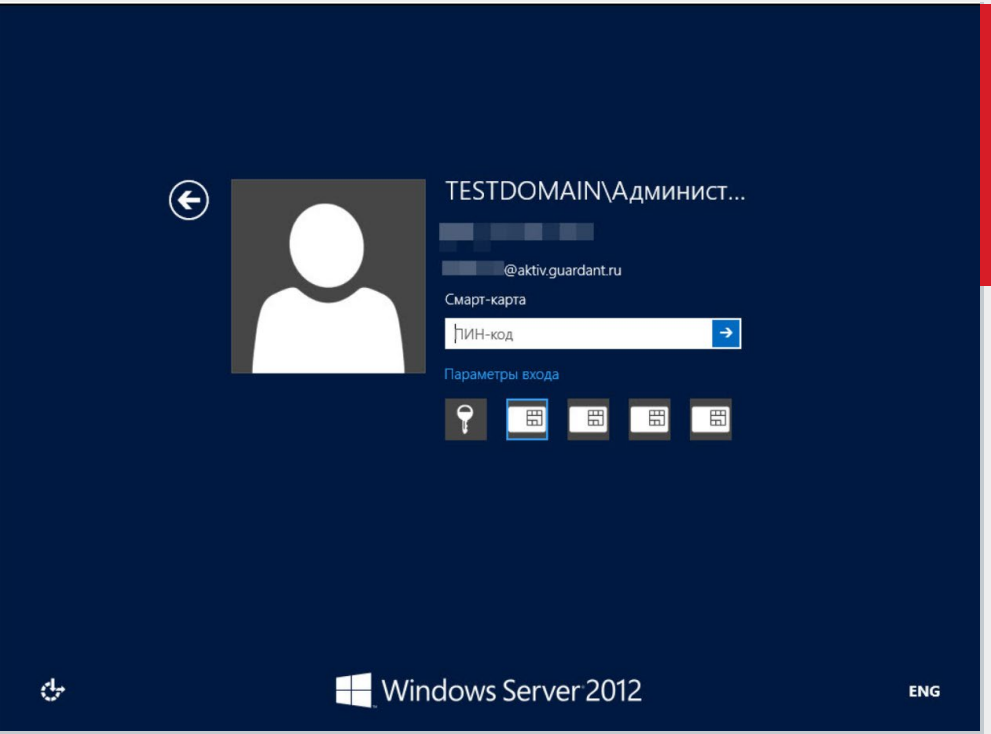
Как защититься

Использовать

несколько элементов — факторов для аутентификации

материальные устройства, которыми невозможно воспользоваться без ведома владельца

«Давным-давно, в далёкой-далёкой галактике...»



Аутентификация в домен Active Directory (AD) на Windows

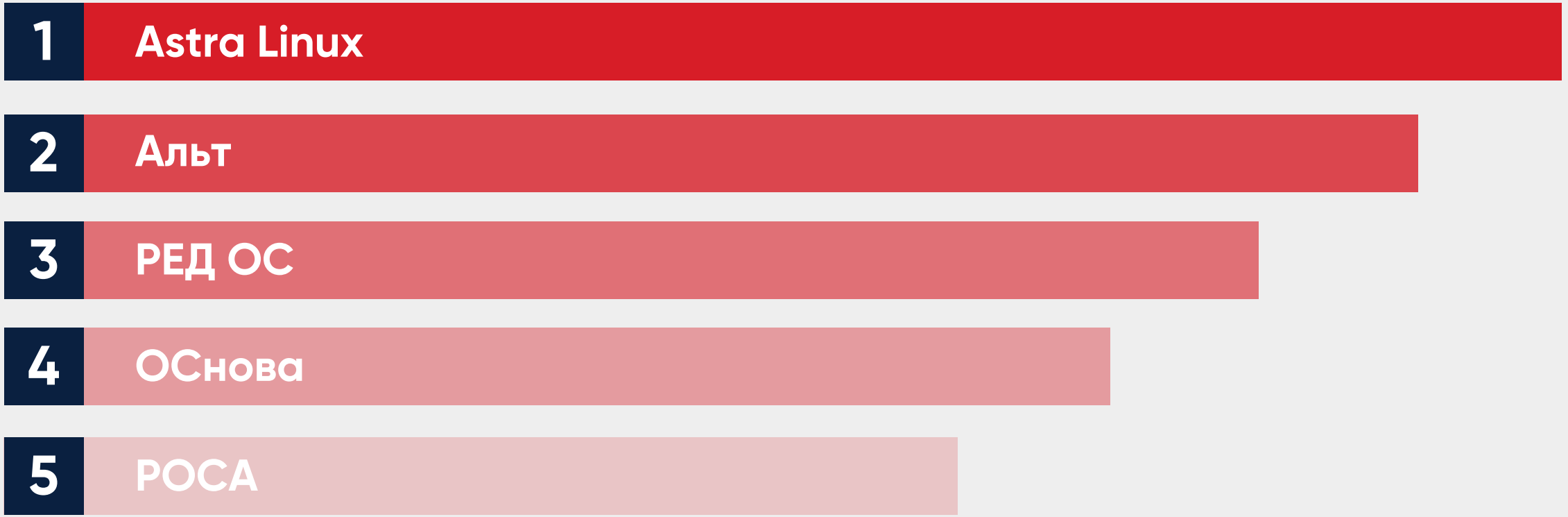
Токены и смарт-карты – нативный компонент AD

Распространение – средствами групповых политик

Не требовались драйвера Рутокен

Импортозамещение

Топ-5 российских операционных систем 2025*



В 2024 году объем российского сегмента составил больше половины от всего рынка, с прогнозом среднегодового роста 23% к 2030 году

*Cnews

С какими болями столкнулись?

- Нет нативных инструментов для токенов и смарт-карт
- Поддержка добавляется различными open-source библиотеками
- Многообразие разных вариантов доменов и гетерогенных сред
- Нет единых возможностей и UX
- Каждый АРМ настраивается вручную

Трудозатраты на внедрение 2FA на Linux возрастают **в 10 раз**

Для настройки станции нужно

- Загрузить корневой сертификат
- Настроить:
  - Kerberos
  - Алгоритмы шифрования
  - TLS для Kerberos
  - SSSD
  - и т.д.

Рутокен Логон для Linux

Инструмент для настройки МФА

Быстрая и удобная настройка
двухфакторной аутентификации
в доменной инфраструктуре
и корпоративной сети

Реализация 2FA
на основе Рутокен

#1 фактор –
владение физическим токеном,
который нужно подключить к ПК

#2 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

Функциональные возможности: устройства

- 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)
- Проверка сертификата: CRL или OCSP-сервер

Поддерживаемые среды

ОС:

- **Astra Linux** 1.7, 1.8 (включая режим «Смоленск»)
- **ОС Альт** 10/11/СП 8 релиз 10
- **РЕД ОС** 7.3, 8

ASTRA LINUX®

base alt

РЕДСОФТ

Архитектуры ОС — x86 и ARM

Домены:

- **Active Directory**
- **ALD Pro**
- **РЕД АДМ 2.0**
- **FreeIPA**
- **SambaDC**

Функциональные возможности: автоматизация

- Командно-строчный интерфейс (CLI)
  ~ в 10 раз быстрее настройка, чем вручную
- Скрипты для быстрого ввода компьютера в различные домены
- Скрипты для развертывания и настройки продукта на рабочих местах
- Интеграция с Рутокен KeyBox

Что нужно для внедрения MFA

#1 Домен

#2 Рабочие места с ОС Linux

#3 Рутокен Логон для Linux

#4 Рутокен ЭЦП 3.0
для каждого сотрудника

#5 Инфраструктура
открытых ключей (PKI)

#6 (Опционально) Рутокен KeyBox

#7 (Опционально) IAM-система

Демонстрация

Кейсы

Единая 2FA в смешанной Windows/Linux среде

Заказчик

Предприятие химической промышленности

50/50 : Linux/Windows
>1 500 рабочих мест

Инструменты

- Штатные средства для Windows
- Рутокен Логон для Linux
- Рутокен KeyBox для управления циклом сертификатов

Результат

- Единый 2FA по токену
- Централизация: выпуск/контроль сертификатов и PIN удаленно
- Снижение нагрузки на админов
- Масштаб для гетерогенной среды

Защита данных в географически распределённых подразделениях

Заказчик

Госорганы

- Linux-инфраструктура и отечественный домен
- Десятки тысяч станций по всей России
- Работа с ПДн, финансами и стратегическими проектами

Инструменты

- Рутокен Логон для Linux
- SafeTech CA - выпуск сертификатов
- Рутокен KeyBox для управления циклом сертификатов

Результат

- Вход по PIN + токен
- Удаленное управление ключами
- Контроль PIN/сертификатов

Преимущества решения Рутокен Логон

Для администратора	Для руководства	Для пользователей
Экономия времени на внедрение	Повышение уровня безопасности	Единый удобный интерфейс
Меньше запросов на обслуживание пользователей	Выполнение требований регуляторов	Короткий PIN вместо длинных комбинаций

Развитие продукта

Функция	v.1.0.0	v.1.0.5	v. 1.1.0
Поддержка **Рутокен БИО**	–	–	✔
Поддержка **OTP**	–	✔	✔
Поддержка ОС **ROSA** XPOM	–	✔	✔
Поддержка ОС **Альт 11**	незначительные ограничения	✔	✔
Поддержка ОС **Основа**	–	–	✔
Поддержка КД **РЕД АДМ**	незначительные ограничения	✔	✔
Поддержка КД **Альт Домен**	–	✔	✔
Поддержка КД **ROSA Dynamic Directory**	–	✔	✔
Инструменты для диагностики инфраструктуры	–	–	✔
Кастомизация интерфейса	–	✔	✔

Ваши вопросы

Контакты

КОМПАНИЯ АКТИВ

presale@rutoken.ru

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

Кирилл Аверченко

Руководитель
технического пресейла

Михаил Моисеев

Эксперт по аутентификации

РУТОКЕН