

РУТОКЕН

КОМПАНИЯ
ПРАКТИВ

Как минимизировать
компрометацию
идентификаторов при работе
с информационными системами



Главная угроза безопасности информационных систем – компрометация идентификаторов



Происходит по трём основным причинам:

#1

**Передача
идентификаторов**
третьим лицам
с раскрытием PIN-кода

#2

Кража идентификаторов
с PIN-кодом
по умолчанию

#3

Потеря идентификаторов
с PIN-кодом
по умолчанию

Последствия компрометации идентификаторов

Финансовые риски

- Незаконные переводы денежных средств
- Оформление кредитов и займов
- Мошеннические операции с активами

Репутационные потери

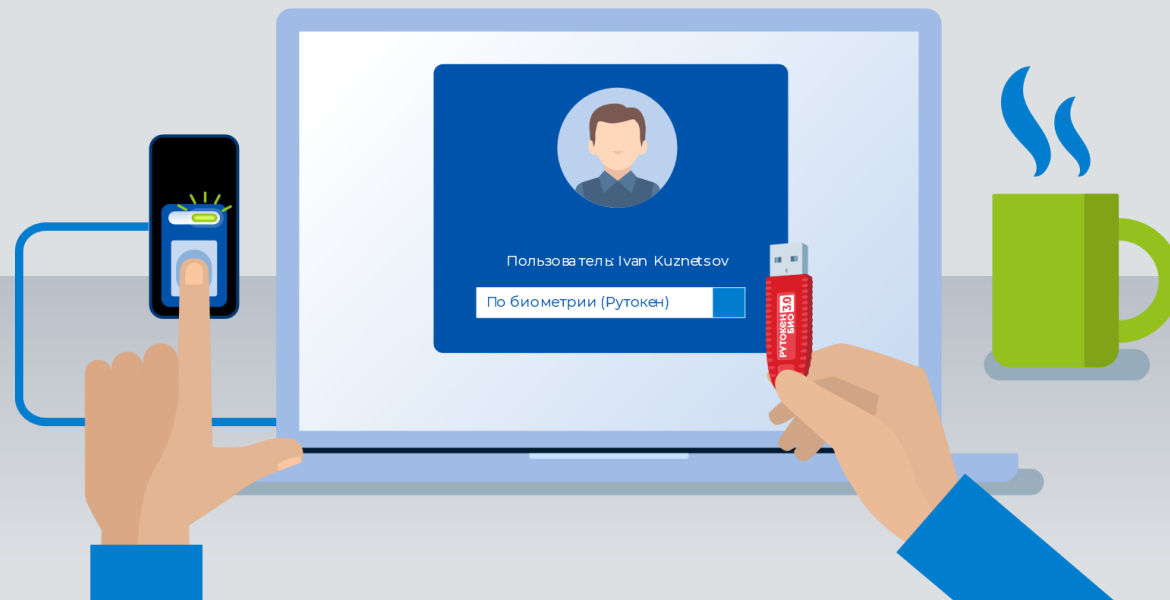
- Ущерб деловой репутации
- Нарушение доверия партнёров
- Сложности с восстановлением доброго имени

Юридические последствия

- Ответственность за действия злоумышленников
- Судебные разбирательства
- Сложности с доказательством невиновности

Решение

Рутокен ЭЦП 3.0 3250 –
это биометрическое решение
для безопасной аутентификации
пользователей. Обеспечивает
дополнительную защиту и удобство
использования



Как это
работает?

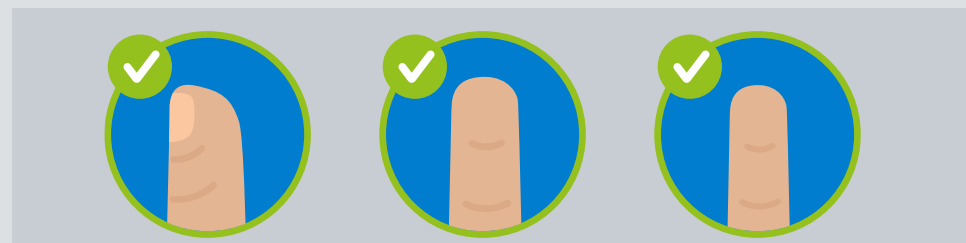
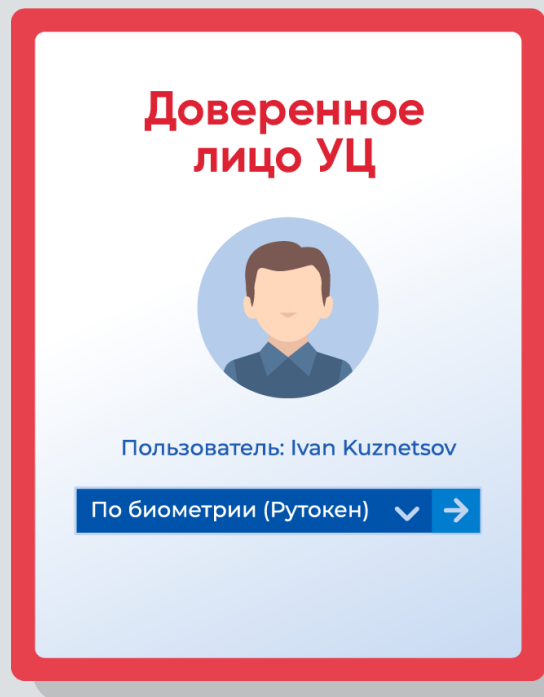


Этап 1: запись биометрических данных и выдача устройств

АРМ Администратора безопасности –
регистрация биометрии в Рутокен ЭЦП 3.0 3250



- 1 Отпечатки трех пальцев владельца устройства
- 2 Сертификат УЦ для аутентификации в ИС



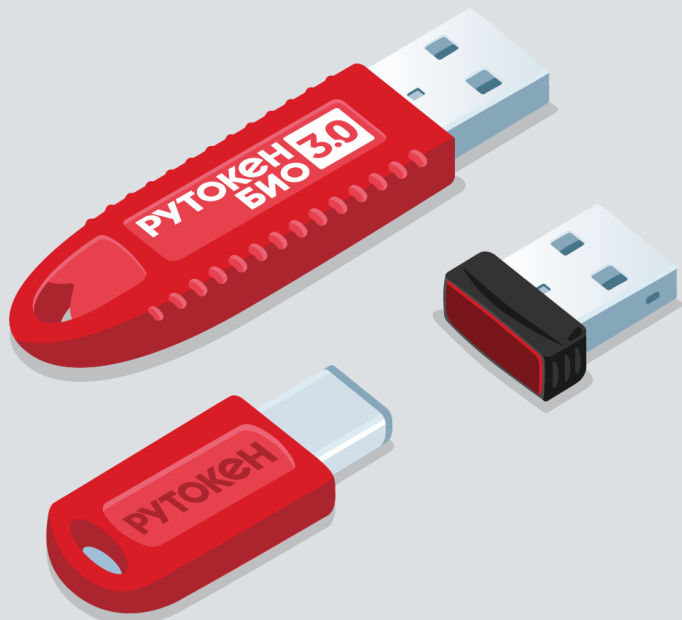
Сбор отпечатков с трех разных пальцев
легитимного пользователя Рутокен



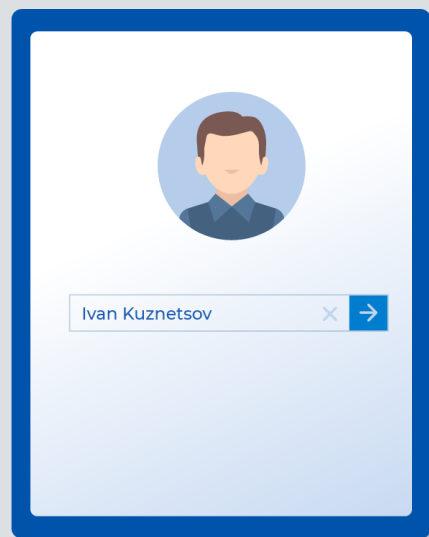
Запись сертификата
аутентификации
и привязка биометрии

Этап 2: трехфакторная аутентификация в информационные системы

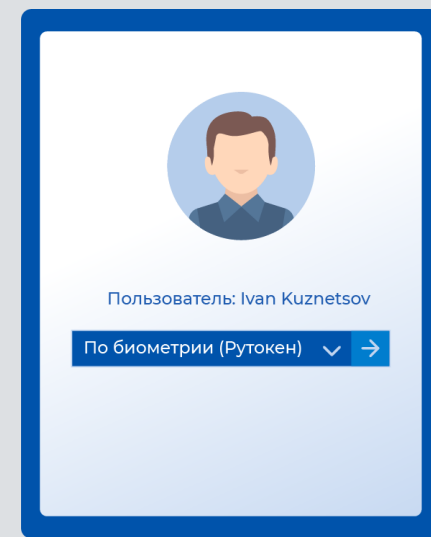
Новое поколение средств аутентификации по отпечатку пальца



Устройства доступны в разных форм-факторах и с разным интерфейсом



Ввод имени пользователя



Выбор биометрического способа входа



Этап 2: трехфакторная аутентификация в информационные системы

Трехфакторная аутентификация в информационные системы



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

*Настраиваемая политика качества PIN-кодов в устройствах Рутокен ЭЦП 3.0 предотвращает использование владельцем простых PIN-кодов, в том числе значения PIN по умолчанию.



Принцип и особенности работы биометрического механизма в Рутокен ЭЦП 3.0 3250



Доступ к закрытому ключу предоставляется только при предъявлении отпечатка зарегистрированного пальца и PIN-кода



Верификация биометрических данных происходит полностью на борту устройства



Механизмы заложенные в архитектуру операционной системы Рутокен:



Отпечатки привязываются к конкретной ключевой паре



После инициализации не допускается извлечение, изменение или удаление отпечатков из устройства

Принцип и особенности работы биометрического механизма в Рутокен ЭЦП 3.0 3250



Механизмы устойчивости к атакам и улучшения **пользовательского опыта**

В состав драйверов устройств Рутокен ЭЦП 3.0 с биометрическими механизмами входят две предобученных нейросети

1 Нейросеть «КПП» Контроль качества прикладывания пальца



Нейросеть распознает качество прикладывания пальца, отсекает случаи когда предъявлен частичный отпечаток или палец приложен недостаточно плотно — в таком случае требуется повторить прикладывание.

**Ошибка первого рода (FAR)*:
< 0.001 %**

Вероятность ложноположительного срабатывания алгоритма

Ошибка второго рода (FRR):
< 3 %**

Вероятность ложноположительного срабатывания алгоритма

2 Нейросеть «Антифейк» Выявление недостоверных отпечатков пальца



Реальный
отпечаток



Силиконовая
накладка



Нейросеть отличает реальные отпечатки пальцев от любых разновидностей подделок: силиконовые наклейки, слепки из эмульсии алифатической смолы, кустарные копии пальца из пластилина типа «play-doh», желатиновые слепки и другие.

*, ** Значения FAR и FRR являются ориентировочными статистическими величинами и прямо зависят от качества тестовой базы отпечатков пальцев, на которой производится замер вероятностей.

Почему использовать Рутокен с биометрией удобно



Уникальное сочетание биометрической и криптографической защиты

- Интеграция биометрии и токенов в единое решение



Гибкость в интеграции с существующими IT-инфраструктурами

- SDK в свободном доступе
- Поддержка различных сканеров отпечатков пальцев



Соответствие требованиям регуляторов, таких как ФСТЭК и ФСБ

- Сертификат ФСБ России
- Сертификация ФСТЭК (планируется в следующем году)



Отсутствие необходимости выстраивания взаимодействия с ЕБС