

Аутентификация в информационных системах с использованием биометрических данных

Усиление двухфакторной аутентификации с применением USB-токенов.

Существующие угрозы:

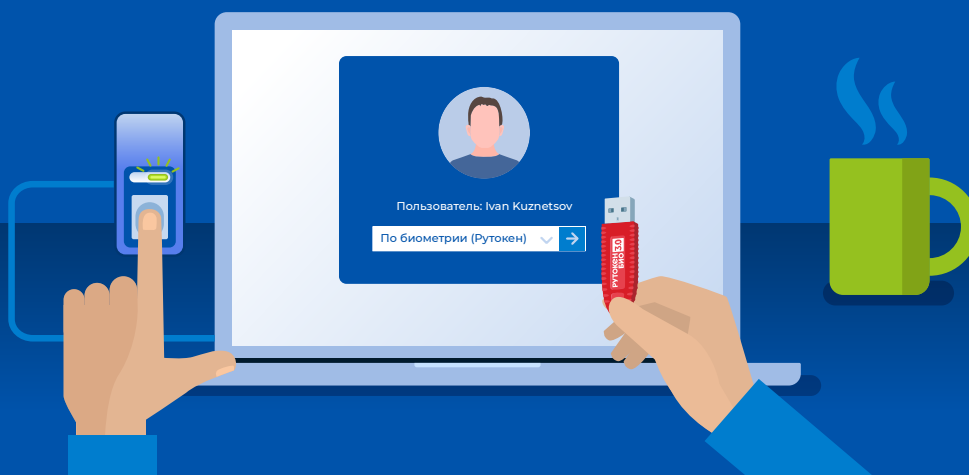


- случайная утеря токена вместе с использованием PIN-кода по умолчанию может привести к компрометации процесса входа в систему и допуска в нее посторонних лиц.
- сознательная передача устройства третьим лицам может привести к несанкционированному доступу к чувствительной информации.



Решение:

надежная «привязка» устройства для аутентификации к его владельцу посредством использования биометрических данных (отпечатков пальцев легитимного пользователя токена).



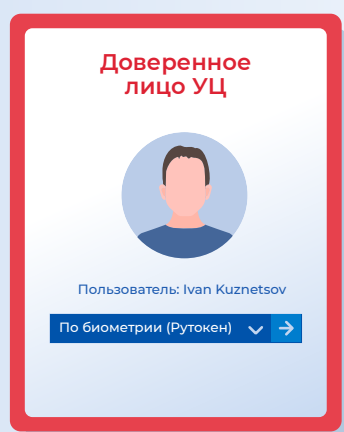
Этап 1 — выдача устройств и запись биометрических данных

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

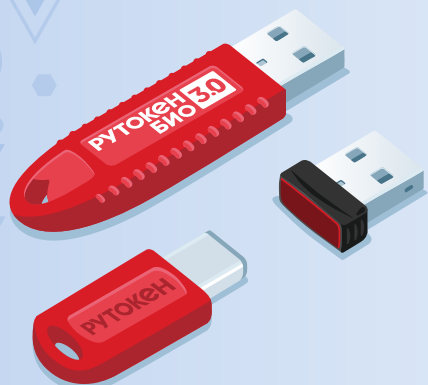


Запись сертификата аутентификации и привязка биометрии

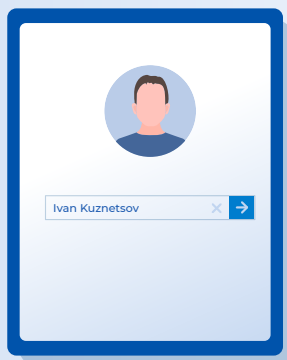
РУТОКЕН

Новое поколение средств аутентификации по отпечатку пальца

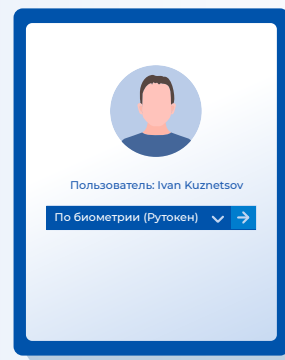
Этап 2 — трехфакторная Аутентификация в информационных системах



Устройства доступны в разных форм-факторах и с разным интерфейсом



Ввод имени пользователя



Выбор биометрического способа входа

Трехфакторная аутентификация в информационные системы



Фактор владения

Защищенное сертифицированное устройство для хранения сертификата аутентификации



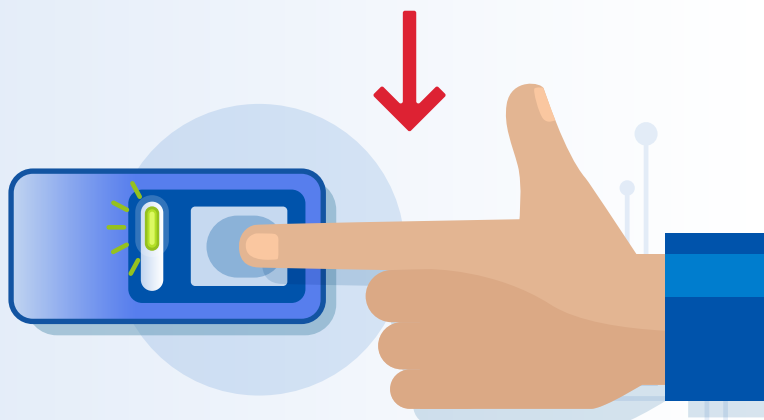
Фактор знания

Персональный PIN-код для доступа к устройству с политикой качества*



Фактор свойства

Отпечаток пальца — уникальное свойство владельца устройства



Предъявление отпечатка одного из зарегистрированных пальцев



Ввод PIN-кода и успешный вход в систему

*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



Формирование шаблонов*

При занесении отпечатков происходит их анализ и математическая обработка

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

Инициализация устройства

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



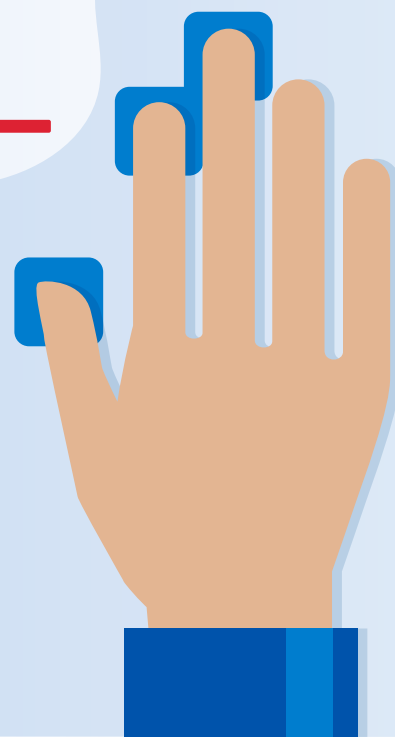
Сбор биометрических данных

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

*Накопительный адаптивный анализ минучий («точек Гальтона») с четырех вариантов отпечатка повышает точность распознавания



Применение триангуляции Делоне обеспечивает устойчивость алгоритма распознавания к углу поворота пальца на считывателе до 60°



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.

Преимущества:

- + У пользователя вырабатывается привычка корректно прикладывать палец, улучшая его опыт
- + Отсечение «плохих» отпечатков до отправки в Рутокен увеличивает скорость аутентификации и снижает количество отказов во входе

Нейросеть отличает реальные отпечатки пальцев от любых разновидностей подделок: силиконовых накладок, слепков из эмульсии алифатической смолы, кустарных копий пальца из пластилина типа «play-doh», желатиновых слепков и других.

2 Нейросеть «Антифейк»

Выявление недостоверных отпечатков пальца



Реальный отпечаток



Силиконовая накладка



Ошибка первого рода (FAR)*:
< 0.001 %

Вероятность ложноположительного срабатывания алгоритма

Ошибка второго рода (FRR):**
< 3 %

Вероятность ложноотрицательного срабатывания алгоритма

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