НИИ ВОСХОД

Технология дистанционной идентификации личности в УЦ с использованием заграничного паспорта

Чижевский Игорь

НИИ «Восход»

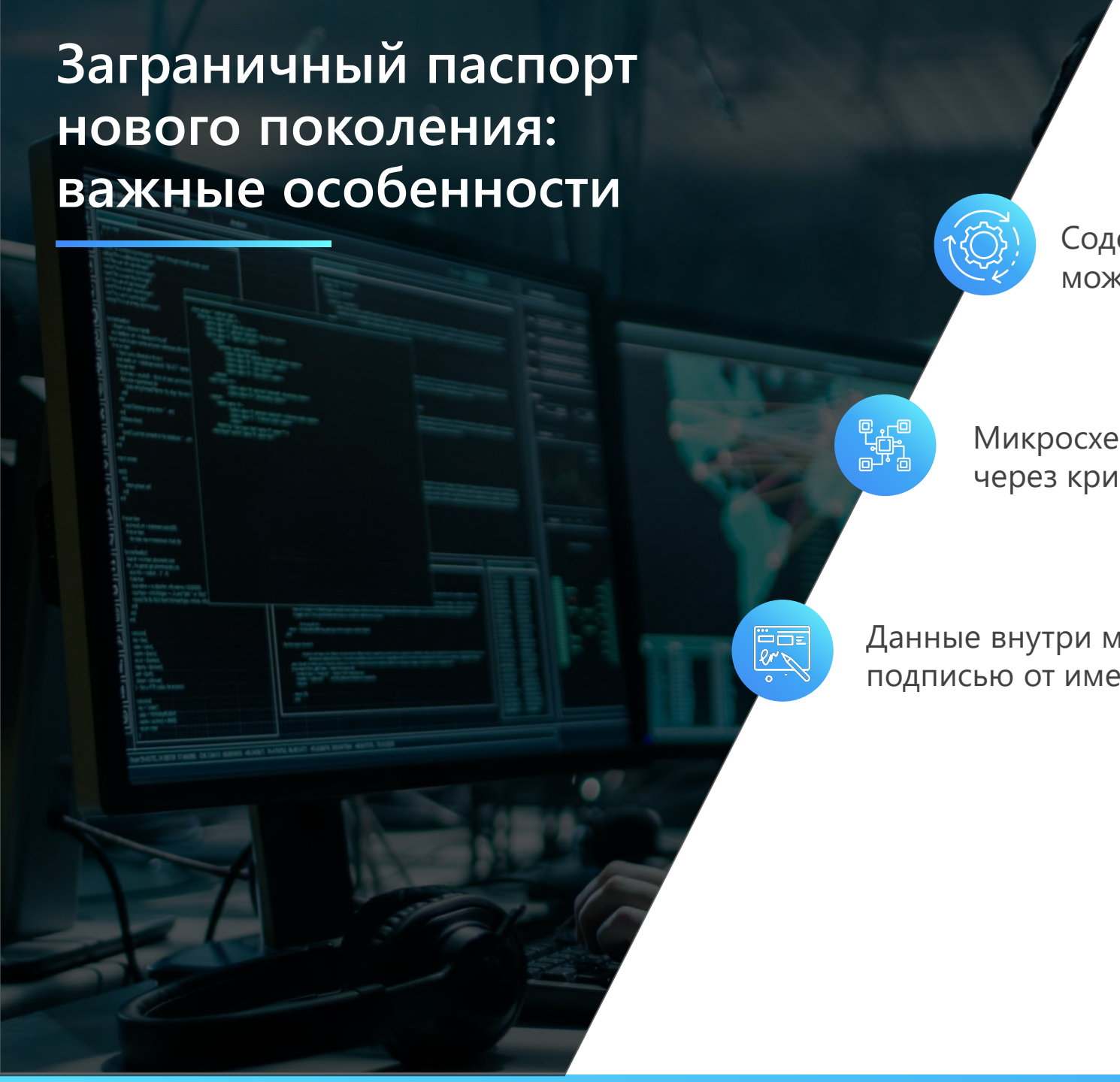
Изменения в 63-ФЗ

Статья 18, пункт 1

1. УЦ может идентифицировать заявителя — физическое лицо — без личного присутствия, путём предоставления информации из заграничного паспорта с электронным носителем

2. Также возможна идентификация по ЕСИА и ЕБС

Заграничный паспорт нового поколения: важные особенности



- Содержит микросхему, работающую через RFID: можно взаимодействовать через смартфон
- Микросхема — не просто флешка, взаимодействие через криптографический протокол
- Данные внутри микросхемы подписаны электронной подписью от имени Российской Федерации (КВ2)

Криптографические протоколы микросхемы загранпаспорта

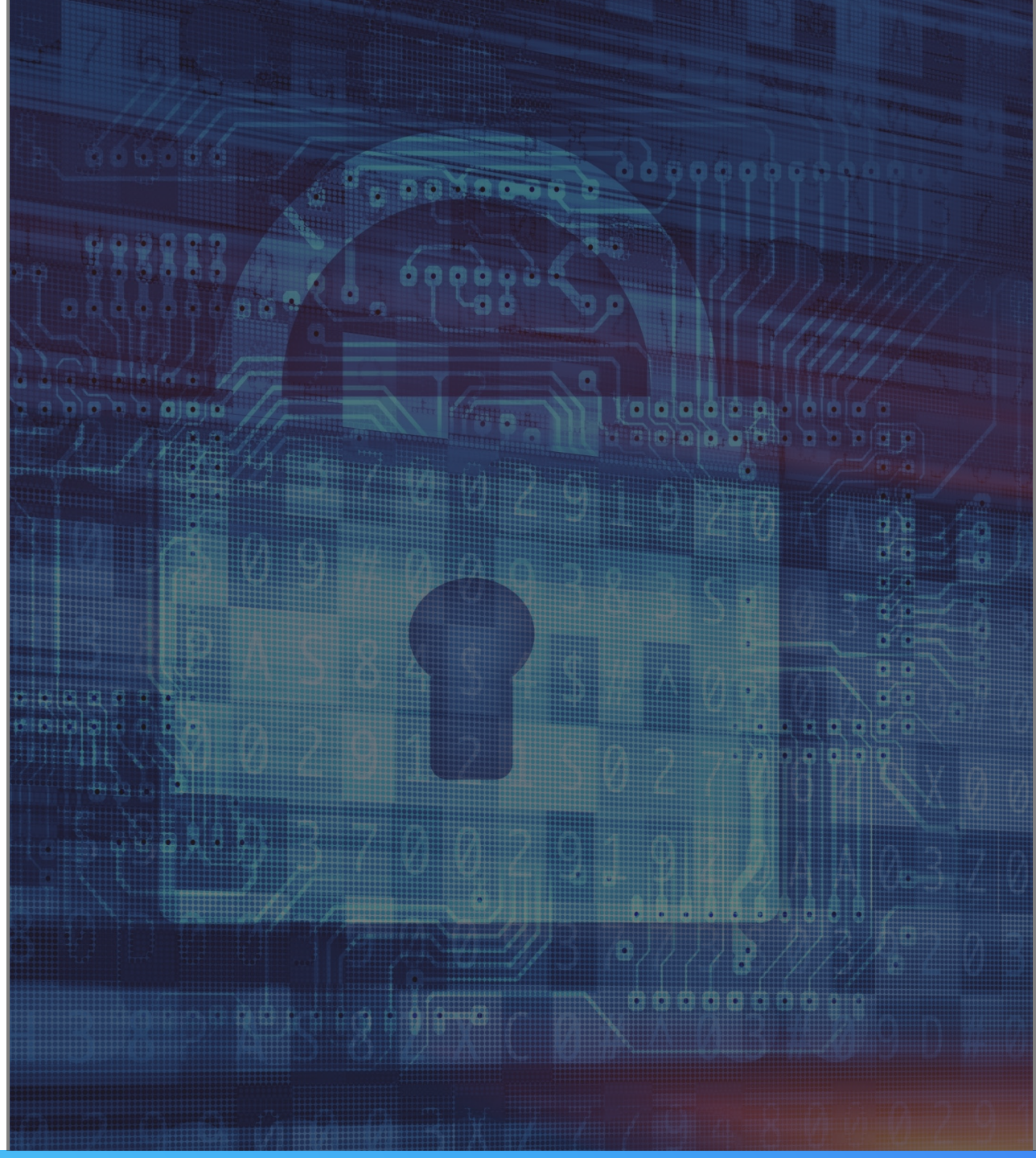
1 BAC: базовый контроль доступа:

- Иностранная криптография (Triple DES)
- Ключ на основе пароля, состоящего из номера паспорта, даты рождения владельца, даты окончания срока действия документа
- Задача — защита от чтения паспорта в кармане

2 EAC: расширенный контроль доступа:

- Есть криптография по ГОСТ
- Выработка сеансового ключа с использованием алгоритма согласования VKO и диверсификации ключа KDF
- Защита от клонирования: микросхема содержит неизвлекаемый закрытый ключ, владение которым доказывает
- Открытый ключ подписан ЭП Российской Федерации
- Аутентификация микросхемы, опционально — аутентификация терминала

3 Документация: DOC ICAO 9303



Какие данные есть в микросхеме загранпаспорта

Метрические

- Дата рождения владельца
- Фамилия и имя на латинице
- Номер документа
- Дата окончания срока действия

Биометрические

- Фотография
- Отпечатки пальцев (с 2015 года)

Можно ли использовать отпечатки пальцев?

- Чувствительная информация: требуется аутентификация терминала
- Верификация на смартфонах невозможна

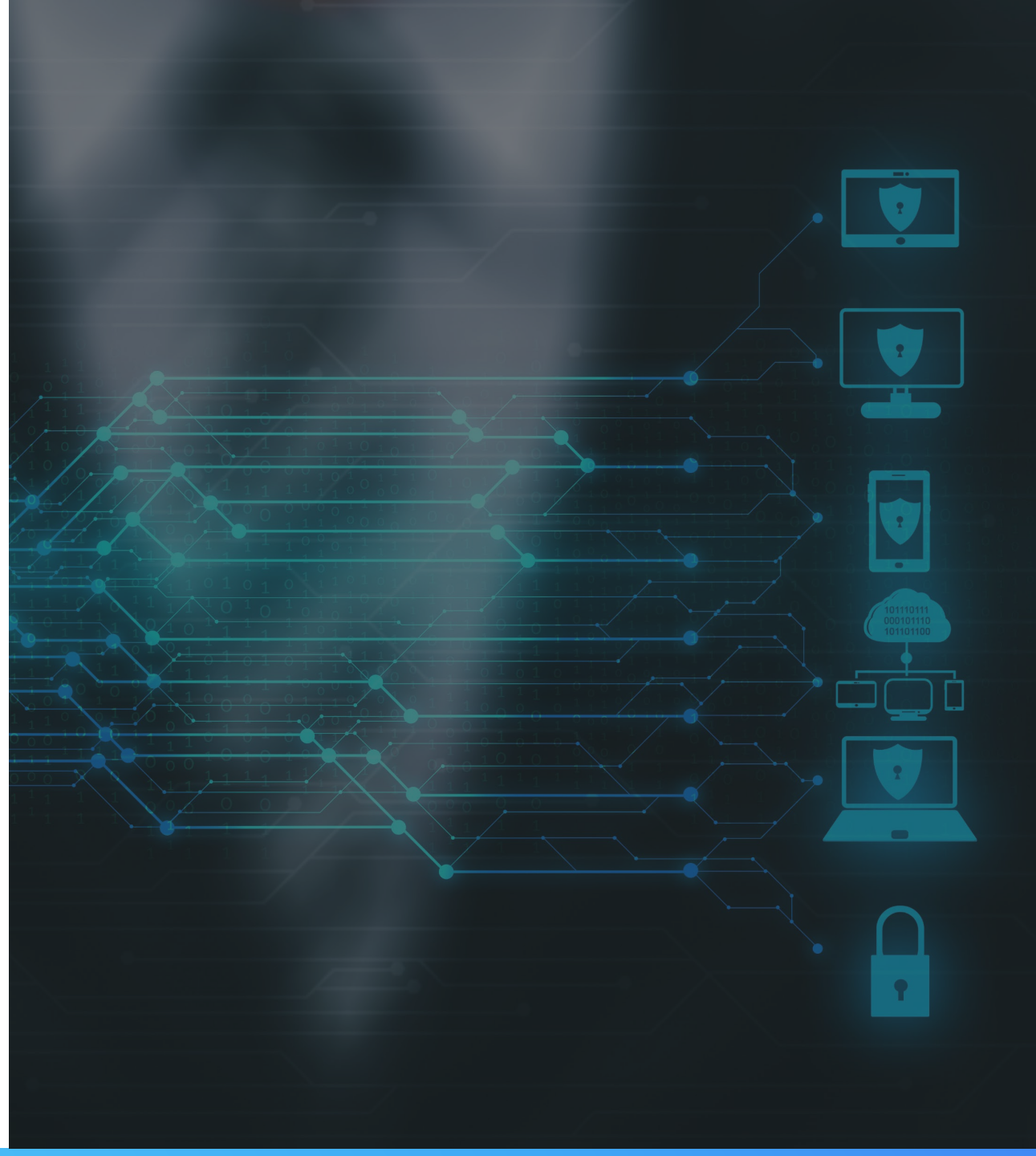
BAC, EAC, микросхема… Всё делать самим?

1 Можно сделать самим, документация открыта, паспорт соответствует международному стандарту + ГОСТ для криптографии

2 Можно воспользоваться государственным сервисом

Служба распределенного терминала

- Уже реализованы все криптопротоколы работы с микросхемой
- Предоставляет мобильное приложение, не надо делать самим работу с NFC
- Сама реализует верификацию подписи Российской Федерации, решая вопросы корневых сертификатов и списков отзыва УЦ эмиссии и контроля
- **Проверяет, не был ли паспорт аннулирован**



Как с этим работать?

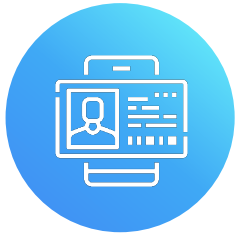
1. Сначала — **аутентификация в ЕСИА**
2. **Передаём** со стороны УЦ **данные заявителя**: фамилию и имя на кириллице, дату рождения
3. **Заявитель читает загранпаспорт** через специальное приложение на смартфоне
4. **УЦ получает результат,** верифицирована личность или нет
5. Внутри — **чтение паспорта по криптопротоколу, проверка электронной подписи, проверка на аннулированность, проверка на совпадение данных**

Ложечка дёгтя

- В микросхеме загранпаспорта — только фамилия и имя, без отчества, и только на латинице (так исторически сложилось)
- Эталона транслитерции нет, гражданин может попросить скорректировать при выдаче паспорта
- Транслитерация не имеет однозначного обратного преобразования
- Проверяем расстояние Левенштейна

Текущий статус

Завершаем разработку, передаём на проведение тематических исследований

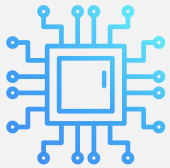


Есть прототип, можно пробовать интегрироваться для проведения тестирования

Есть примеры успешных интеграций

Дальнейший план — Минцифры

Перспективы



Новая микросхема заграничного паспорта:

- SESPAKE
- ГОСТ 2012
- Возможно, данные на кириллице

Паспорт гражданина России с электронным носителем

Осторожно!

! Для граждан:

- Никогда не теряйте заграничный паспорт!
- Потеряли – сразу аннулируйте!
- Сделайте надёжным пароль от учетной записи в ЕСИА

! Для УЦ:

- Проверка по ЕСИА – обязательна!

Вопросы

НИИ ВОСХОД

+7 (495) 981-88-99
voskhod.ru
info@voskhod.ru