Доверенные сервисы идентификации и аутентификации. Качество идентификации как один из источников злоупотреблений на рынке электронной подписи

Сабанов Алексей Геннадьевич,
к.т.н., доцент МГТУ им. Баумана,
Эксперт ISO/C1/SC27/WG5,
Член ТК 362, РГ ТК 26, ТК 122
Зам. ген. директора ЗАО "Аладдин Р.Д."

Что такое доверенный сервис

Доверенный сервис - сервис безопасности, квалифицированный по определенному уровню доверия

уровень доверия (assurance level): степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия. Степень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.

метод обеспечения доверия: общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

доверие (assurance): выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

уверенность (confidence): убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно, в соответствии с политикой безопасности)

ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005, пункты 2.4,10,11,18).

Проблемы идентификации и аутентификации

- **Нормативно-правовые**: ни в одном документе не содержится технических требований к процессам и системам идентификации и аутентификации. На гос.уровне не имеется документов уровня Указа Президента, ФЗ. (Примеры: OMB Memorandum 04-04 2003, Homeland Security Presidential Directive 12- 2004г. Identification Standard, Стратегия по аутентификации 2010г.)
- **Организационные**: нет единого Заказчика со сбалансированными в сфере ИБ требованиями, недостаточно специалистов по идентификации и аутентификации, командуют юристы и экономисты – нет технических требований
- **Образовательные**: учебники быстро устаревают, нет лабораторных работ
- **Научные**: нет общепринятых методов и моделей исследования, мало исследований процессов и систем идентификации и аутентификации. Отдельный научный интерес вызывают большие ИС и применение биометрии

Роль идентификации и аутентификации в PKI

- Идентификация и аутентификация (ИА) – сервисы безопасности на базе PKI, обеспечивающие совместно с другими сервисами (штампы времени, проверка валидности цифровых сертификатов, электронная подпись, проверка полномочий, доверенная гарантированная доставка сообщений и документов) определенный уровень доверия к электронным транзакциям, сообщениям и документам;
- ИА должны обеспечивать определенный уровень доверия к определению лица, подписавшего документ. Для этого требуется корректное решение задачи доступа субъекта прикладному ПО, из которого поступает вызов СКЗИ для подписи документа;
- ИА совместно с волеизъявлением при подписании документа, наличия штампа времени и проверки полномочий позволяет решить задачу неотказуемости подписи.

Виды идентификации

- Идентификация включает первичную идентификацию, проводимую в момент регистрации нового субъекта доступа в ИС, и вторичную идентификацию (регулярно повторяющуюся), выполняемую при каждом новом запросе на доступ.
- Первичная идентификация субъекта доступа может являться одновременно частью как процесса идентификации, так и процесса аутентификации (если используется процесс аутентификации).

Первичная идентификация

- Целью первичной идентификации является обеспечение отсутствия коллизий представленной заявителем для целей включения в состав пользователем ИС от другой (принадлежащих другим пользователям данной ИС) идентификационной информации (ИИ), имеющейся в данной ИС.
- Полнота и строгость проверки представленной заявителем ИИ определяется политикой безопасности оператора ИС.
- Первичная идентификация должна завершаться регистрацией (присвоением новому пользователю уникального идентификатора в данной ИС) или обоснованным отказом. Причиной отказа может являться недостаточный объем подтверждённой ИИ. Объём связанной с новым пользователем необходимой ИИ определяется политикой безопасности оператора ИС.
- Первичная идентификация должна ответить на вопрос: тот ли это субъект, за кого себя выдает? и определить возможность регистрации данного субъекта или объекта в конкретной ИС.

ISO/IEC 29003 Уровни доверия к идентификации

Уровень подтверждения идентификационных данных	**Описание**	**Цель**
1-й уровень подтверждения идентификационных данных	Низкая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и имеется предположение о существовании идентификационных данных и субъект предположительно привязан к идентификационным данным.
2-й уровень подтверждения идентификационных данных	Средняя уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и умеренное установление существования идентификационных данных[a] и у субъекта есть некоторая привязка к идентификационным данным.
3-й уровень подтверждения идентификационных данных	Высокая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и строгое установление существования идентификационных данных[a] и у субъекта есть сильная привязка к идентификационным данным.

[a] Понятие требует совпадения значений идентифицирующего атрибута со значениями свидетельства идентичности.

ISO/IEC 29003 Требования к подтверждению

Минимальные требования к уровню подтверждения идентификационных данных относительно привязки идентификационных данных к субъекту

Цель	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	3-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны к субъекту	Привязка к идентификационным данным не проверяется.	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя один фактор.	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя два или более факторов.

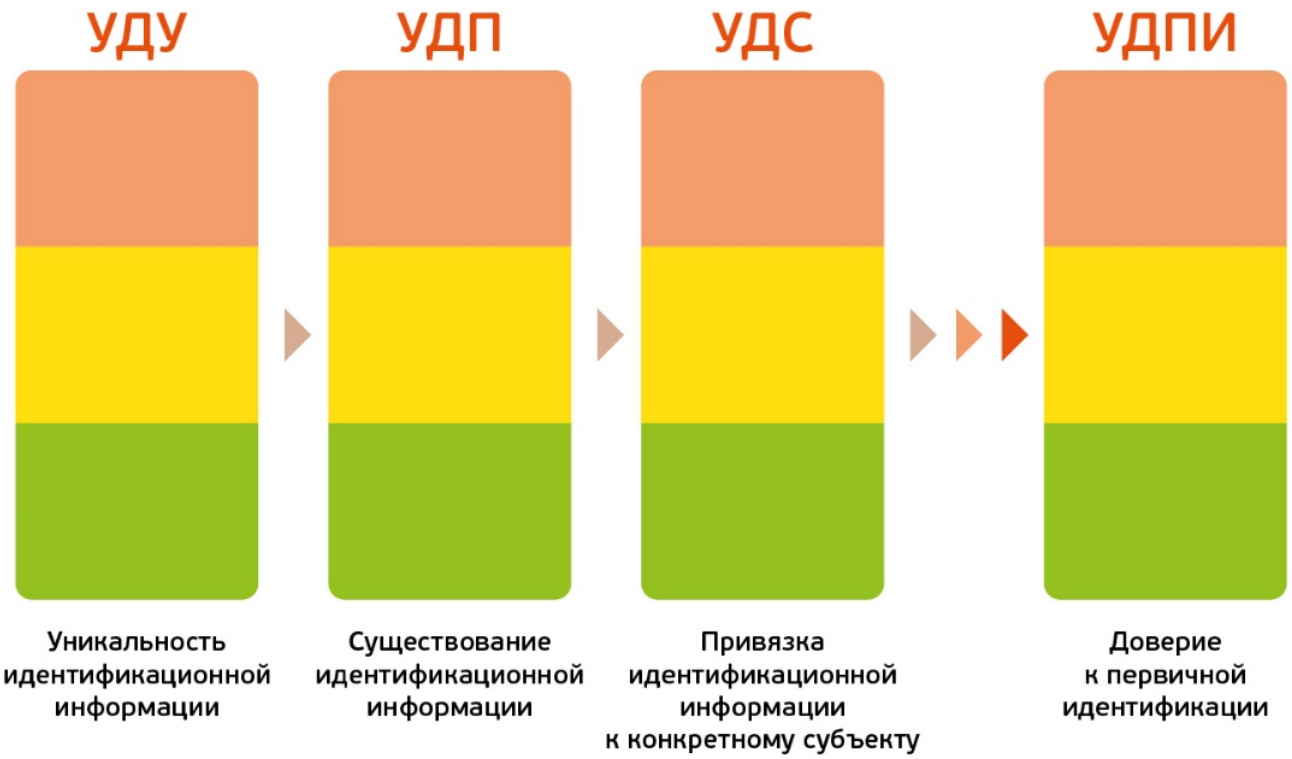
ISO/IEC 29003 Существование и привязка

	Идентификационные данные существуют на 1-м уровне подтверждения идентификационных данных	**Идентификационные данные существуют на 2-м уровне подтверждения идентификационных данных**	**Идентификационные данные существуют на 3-м уровне подтверждения идентификационных данных**
Идентификационные данные привязаны на 1-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 2-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 3-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	3-й уровень подтверждения идентификационных данных

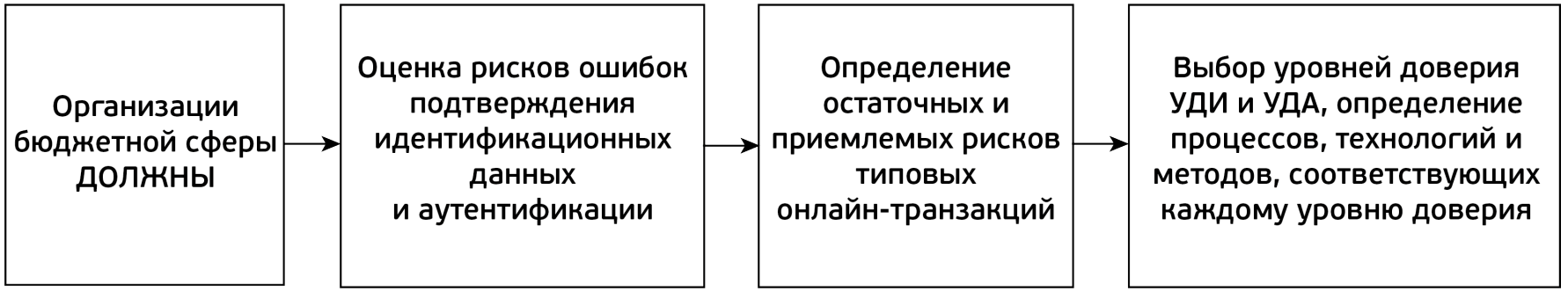
Характеристики доверия к результату первичной идентификации

Первичная регистрация субъекта (объекта) доступа			Допущения, определяемые правилами управления доступом	Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным	Уровень доверия к результатам первичной идентификации	Возможность регистрации субъекта (объекта) доступа
Уникальность идентификационной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных	Привязка идентификационных данных				
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Необходимо подтверждение идентификационных данных	Нет никакой уверенности	Доверие к идентификационным данным отсутствует	Отказ в регистрации субъекта (объекта) доступа
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Отсутствует необходимость подтверждения идентификационных данных	Нет никакой уверенности	Доверие к идентификационным данным отсутствует	Регистрация субъекта (объекта) доступа как «анонима»
Уникальность обеспечивается	Существование идентификационных данных не проверяется	Привязка идентификационных данных не проверяется	Необходимо подтверждение идентификационных данных	Некоторая уверенность	Низкий уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование идентификационных атрибутов и достоверность их значений в подтверждающих свидетельствах	Привязка идентификационных данных с использованием одного фактора	Необходимо подтверждение идентификационных данных	Умеренная уверенность	Средний уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование идентификационных атрибутов и достоверность их значений в официальных свидетельствах	Привязка идентификационных данных с использованием не менее двух факторов	Необходимо подтверждение идентификационных данных	Высокая уверенность	Высокий уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа

Формирование уровней доверия к результатам первичной идентификации



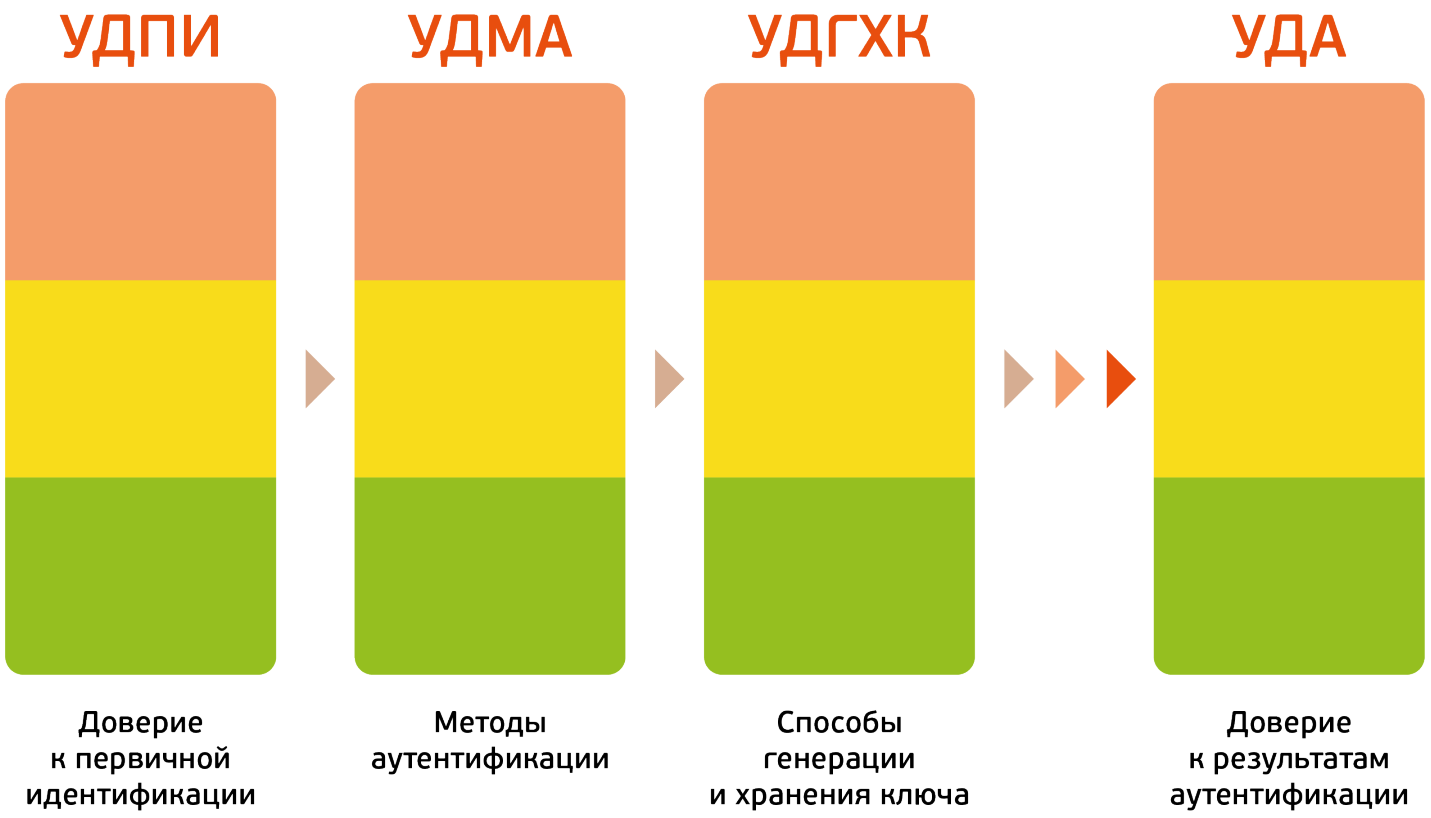
Выбор уровней доверия по NIST SP 800-63-3



Критерии доверия к результатам идентификации

1. **достоверность** (полнота, точность, аутентичность и степень связанности с заявителем) результатов; при этом проверяется подлинность бумажных документов и соответствие данных с е-реестрами;
2. функциональная **надежность** работы системы идентификации;
3. выполнение в процессе первичной идентификации требований **информационной безопасности**, в том числе в отношении персональных идентификационных данных субъектов доступа.

Уровни доверия к результатам аутентификации



Общая характеристика уровней доверия к результатам аутентификации по методам аутентификации

Метод аутентификации субъекта (объекта) доступа			Вид аутентификации субъекта (объекта) доступа	Уверенностью в том, что субъект и (или) объект доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за кого себя выдает	Уровень доверия к результатам аутентификации субъекта (объекта) доступа
Однофакторная аутентификация	Односторонняя аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Простая	Некоторая уверенность	Низкий уровень доверия
Многофакторная аутентификация	Односторонняя или взаимная аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Усиленная	Умеренная уверенность	Средний уровень доверия
Многофакторная аутентификации	Взаимная аутентификация	Криптографические протоколы аутентификации	Строгая	Высокая уверенность	Высокий уровень доверия

Уровни доверия к методам аутентификации

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от известных атак	односторонний	знание	низкий
2	сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	одноразовый пароль	доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	односторонний	владение	
3	"второй канал" (пример: телефон+SMS)	одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение	средний
4	устройство одноразовых паролей, динамически генерирующее OTP	одноразовый пароль	защита устройства	односторонний	владение	
5	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия	высокий
6	криптографическй ключ в СВТ или на незащенном паролем носителе	криптографические ключи	защита ключей	односторонний или взаимный	владение	
7	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание	
8	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	очень высокий
9	СВТ с криптографическим ПО и отдельное устройство с помещённым в него и хранящемся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия	
10	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия	самый высокий

Доверие к результатам идентификации и аутентификации

	Низкий уровень доверия к результатам идентификации	Средний уровень доверия к результатам идентификации	Высокий уровень доверия к результатам идентификации
Низкий уровень доверия к результатам аутентификации	Низкий уровень доверия	Низкий уровень доверия	Низкий уровень доверия
Средний уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Средний уровень доверия
Высокий уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Высокий уровень доверия

Задачи УЦ

- Обеспечение жизненного цикла сертификатов ключа проверки электронной подписи клиентов
- Обеспечение пространства доверия к открытым ключам и квалифицированной электронной подписи
- Построение систем доверия с применением сервисов безопасности на базе инфраструктуры открытых ключей
- Определение личности обратившегося за сертификатом ключа проверки подписи

Одни из главных причин мошенничеств с ЭП

1. Подавляющая часть злоупотреблений связана с некачественной первичной идентификацией будущего клиента УЦ (принимают копию паспорта, не проверяют его действительность и подлинность)

2. Несовершенство законодательства (имеются факты привода в УЦ сомнительных личностей без определенного занятия, выдача средств ЭП и СКЭП по доверенности)

3.Неосторожное обращение со средствами ЭП и закрытым ключом

4. Корректность вызова ЭП из прикладного ПО

Что такое качество идентификации

По материалам ISO это прежде всего:

1. Надежность работы системы
2. Безопасность обрабатываемой информации, прежде всего, ПДн
3. Доверие к полученным результатам идентификации (уровни доверия)

Требования ISO:

- Secure by Design
- Privacy by Design

21 защитный признак паспорта

1. Защита бумаги – 4 признака. Трехтоновый водяной знак в виде букв «РФ», регулярно повторяющийся по всей поверхности страницы;

Защитные волокна 3-х типов

2. Полиграфическая защита (способы печати) – 8 признаков

Фоновая сетка печатается с ирисовым раскатом - цвет линий сетки плавно меняется от одного края страницы к другому

• рельефная фоновая сетка, выполненная офсетной печатью (все страницы бланка, кроме первой и последней)/контролируется с помощь лупы.

• металлографская печать:

• изображение Кремля и виньетки на переднем форзаце и др.

3. Защита на ламинирующей пленке – 2 признака

Между стр. 2 и 3 паспорта вшита специальная защитная ламинирующая пленка (холодного или горячего тиснения). В местах прилегания пленки к левому и верхнему краю фотографии и по обеим сторонам от прошивки на внутренней стороне ламината нанесен узор из линий красного цвета, который в процессе тиснения переходит на бумагу / контролировать с помощью лупы отсутствие разрывов и смещений красных линий по краю фотографии и в районе прошивки..

4. Защитные элементы, люминесцирующие в УФ-лучах – 6 признаков

Контролируется с помощью приборов «Ультрамаг-5СЛГ», «Ультрамаг-А36М», «Ультрамаг-С6ВП» в режиме УФ-подсветки. При подсветке ультрафиолетовыми лучами:

• бумага бланка паспорта выглядит темно-синей, наблюдается свечение защитных волокон (описаны выше);

• светится желто-зеленым свечением краска рамки переднего форзац,…

5. ИК-защита

При исследовании бланка паспорта в инфракрасном диапазоне спектра, на первой и последней страницах наблюдается только часть изображения, видимого при обычном освещении / Контролируется с помощью прибора «Ультрамаг-С6ВП» в режиме проверки ИК-зашиты.

Подделка 3-ей страницы паспорта

1. Отслаивание ламината, замена имеющейся фотокарточки на новую фотокарточку и повторное ламинирование.
2. Вырезание фотокарточки и наклеивание на ее место новой с новым ламинатом.
3. Наклеивание на третью страницу паспорта (поверх ламината, фотокарточки и установочных данных) листа бумаги с имитированными реквизитами, фотокарточки и ламинирование новым ламинатом.
4. Удаление ламината, фотокарточки и поверхностного слоя бумаги с установочными данными, нанесение на бумагу имитированных изображений бланка, фотокарточки, установочных данных и ламинирование новым ламинатом.
5. «Расшивка» паспорта, удаление имеющегося листа и «вшивка» нового листа с имитированными реквизитами бланка, установочными данными, фотокарточкой и ламинатом.

Спасибо за внимание!

asabanov@mail.ru
+7-985-924-52-09