

АНАЛИТИЧЕСКИЙ ОТЧЕТ

Исследование актуальных угроз мошенничества с использованием поддельных документов

2019-2023 гг

+ Чек-лист: как выбрать ИИ-решение
для безопасной идентификации?

Условия использования

Настоящий Отчет представляет собой результат работы авторов и является интеллектуальной собственностью компаний Smart Engines и INTELLECT Law Firm.

Распространение, перепечатка, копирование (включая цифровое копирование на любой вид электронных носителей), использование или воспроизведение Отчета или его фрагментов производится исключительно с согласия правообладателей. Цитирование в силу ст. 1274 ГК РФ допускается только в информационных, научных, учебных и культурных целях при условии обязательного указания авторов.

Пользователь Отчета имеет право на его использование исключительно для внутренних нужд организации Пользователя, включая использование Отчета его сотрудниками. Любая передача Отчета или его фрагментов Пользователем в пользу иных лиц или использование Отчета в иных целях (реклама и продвижение собственных услуг, включение в состав собственных продуктов и услуг) допускаются только с письменного разрешения правообладателя. Нарушение указанных правил влечет за собой взыскание убытков, предусмотренных действующим законодательством.

Правообладатель не гарантирует и не делает никаких заявлений относительно результатов использования сведений, содержащихся в Отчете, в том числе относительно их точности, актуальности и применимости к конкретному внутреннему использованию, которое изберет Пользователь. Использование сведений, содержащихся в Отчете, осуществляется исключительно на собственный риск Пользователя и исключает возникновение связанных с их использованием или невозможностью их использования убытков.

Содержание

Условия использования	1
Авторы отчета	3
Введение	4
Только цифры	8
Общая статистика преступлений с использованием поддельных документов за 2019-2023 гг.	9
Детальная статистика по судебным делам за 2023 год	10
Что подделывают?	14
Виды подделок документов	17
Кто несет ответственность за проверку документов?	18
Примеры из судебной практики	20
Как ловят мошенников в разных каналах?	30
Как устроены антифрод-системы на базе ИИ	35
Возможности антифрод-системы на базе ИИ Smart Engines	41
Чек-лист: как выбрать ИИ-решение для безопасной идентификации?	44

Авторы отчета

Smart Engines – ведущий российский разработчик систем распознавания и проверки подлинности документов. Компания основана в 2016 году учеными с 25-летним опытом работы в сфере распознавания символов, изображений и обработки документов. Специалисты Smart Engines обладают уникальной экспертизой в области проверки подлинности документов.

Компания представила линейку программных продуктов на базе ИИ для борьбы с мошенниками и обнаружения поддельных документов как в физических, так и в цифровых каналах.

INTELLECT – современная юридическая фирма с уникальным опытом в судебных спорах и в регулярном консалтинге для бизнеса. На рынке юридических услуг с 2000 года.

Высокий уровень команды INTELLECT и реализуемых ею проектов подтвержден такими международными рейтингами, как Best Lawyers (США), Chambers Europe, Legal 500 EMEA, World Trademark Review 1000 (Великобритания), а также национальным рейтингом “Право.Ru-300”.



Введение

Экспертно-аналитический центр Smart Engines, компании-лидера на рынке распознавания, и юридическая фирма Intellect представляют отчет по результатам исследования, посвященного случаям мошенничества с использованием поддельных документов в России за 2019-2023 гг.

В отчете дана статистика по судебным делам, связанным с подделкой документов за пятилетний период, распределение по типам документов, приводятся примеры из судебной практики, в которых ответственность за недостаточную проверку документа возлагается на оказывающую услугу организацию.

Тренд на увеличение числа преступлений, связанных с поддельными документами, сохраняется. Вследствие этого страдают обычные граждане, с которых мошенники, например, по сфальсифицированным судебным приказам, пытаются взыскать несуществующие задолженности. Нередко пострадавшими также оказываются работники банков, сотрудники Росреестра или нотариальных палат, поскольку именно они часто несут ответственность за проверку подлинности документов.

В основу анализа легла информация из следующих источников:

- Статистические анализы МВД России “Состояние преступности в России” за 2019-2023 гг.
- Статистические отчеты Судебного департамента при Верховном Суде РФ
- Результаты рассмотрения уголовных дел за 2019-2023 гг.
- Официальная база судебных актов ГАС “Правосудие” (bsr.sudrf.ru)
- Неофициальная база судебных актов Sudact (sudact.ru)
- Российский федеральный портал открытых данных
- Банк судебной практики СПС “ГАРАНТ”
- Публикации официальных СМИ

Имеющиеся сведения носят ориентировочный характер, поскольку использование поддельных документов может быть квалифицировано как часть более широкого состава преступления. Например, использование поддельного паспорта с целью хищения средств квалифицируется как мошенничество (ст. 159 УК РФ), такое же действие с целью побега из военной части – как дезертирство (ст. 338 УК РФ).

“Число преступлений с использованием поддельных документов, как мы видим, по-прежнему остается на крайне высоком уровне. Это обусловлено, с одной стороны, доступностью технологий – мошенники осваивают новые инструменты с ИИ, что позволяет им создавать все более качественные и трудновывяляемые подделки. Еще одна причина – халатное отношение организаций к персональным данным своих клиентов и, как следствие, масштабные утечки. Украденная информация становится отличным подспорьем для изготовления муляжей и последующего получения услуг по фальшивым документам.

При этом за последний год существенно выросло число инцидентов с использованием документов, не относящихся к классу удостоверений личности, – это прежде всего нотариальные доверенности, судебные приказы, свидетельства о рождении, смерти”

Владимир Арлазаров

генеральный директор Smart Engines
доктор технических наук

“Подделка документов и удостоверений – одно из древнейших преступлений. Мотивы и цели создания подделок могут быть разные. Но независимо от этого тема распознавания фальшивок не только остается актуальной – ее значимость многократно возросла. От подделок страдают не только страховые и кредитные организации, но и обычные граждане, проявляющие излишнюю доверчивость, передавая свои персональные данные “липовым” сотрудникам банков, правоохранительных органов и т.п.

Подделка некоторых категорий документов поставлена на поток, и там замешаны как организованные группировки, так и целые подпольные фабрики. Злоумышленники постоянно придумывают новые способы фальсификации документов с использованием ИИ. Поэтому очень отрадно, что с помощью ИИ удалось решить проблему с распознаванием подделки на стадии ее предъявления/использования для получения каких-либо выгод”

Дмитрий Загайнов

управляющий партнер АБ “ИНТЕЛЛЕКТ”
почетный адвокат России

Только цифры

48 000

общее количество судебных дел по статьям 324-327.2 УК РФ (незаконное приобретение и сбыт документов) за 2019-2023 годы

21 000

общее количество судебных дел по статье 327 УК РФ (подделка, изготовление и оборот документов) за 2019-2023 годы

10 000

количество судебных дел по статьям 324-327.2 УК РФ (подделка, незаконное приобретение и сбыт документов) за 2023 год

3 500

количество судебных дел по статье 327 УК РФ (подделка, изготовление и оборот документов) в 2023 году

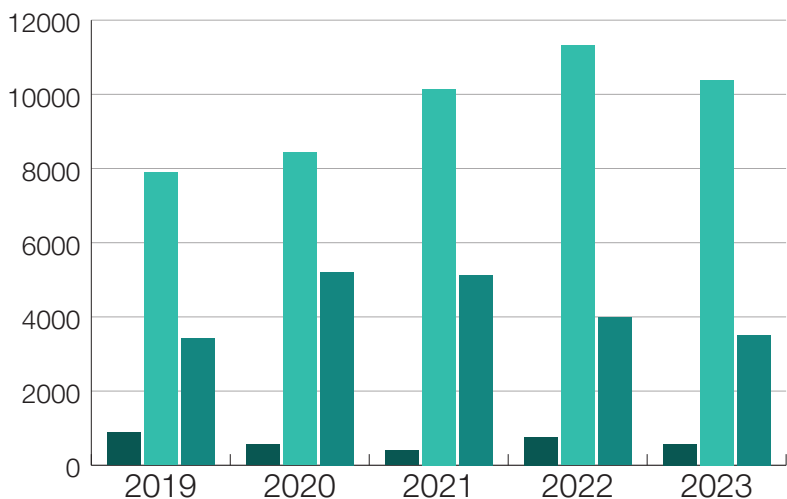
92%

количество судебных дел по ч.2 статьи 327 УК РФ (подделка документов удостоверений личности) в общей массе

5 000 000

размер компенсации, которую решением суда обязали выплатить страховую компанию в 2023 году

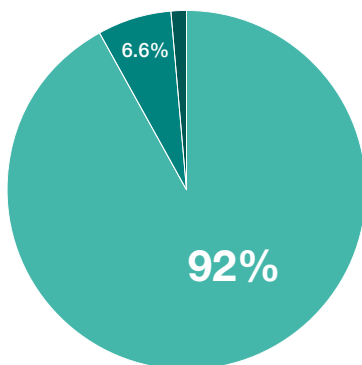
Общая статистика преступлений с использованием поддельных документов за 2019-2023 гг.



- Статистика судебных дел по ст. 327 УК РФ
- Судебные дела по ст. 324-327.2 УК РФ
- Количество новых преступлений, выявленных МВД

Детальная статистика по судебным делам за 2023 год

Количество уголовных дел, в которых фигурируют
поддельные документы (ст. 327 УК РФ) – **3 508**.



- **3 228 (92.0%)**

количество уголовных дел по ч. 2 ст. 327 УК РФ
(подделка удостоверений личности)

- **232 (6.6%)**

количество уголовных дел по ч. 1 ст. 327 УК РФ
(подделка документов за исключением ДУЛ)

- **48 (1.4%)**

количество уголовных дел по ч. 3 ст. 327 УК РФ
(приобретение, хранение и сбыт
поддельных документов)

12%

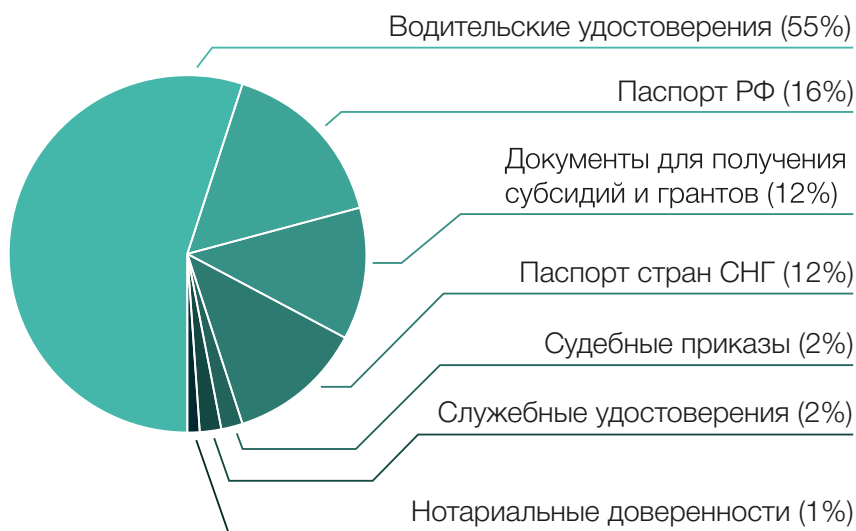
Рост числа случаев подделки документов за исключением документов, удостоверяющих личность

(ч. 1 ст. 327 УК РФ) в 2023 году (YOY).

- бухгалтерские отчеты
- налоговые декларации
- выписки по банковским счетам
- свидетельства о регистрации предприятий
- судебные приказы
- нотариальные доверенности

Детальная статистика за 2023 год: распределение по документам

В 2023 году большинство поддельных документов составляют удостоверения личности: общегражданские паспорта РФ и паспорта стран СНГ, водительские удостоверения, миграционные карты, разрешения на работу и другие.



Что подделывают?

В 2023 году почти все поддельные документы – это удостоверяющие документы: общегражданские паспорта РФ и паспорта стран СНГ, водительские удостоверения, миграционные карты, разрешения на работу и др. На них приходится 95% от общего числа поддельных документов. При этом на официальные документы – доверенности, судебные приказы, награды или госзнаки – приходится всего 5%.

Водительские удостоверения

Водительские удостоверения среди подделок являются безоговорочным лидером – 55% от общего объема. Показатель свидетельствует о том, что подпольное производство подобного типа документов буквально поставлено на поток и россиянам зачастую не составляет особого труда купить водительское удостоверение – “нужного специалиста” можно легко найти в сети Интернет.

Иностранные удостоверения личности

Часто изготавливаются на подпольных фабриках, куда иностранцев (в большинстве случаев – граждан Кыргызстана и Узбекистана) завлекают рекламой в Интернете и обещаниями удалить все их данные после того, как услуга будет оказана. В большинстве случаев подделывают миграционные карты или фальсифицируют отметки о въезде и виде на жительство в оригинальном национальном паспорте

Внутренние паспорта

Внутренние паспорта как граждан РФ, так и стран СНГ сохраняют место в тройке лидеров и составляют 16%. Внутренние паспорта используются в большинстве случаев при оформлении потребительского кредита, покупки билета на самолет или поезд. Хотя встречаются случаи, когда поддельные удостове-

рения личности используются для вступления в наследство или для проникновения в закрытые административно-территориальные образования (ЗАО). Большая часть случаев (дошедших до суда) приходится на подделку собственными силами. В частности, переклейку фотографий. При этом в отчете не учитываются случаи подделки изображений документов в фоторедакторах, которые не доходят до суда.

Внутренние финансовые документы

Это могут быть бухгалтерские отчеты, налоговые декларации, выписки по банковским счетам, свидетельства о регистрации предприятий и другие документы. Подобные бумаги могут фальсифицироваться в том числе для того, чтобы получать от государства финансовую поддержку на открытие своего дела.

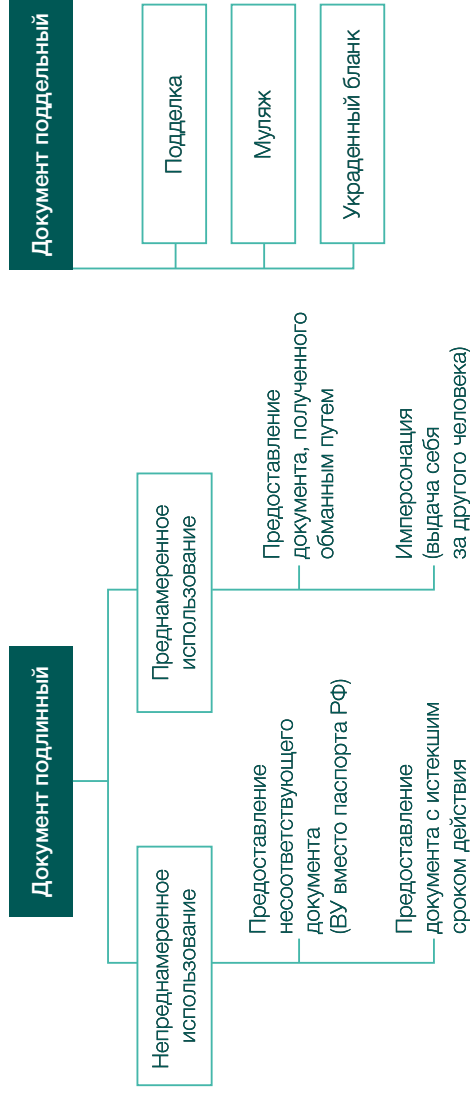
Судебные приказы и нотариальные доверенности

На поддельные нотариальные доверенности и судебные приказы приходится 1% и 2% соответственно. Несмотря на то, что количество уголовных дел, связанных с подделкой этих типов документов, крайне невелико, в действительности именно они несут высокий риск и максимальный ущерб.

Во-первых, это связано с огромным объемом подделок. Так, в одном деле, где фигурирует подделка судебных приказов, может идти речь об обороте десятков, сотен и даже тысяч фальшивок. Фактически это напоминает ситуацию с водительскими удостоверениями и паспортами стран СНГ, где за незаконным изготовлением документов стоят не отдельные люди, а хорошо организованные группы.

Во-вторых, поддельные судебные приказы и нотариальные доверенности используются для незаконных операций с недвижимостью или организации мошеннических схем - в частности, для взыскания с людей несуществующих задолженностей.

Мошенничество с документами



Виды подделок документов

Цифровые подделки

- замена цифр с целью выдать недействительный документ за действительный
- использование дипфейков для процессов аутентификации и верификации
- синтез данных

Физические подделки

- переклейка фото
- полная замена листа документа
- внесение точечных изменений в персональные данные
- клонирование документов

168

утечек зафиксировал
Роскомнадзор в 2023 году

300 млн

уникальных записей россиян
утекло за 2023 год

200

утечек уже зафиксировано
по данным F.A.C.C.T за 2024 год

500 млн

уникальных записей россиян
утекло за 2024 год

Кто несет ответственность за проверку документов?

Нотариусы

Как указано в п. 7 Обзора судебной практики Верховного Суда Российской Федерации №1 (2021), в силу возложенной законом обязанности удостоверить личность гражданина, обратившегося за совершением нотариальных действий, нотариус отвечает за имущественный вред, причиненный покупателю недвижимого имущества в результате ненадлежащего установления нотариусом личности гражданина, от имени которого выдана доверенность на продажу этого имущества.

Однако судебная практика далеко не всегда привлекает нотариусов к ответственности за указанное нарушение, и указанная обязанность по проверке может толковаться достаточно ограниченно.

Кроме того, важно, чтобы у лица были реальные возможности проверки подлинности документа, в т.ч. посредством онлайн-сервисов (например, “Проверка доверенности” от ФНП). Между тем, в зависимости от обстоятельств дела даже наличие указанных возможностей может быть недостаточным для возложения ответственности за недостаточную проверку документа.

Судебные приставы-исполнители и работники Росреестра

Невыполнение судебным приставом-исполнителем обязанности по проверке подлинности документов может в том числе стать основанием для привлечения такого должностного лица к ответственности по ст. 293 УК РФ, если судебный приказ носил очевидные признаки подделки:

- Превышение взысканной по приказу суммы установленных законом предельных сумм, по которым может выноситься судебный приказ

- Явное несоответствие качества печати документа или размытость печати суда
- Фактические ошибки в документе (разное ФИО судьи / наименование суда в преамбуле и подписи документа)
- Отсутствие в судебном приказе обязательных реквизитов (печать, подпись, указание суда и т.д.)

Работники банков

Согласно ст. 856 ГК РФ банк несет ответственность в случае необоснованного списания денежных средств со счетов клиентов.

В соответствии с ч. 6 ст. 70 Закона “Об исполнительном производстве” в случае обоснованных сомнений в подлинности исполнительного документа, полученного непосредственно от взыскателя (его представителя), банк или иная кредитная организация вправе для проверки подлинности исполнительного документа либо достоверности сведений задержать исполнение исполнительного документа, но не более чем на семь дней.

Более того, в Письме Банка России от 02.10.2014 № 167-Т “О мерах по снижению операционных рисков при принятии к исполнению исполнительных документов” дается прямое указание на то, что в целях снижения операционных рисков кредитных организаций Банк России рекомендует кредитным организациям тщательно проверять подлинность предъявляемых исполнительных документов перед принятием решения о списании денежных средств со счетов клиентов.

Между тем, в большинстве случаев к банку предъявляются более мягкие требования в части должной осмотрительности по сравнению с государственными служащими. Банк несет ответственность только в случае наличия очевидных признаков подделки либо установленного факта сговора между работником банка, осуществлявшим проверку исполнительного документа, и лицами, подделавшими последний. В последнем случае банк имеет возможность регрессного взыскания суммы ущерба с виновного работника.

Примеры из судебной практики

Решение Арбитражного суда г. Москвы от 17 февраля 2023 г. по делу No А40-264158/2022

В АО “Россельхозбанк” поступило заявление гражданки Саматовой Н.Е. с судебным приказом мирового судьи судебного участка №113 г. Тольятти. В заявлении были указаны банковские реквизиты Саматовой Н.Е. в Райффайзенбанк и просьба перевести на них денежные средства в размере 390 тыс. руб., взысканные мировым судьей с ООО “Резерв”, у которого был открыт счет в Россельхозбанк. В картотеке мирового судьи судебного участка №113 г. Тольятти действительно имелось указанное дело с решением о взыскании, банк исполнил требования и перевел денежные средства взыскательнице, которые были выданы через банкомат.

Между тем, после этого оказалось, что:

- Судебный приказ был подделан
- Счет взыскателя в Райффайзенбанк был открыт на основании поддельного паспорта

После этого Россельхозбанк самостоятельно восполнил ООО “Резерв” денежные средства, взысканные с него мошенниками, и обратился с убытками к Райффайзенбанк, вменяя последнему непроведение достаточных мероприятий по идентификации гражданки при открытии на ее имя счета.

Суд установил, что АО “Россельхозбанк” провело достаточные мероприятия по проверке судебного приказа, так как на момент проверки в картотеке дел мирового суда действительно имелась информация о взыскании (судебный приказ был отменен позднее). Суд также установил, что АО “Райффайзенбанк” не предприняло мер по осуществлению надлежащей проверки предоставленного документа, удостоверяющего личность (паспорта), в результате чего был принят поддельный паспорт и открыт банковской счет. В итоге суд взыскал убытки с Райффайзенбанк в размере 400 тыс. руб. Мошенников еще не нашли.

Привлеченное к ответственности лицо:
АО “Райффайзенбанк”

Размер и вид назначенного наказания:
штраф 400 000 руб.

Дело No 12401400005001566

ст. 327 УК РФ

Организованная группа лиц продолжительное время осуществляла серую схему по ввозу в Россию автомобилей премиум-класса с уклонением от уплаты таможенных пошлин. Реализация схемы проходила через петербургскую фирму “Пикап-Центр Макса Бороды” и несколько фирм-сателлитов.

Автомобили оформлялись на граждан Киргизии, причем не все из них подозревали о поставке их на учет как покупателей авто. Цена поставленных в Киргизию автомобилей занижалась посредством подменных шильдов с техническими характеристиками, что позволяло практически вдвое сократить налоговые пошлины. В Санкт-Петербурге с помощью Средства Криптографической Защиты Информации и доступа к АО “Электронный паспорт” сотрудниками фирмы создавался недостоверный шаблон СБКТС, который направлялся к российскому покупателю автомобиля.

Реализация схемы позволяла уйти от полноценной уплаты налогов с последующим выводом денежных средств. В поле зрения следователей на сегодняшний день порядка 140 автомобилей, прошедших по вышеуказанным схемам.

Киргизия в качестве промежуточной страны выбрана неслучайно, поскольку сопряженные с этой страной таможенные правила позволяли существенно снизить стоимость автомобилей для минимизации таможенных платежей.

Разбирательство продолжается

Приговор Петровского районного суда Ставропольского края от 25.05.2023 по делу № 1-7/2023

Фабула: был угнан автомобиль, после чего угонщик совершил перерегистрацию транспортного средства.

Суд установил, что должностное лицо, несмотря на несоответствие идентификационного номера автомобиля и номера, указанного в паспорте транспортного средства, номеру, указанному в заявлении о внесении изменений в регистрационные данные, полученному из специального программного обеспечения Федеральной информационной системы Госавтоинспекции МВД России, не отказал в регистрационных действиях.

Привлеченное к ответственности лицо:

старший государственный инспектор безопасности дорожного движения.

Размер и вид назначенного наказания:

лишение свободы сроком на [...] месяцев с отбыванием в исправительной колонии общего режима на основании ч. 3 ст. 47 УК РФ с лишением права занимать должности, связанные с осуществлением функций представителя власти, организационно-распорядительных и административно-хозяйственных функций в государственных органах, органах местного самоуправления, государственных и муниципальных учреждениях, в правоохранительных органах, на срок [...] года.

Апелляционное постановление Верховного Суда Республики Крым от 14.05.2023 по делу № 22-312/2023

Фабула: Была произведена продажа квартиры, при этом продавец зарегистрировал свое право собственности на данную квартиру на основании поддельного свидетельства о праве на наследство, которое другим нотариусом не выдавалось. Привлекаемый к ответственности нотариус сделку по продаже квартиры удостоверил.

Впоследствии суд установил, что нотариус:

- Проигнорировал то, что регистрация права собственности на объект недвижимости за продавцом является необходимой информацией для совершения нотариальных действий при удостоверении сделки по продаже недвижимости и такая информация может и должна быть получена не только по сведениям Единого государственного реестра недвижимости, но и по сведениям из Единой информационной системы нотариата
- Не исследовал тот факт, что свидетельство о праве на наследство не выдавалось, его реестровый номер не существует, а наследственное дело иным нотариусом не заводилось

Привлеченное к ответственности лицо:
страховая компания

Размер и вид назначенного наказания:
убытки в размере 2 400 000 руб.

Приговор Евпаторийского городского суда Республики Крым от 22.03.2023 по делу № 1-14/2023

Фабула: регистратор проигнорировал многочисленные изъяны в представленной документации, свидетельствующие о подделке предоставленных документов, а именно:

- Не провел правовую экспертизу правоустанавливающих документов, изготовленных на иностранном языке, не переведенных на русский язык и не заверенных в установленном законом порядке
- Не провел правовую экспертизу судебного решения, которое не являлось подлинным, содержащиеся в нем сведения были недостоверными, а его форма не соответствовала требованиям законодательства Российской Федерации
- Не провел правовую экспертизу судебного решения, не заверенного гербовой печатью суда

Привлеченное к ответственности лицо:
сотрудник Росреестра

Размер и вид назначенного наказания:

лицо признано виновным, назначено наказание в виде штрафа в размере 50 000 руб. (смягчено в соответствии с ч. 5 ст. 72 УК РФ), однако впоследствии на основании п. 3 ч. 1 ст. 24 УПК РФ и п. “а” ч. 1 ст. 78 УК РФ подсудимый освобожден от наказания в связи с истечением сроков давности привлечения к уголовной ответственности.

Апелляционное определение Судебной коллегии по гражданским делам Ростовского областного суда от 22.11.2023 по делу № 33-16473/2023

Фабула: оспорена сделка по купле-продаже квартиры, признано недействительным зарегистрированное за покупателем право. Суды установили, что основаниями для регистрации права собственности на квартиру явились в том числе заявление об отсутствии брака и доверенность – оба документа собственником квартиры никогда не выдавались и не подписывались. Покупатель предъявил иск к нотариусу, размер убытков составил 5 688 237 руб.

Суд установил, что при проверке подлинности документов были допущены нарушения, особенно обратив внимание на то, что, согласно представленной в материалы дела копии поддельного паспорта, в паспорте размещена фотография гражданина, возраст которого очевидно не соответствует возрасту 27 лет, наступившему при выдаче паспорта 03.04.2003 года.

Привлеченное к ответственности лицо:
нотариус, страховые компании

Размер и вид назначенного наказания:

- С нотариуса взысканы убытки в размере 188 237 руб.
- Взысканы убытки в размере 5 000 000 руб.

Определение Судебной коллегии по гражданским делам Первого кассационного суда общей юрисдикции от 12.12.2022 по делу No 8Г-31768/2022 [88-33504/2022]

Фабула: на основании поддельного судебного приказа судебный пристав-исполнитель необоснованно взыскал задолженность, в связи с чем в его отношении была возбуждена служебная проверка, по результату которой было вынесено предупреждение о неполном служебном соответствии за совершение дисциплинарного проступка.

Впоследствии судебный пристав-исполнитель оспаривал в суде результаты проверки – первые две инстанции встали на его сторону, кассация судебные акты отменила и отправила на новое рассмотрение. **Суд установил,** что предъявленный документ имел явные признаки подделки (наличие ошибок, опечаток, нарушение правил форматирования документов).

Привлеченное к ответственности лицо:
судебный пристав-исполнитель

Размер и вид назначенного наказания:
отменены судебные акты, признающие незаконным применение дисциплинарной ответственности (наложение дисциплинарного взыскания в виде предупреждения о неполном служебном соответствии за совершение дисциплинарного проступка)

Решение АС Свердловской области от 06.06.2023 по делу No A60-69109/2022, Решение АС Калужской области от 15.11.2023 по делу No A23-5356/2022.

Аналогичное дело: Решение Никулинского районного суда г. Москвы от 30.03.2023 г. по делу No 02-1342/2023

Фабула: Компания не заключала договоров и не давала разрешений на создание электронной подписи. В удостоверяющий центр обратилось неизвестное лицо с поддельным удостоверением личности и СНИЛС директора компании, попросив выпустить сертификат ключа проверки электронной подписи на имя потерпевшей компании. Удостоверяющий центр не провел достаточных мероприятий по проверке подлинности удостоверений и выпустил сертификат.

Впоследствии неизвестные лица использовали поддельную подпись для подачи налоговой отчетности от имени истца. Это привело к поступлению требований и решений от налогового органа на имя потерпевшей компании.

Ответственное за проверку удостоверения лицо:
удостоверяющий центр

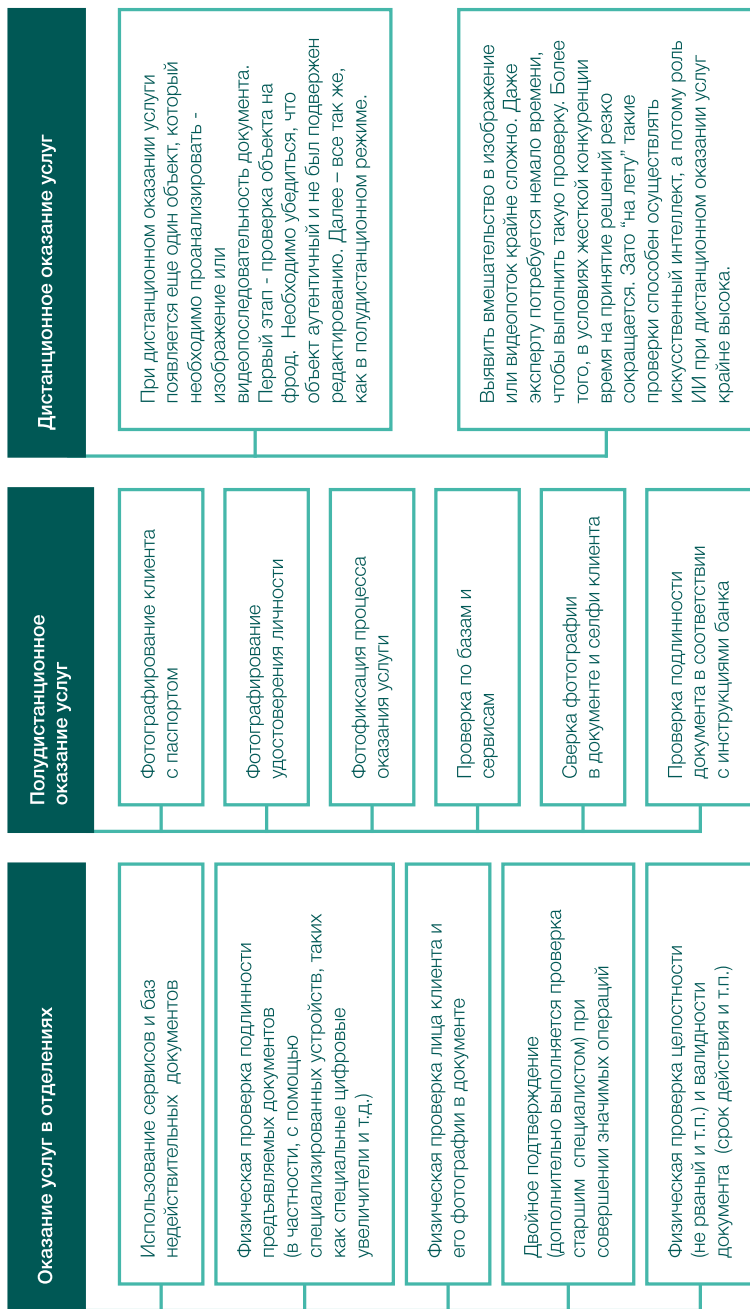
Ответственность:
размер убытков устанавливается

Как ловят мошенников в разных каналах?

Самый надежный способ защиты от мошенника при оказании финансовой услуги – это предварительная идентификация и аутентификация клиента.

Обязательная идентификация клиента банками прописана в федеральных законах, а проверка подлинности паспорта – Положением Банка России от 19 августа 2004 года “Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма”. В соответствии с указанием банки должны проверять на подлинность паспорт при идентификации клиентов в рамках любых операций, включая открытие вклада, выдачу кредита, обмен валюты и денежные переводы (обе последние операции – на сумму свыше 15 тыс. рублей).

Современные финансовые организации оказывают услуги фактически тремя способами: традиционно через отделения, полудистанционно с помощью выездных сотрудников и дистанционно. Рассмотрим каждый из данных пунктов подробнее с точки зрения используемых методов антифрода и необходимости применения систем на базе ИИ.



Традиционное оказание финансовых услуг в отделениях

Клиент приходит лично с “живыми” документами. В качестве технологий антифрода используются:

- Физическая проверка подлинности предъявляемых документов, в том числе с использованием специализированных устройств, таких как мультиспектральные считыватели документов, ультрамаги (настольные приборы для проверки подлинности документов), специальные цифровые увеличители и др.
- Физическая проверка целостности – документ не рваный, не надорванный, валидности – срок действия по имеющейся у организации политике безопасности
- Физическая сверка лица клиента в момент обслуживания и лица в документе
- Использование сервисов и баз недействительных документов
- Двойное подтверждение (дополнительно выполняется проверка старшим специалистом) при совершении значимых операций

Хотя проверка документа на валидность и подлинность присутствует, ее результат может быть недостоверным, например, по следующим причинам:

- Невнимательность и халатность сотрудника
- Сговор сотрудника с мошенником
- Отсутствие полноты информации о способе проверки документов

Системы антифрода на базе ИИ, работающие с мультиспектральными данными, полностью исключают человеческий фактор.

Проверять на подлинность следует не только удостоверение личности, но и основание предъявления документа (например, доверенность, по которой разрешается оказание услуг, или судебный приказ, по которому выполняется требование о переводе денег).

Полудистанционное оказание услуг

Другая распространенная практика – выездной сотрудник передает клиенту банковскую карту или забирает у него заявление на открытие счета. В этом случае методы борьбы с мошенниками построены на базе расширенной идентификации личности, а также удостоверения факта оказания услуги именно клиенту, чей документ предъявляется, проверки подлинности и “живости” этого самого документа.

Из распространенных методов антифрода здесь стоит отметить:

- Фотографирование клиента с паспортом (клиента с карточкой)
- Фотографирование документа, удостоверяющего личность
- Фотофиксация процесса оказания услуги
- Проверка подлинности документа в соответствии с инструкцией банка
- Проверка по базам и сервисам
- Сверка лица из документа и селфи

Сами по себе “полевые условия” за счет в том числе человеческого фактора не позволяют внимательно относиться к процессу идентификации и аутентификации, что непосредственно приводит к большому количеству случаев мошенничества. Кроме того, важным фактором выступает время оказания услуги. В данном случае роль ИИ – упорядочить и упростить процесс идентификации и аутентификации клиента за счет технологий распознавания и проверки подлинности фотографий и видеоданных, обеспечить ускорение процесса оказания услуги.

Дистанционное оказание услуг

При дистанционном оказании услуги появляется еще один объект, который необходимо проанализировать – изображение или видеопоследовательность документа. Первый этап – проверка объекта на фрод. Необходимо убедиться, что объект аутентичный и не был подвержен редактированию. Далее – все так же, как в полудистанционном режиме.

Выявить вмешательство в изображение или видеопоток крайне сложно. Даже эксперту потребуется немало времени, чтобы выполнить такую проверку. Более того, в условиях жесткой конкуренции время на принятие решений резко сокращается. Зато “на лету” такие проверки способен осуществлять искусственный интеллект, а потому роль ИИ при дистанционном оказании услуг крайне высока.

Как устроены антифрод-системы на базе ИИ

**(какие атаки детектируют, как оценивать
качество работы)**

При беглом взгляде может показаться, что антифрод-система по своей природе аналогична традиционной системе распознавания образов. Отчасти это действительно так: в антифрод-системах используются такие же семейства алгоритмов ИИ, как и в других системах распознавания. Тем не менее современные антифрод-системы серьезно отличаются от классических систем распознавания образов на всех уровнях построения за счет большого количества особенностей.

1. **Большее число операций**

В отличие от систем распознавания текста документов, система антифрода более сложная и комплексная на всех уровнях, начиная с анализа входного изображения – системе распознавания достаточно найти документ, а система антифрода должна не только найти документ, но и найти аномалии как внутри, так и снаружи документа. На уровне анализа шаблона – распознать тип документа и проверить ключевые особенности этого типа. На уровне распознавания буквы – вместе с идентификацией символа необходимо также проверить шрифт и способ нанесения. Это делает системы антифрода более комплексными и сложными в разработке, чем системы “простого” распознавания.

2. **Анализ обширного объема данных**

На входе антифрод-системы рассматривают комплексированные данные, содержащие наборы изображений (зарегистрированных в различных спектрах), результаты распознавания (информация о найденном документе и его атрибутах), ответы от отдельных модулей анализа и понимания документа. Опираясь таким обширным набором данных разной природы, антифрод-система должна принять решение о наличии фальсификации.

3. **Комплексный вывод**

На выходе антифрод-система возвращает коллекцию выявленных признаков фальсификаций, про каждый из которых известен не просто бинарный ответ: был ли в результате выявлен каждый признак или нет. Современные антифрод-системы на базе ИИ возвращают пару значений: достаточно ли данных для выявления признака и вероятность выявления признака на анализируемых данных. В некоторых случаях антифрод-системы, помимо коллекции признаков, возвращают также уверенность в подлинности рассматриваемого документа, которая мо-

жет определяться как с помощью детерминированных правил путем взвешивания значений отдельных признаков, так и с помощью применения предобученных моделей ИИ.

4. Видит то, что не видит человек

За счет активного применения методов машинного обучения системы антифрода на базе ИИ, в отличие от большинства традиционных систем распознавания, выявляют и детектируют на входных данных сложно интерпретируемые человеком элементы (например, выявляют аномалии в распределении шумов на изображении, что человеку практически невозможно сделать). Такое поведение затрудняет понимание причин отнесения отдельных рассматриваемых случаев случаев к подделкам, но позволяет эффективно находить даже те случаи фрода, которые опытные сотрудники выявляют с трудом.

5. Требования к качеству работы

Данная особенность является ключевой в части отличия антифрод-систем от других систем распознавания. Требования к качеству работы у антифрод-систем принципиально отличаются от аналогичных требований к традиционным распознающим системам. Например, когда рассматривается система распознавания текста, то вполне достаточным является показатель правильности распознавания (ассурасу), демонстрирующий, сколько слов система правильно распознала. Чем выше показатель правильности, тем меньше ручной работы придется делать после применения системы распознавания.

Когда речь заходит об антифрод-системах, одним показателем обойтись нельзя. Антифрод-системы обрабатывают как подлинные документы, так и подделки. При этом цена ошибки на подлинных документах (когда подлинный документ распознан как ошибка) и на подделках (когда подделка была распоз-

нана такой системой как подлинный документ) принципиально отличается. Качество работы таких систем измеряют путем вычисления двух показателей:

- Ошибка первого рода (“ложноположительное” заключение, обозначается α) – когда антифрод-система неверно приняла подлинный документ за подделку
- Ошибка второго рода (“ложноотрицательное” заключение, обозначается β) – когда антифрод-система неверно пропустила подделку

Будучи “дополнительным щитом” против мошенника, антифрод-системы не должны сильно препятствовать прохождению подлинных документов. Это значит, что количество ложных срабатываний (ситуаций, когда антифрод-система принимает подлинный документ за подделку) должно быть минимальным. Современные антифрод-системы на базе искусственного интеллекта могут обеспечивать значение ошибки первого рода на уровне не выше 0.1%, что говорит о том, что антифрод-система ошибается на подлинных документах не чаще 1 раза на 1000 подлинных документов.

Почему так важно редко ошибаться на подлинных документах? Для примера рассмотрим антифрод-систему, которая одинаково ошибается как на подлинных документах, так и на подделках с вероятностью 1% (то есть $\alpha = \beta = 0.01$). Пусть также в примере поддельные документы встречаются не очень часто – с вероятностью $p = 1\% = 0.01$ (то есть на 100 предъявленных документов всего 1 поддельный), что на самом деле в некотором приближении соответствует практике. Какова вероятность того, что документ поддельный, если такая гипотетическая система распознала его как поддельный? Совсем не 99%, как может показаться на первый взгляд. Чтобы получить правильный ответ, следует обратиться к теории вероятности, а именно – к формуле Байеса:

$$P_{\alpha=0.01}(\text{подделка}|\text{распозналась подделка}) = \frac{0.99 \cdot 0.01}{0.01 \cdot 0.99 + 0.99 \cdot 0.01} = 0.5$$

Если гипотетическая система с рассмотренными выше параметрами “сработала”, вероятность того, что перед нами действительно подделка, составляет всего 50%

Однако если в том же примере ошибка первого рода будет 0.1%, то вероятность выявления подделки резко возрастает:

$$P_{\alpha=0.001}(\text{подделка}|\text{распознала подделка}) = \frac{0.999 \cdot 0.001}{0.01 \cdot 0.999 + 0.99 \cdot 0.01} \approx 0.91$$

Таким образом, требования к качеству работы антифрод-систем принципиально отличаются от требований к традиционным распознающим системам.

На сегодняшний день продвинутые автоматические антифрод-системы способны:

- Контролировать действительность документа в части присутствующих дат
- Контролировать соответствие данных документа (например, контролировать соответствие данных визуально-контролируемой зоны машиночитаемой зоне)
- Выполнять проверку контрольных сумм заданного набора целевых полей
- Контролировать целостность данных (соответствие присутствующих в документе атрибутов требованиям стандартов)
- Контролировать наличие обязательных атрибутов в документе (в том числе печатей и подписей)
- Выполнять детализированную проверку бланка документа на предмет правильности оформления
- Выполнять проверку цветности документа в целом и отдельных атрибутов
- Контролировать подлинность используемых шрифтов при оформлении документа

- Выполнять проверку динамически изменяемых элементов (например, голограмм) для распознавания в видеопотоке
- Контролировать и сверять фотографию держателя документа
- Распознавать уникальные атрибуты в графических реквизитах (например, распознавать печать в документе)
- Контролировать наличие на документе защитных элементов в мультиспектральном режиме (элементы защищенной полиграфии)
- Выявлять аномалии захвата изображения (в том числе выявлять “пересъемку с экрана”)
- Выявлять физические вмешательства в документ (переклейку фотографии, исправление реквизитов и т.д.) при анализе мультиспектральных изображений
- Выявлять вмешательства в изображение с помощью фоторедакторов
- Выявлять синтезированные изображения, в том числе выполненные с применением методов глубокого обучения
- Проверять документ по базам данных в случае необходимого доступа

Все эти функции позволяют выявлять подавляющее большинство классов подделок:

- Муляжи и макеты документов, а также клоны документов
- Случаи предъявления ксерокопий документов
- Случаи предъявления цифровых образов документов
- Случаи предъявления документов с переклеенной фотографией
- Случаи предъявления физически модифицированного документа
- Случаи предъявления “просроченного” документа
- Цифровой фрод

Возможности антифрод-системы на базе ИИ Smart Engines

Технология проверки подлинности и “живости” документов на базе искусственного интеллекта от Smart Engines (Computation Document Forensic AI) представляет собой омниканальное решение для выявления подделок документов в задачах идентификации и аутентификации клиентов в цифровых каналах и при оффлайн-обслуживании клиентов. Технология включает в себя следующие модули:

Модуль выявления цифрового вмешательства (“антифотошоп”)

- Поиск цифрового вмешательства в изображение документа
- Проверка метаданных и структуры файла с изображением
- Поиск модификаций в изображении методом вставки (copy-move, copy-paste, splicing)
- Обнаружение областей изображения с затертыми данными (erase-fill)
- Выявление многократного сжатия изображения документа
- Поиск модификаций текстовых атрибутов в документе, выполненных с помощью инструментов графических редакторов
- Выявление признаков синтеза документа, в том числе с применением генеративных нейронных сетей (deepfake)

Модуль выявления признаков компрометации документов (“антифрод”)

- Проверка валидности бланка документа (template validation)
- Проверка специальных визуальных элементов дизайна бланка документа
- Контроль способа нанесения данных (типов и способов) печати атрибутов
- Проверка гарнитуры (начертания шрифтов) текстовых атрибутов
- Контроль срока действия документа
- Сквозная проверка данных лицевой и оборотной стороны документа
- Проверка контрольных разрядов, формата и правил заполнения реквизитов
- Анализ согласованности реквизитов документа
- Проверка характеристик и распознавание штампов и печатей
- Кросс-валидация распознанных данных документа (VIZ-MRZ-Chip-Barcode)
- Проверка соблюдения правил заполнения документа
- Выявление признаков переклейки фотографии в документе

Модуль проверки “живости” документов (document liveness detection)

- Детекция и контроль оптически-переменных элементов (OVD), включая голограммы, айдентиграммы, датаграммы
- Детекция и контроль текстовых и графических элементов, выполненных оптически-переменными чернилами (OVI)
- Выявление признаков съемки документа с экрана (screen recapture)

- Выявление фотокопий (ксерокопий) документов
- Выявление признаков подмены сцены
- Обнаружение объектов, перекрывающих значимые атрибуты и реквизиты документа

Модуль мультиспектральной проверки подлинности документов

- Контроль люминесценции бланка при освещении документа излучением в УФ-диапазоне 365 нм
- Контроль бланка и реквизитов документа в ближнем ИК-диапазоне
- Выявление клеевых пятен и следов изменения данных (потертостей)
- Выявление разрывов и надрывов документа
- Контроль наличия, целостности и отсутствия специальных элементов защиты (люминесцирующих волокон и других объектов защищенной полиграфии) в оптическом, ИК- и УФ-диапазонах
- Многоуровневое комплексное обнаружение переклейки фотографий держателя документа
- Многостраничный анализ документа

Модуль небιοметрической сверки лиц

- Сквозная нейросетевая модель, комплексно решающая задачу сверки двух лиц без выделения биометрических дескрипторов
- Недискриминирующая нейросетевая модель, устойчивая к полу, расе, возрасту, макияжу
- Специальный метод обучения сквозных нейросетевых моделей, препятствующий возникновению биометрических признаков в скрытых пространствах

Чек-лист: как выбрать ИИ-решение для безопасной идентификации?

Если вы планируете автоматизировать процесс удостоверения личности и не определились с выбором технологии, предлагаем ознакомиться с нашим чек-листом. Эти вопросы помогут выбрать функциональное решение, наиболее соответствующее вашим требованиям.

Вопросы разделены на три группы в соответствии с ключевыми этапами процесса идентификации человека.

Что включает в себя процесс идентификации человека

1. Распознавание документа

На данном этапе удостоверяющий личность документ сканируется, искусственный интеллект распознает содержащиеся в нем данные, извлекает и вносит их в соответствующие поля информационной системы.

2. Аутентификация документа

На данном этапе обеспечивается проверка подлинности и “живости” (liveness) предъявленного документа, его оригинальности и действительности.

3. Аутентификация предъявителя документа

На данном этапе производится сравнение предъявителя с фотографией в документе, удостоверяющем личность.

В настоящее время рынок изобилует десятками систем, некоторые из которых построены на базе искусственного интеллекта, предлагающих автоматизировать процесс идентификации личности. У каждой технологии есть свои особенности, которые существенно влияют на организацию процесса идентификации.

Детальный перечень вопросов ниже поможет вам определить функциональность, которая идеально подойдет непосредственно для вашего бизнес-процесса.

Этап 1. Распознавание документа

- Готовы ли вы брать на себя юридические риски в области административной и уголовной ответственности при использовании сервисов и краудсорсинговых платформ в целях обработки персональных данных?
- Требуется ли вам on-premise решение, которое функционирует в контуре и не передает данные третьим лицам?
- Готовы ли вы доверить распознавание документов с чувствительной информацией, включая персональные данные, программному обеспечению иностранных вендоров?
- Хотите ли вы максимально исключить оператора из процесса ввода персональных данных и делегировать эту задачу алгоритмам ИИ?
- Готовы ли вы к тому, что ваши сотрудники и клиенты будут тратить минуты на ожидание при вводе данных?
- Необходимо ли в рамках вашего процесса распознавание в режиме реального времени?
- Требуется ли возможность распознавания как сканов, так и фотографий документов?
- Важно ли для вас, чтобы ИИ мог распознавать данные в любых условиях, не заставляя пользователя долго подбирать ракурс и освещение?
- Требуется ли поддержка актуальных удостоверяющих документов СНГ, ЕАЭС, БРИКС и всего мира (паспортов,

ID-карт, ВНЖ, миграционных карт, водительские удостоверений и т.п.)?

- Хотите ли вы автоматически распознавать рукописные паспорта, адреса прописки?
- Требуется ли распознавание всех полей документа, в том числе написанных на национальных языках?
- Есть ли необходимость в распознавании всех страниц паспорта (не только основного разворота и страницы с пропиской, но и сведений о ранее выданных паспортах и пр.)?
- Важна ли работоспособность решения на различных (в том числе отечественных) серверных и мобильных вычислительных платформах?
- Хотите ли вы безопасно распознавать документы непосредственно на веб-странице?
- Требуется ли возможность распознавания нескольких документов на одном изображении?

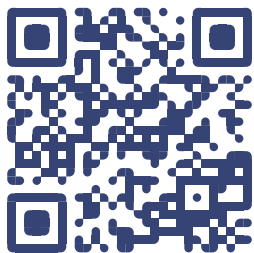
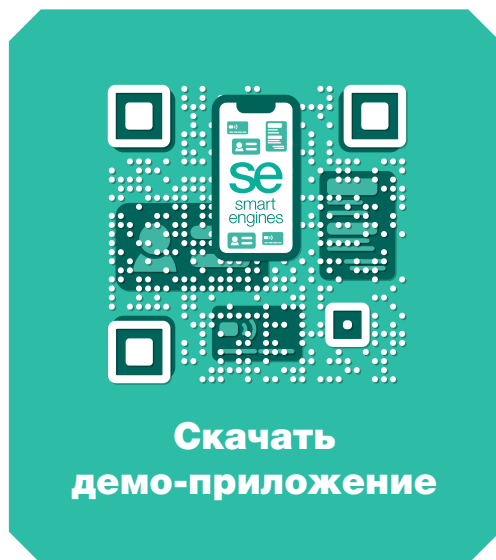
Этап 2. Аутентификация документа

- Хотите ли вы, чтобы решение было полностью автономным и соответствовало законодательству РФ в области обработки персональных данных?
- Готовы ли вы доверить процесс проверки подлинности документов облачным сервисам, в том числе из недружественных юрисдикций?
- Требуется ли в вашем процессе проверка действительности и подлинности удостоверяющего документа в соответствии с законодательством РФ?
- Важно ли для вас получать интерпретируемый с человеческой точки зрения ответ от алгоритмов ИИ в части проверки подлинности?

- Требуется ли контроль срока действия документа?
- Требуется ли выявлять факты предъявления фотокопий документа вместо оригинала?
- Требуется ли выявлять факты предъявления скриншотов и пересъемов документа с экрана вместо оригинала?
- Требуется ли выявлять случаи “фотошопа” (фальсификации документов в фоторедакторах)?
- Необходимо ли выявлять посторонние предметы (скрепки, карандаши, пальцы и т.п.), перекрывающие значимые атрибуты документа?
- Необходимо ли проверять голографическую защиту документа?

Этап 3. Аутентификация предъявителя документа

- Готовы ли вы обязать каждого клиента давать письменное согласие на передачу его биометрических данных в ЕБС?
- Готовы ли вы нести административную и уголовную ответственность при нарушениях законодательства РФ в области обработки персональных и биометрических данных в случае привлечения сервисов и краудсорсинговых структур?
- Должно ли сравнение лиц выполняться на устройстве (on-premise), чтобы избежать юридической ответственности и заключения дополнительных согласий на передачу и обработку данных?
- Требуется ли технология сравнения лиц, устойчивая к полу, расе, возрасту, макияжу?
- Требуется ли модуль, способный отличать лицо реального человека от фотографии или видеозаписи (модуль определения “живости” лица)?



smartengines.ru

117312, г. Москва, проспект
60-летия Октября, д. 9

 **+7 (495) 649 82 60**

 **sales@smartengines.ru**

2024

Разработчик систем распознавания и проверки подлинности Smart Engines | Москва | smartengines.ru
Юридическая фирма INTELLECT | Екатеринбург | www.intellect.law