

Аналитический отчет

Исследование актуальных угроз мошенничества с использованием поддельных документов

2019–2025 гг.

Условия использования

1. Права на Отчет

1.1. Настоящий Отчет, включая его название, структуру, тексты, аналитические материалы, выводы, методологию, таблицы, графики, диаграммы, инфографику, иллюстрации, подборку и систематизацию данных, а также любые его части и элементы (далее – «Отчет»), является интеллектуальной собственностью ООО «Смарт Энджинс Сервис» и ООО Агентство юридической безопасности ИНТЕЛЛЕКТ-С (далее совместно – «Правообладатели»).

1.2. Отчет может содержать материалы третьих лиц (данные из открытых источников, иллюстрации, цитаты), права на которые принадлежат их правообладателям. Настоящие Условия не предоставляют каких-либо прав на такие материалы.

1.3. Настоящие Условия не предоставляют прав на товарные знаки, фирменные наименования и иные средства индивидуализации Правообладателей, а также на программное обеспечение и технологии, упоминаемые в Отчете.

2. Принятие Условий

2.1. Получение доступа к Отчету, его скачивание, открытие, ознакомление с ним или иное использование означает, что лицо, совершившее такие действия (далее – «Пользователь»), полностью и безоговорочно принимает настоящие Условия (статьи 428 и 438 Гражданского кодекса Российской Федерации). Пользователь, не согласный с настоящими Условиями, обязан немедленно прекратить использование Отчета и удалить все его копии.

2.2. Отчет предназначен для использования в профессиональной деятельности и не предназначен для личных, семейных, домашних и иных нужд, не связанных с профессиональной деятельностью.

3. Объем предоставляемых прав

3.1. Правообладатели предоставляют Пользователю безвозмездную простую (неисключительную) непередаваемую лицензию без права сублицензирования на воспроизведение Отчета в электронной форме (включая хранение) и ознакомление с ним исключительно для внутренних нужд организации Пользователя, включая использование Отчета ее работниками при исполнении трудовых обязанностей. Лицензия действует на территории всего мира в течение срока действия исключительных прав на Отчет.

3.2. Пользователь несет ответственность за соблюдение настоящих Условий своими работниками и иными лицами, получившими доступ к Отчету через Пользователя. Передача Отчета или его частей аффилированным лицам, консультантам, подрядчикам, клиентам, партнерам и иным лицам допускается только с предварительного письменного согласия Правообладателей.

3.3. Право использования Отчета, прямо не указанное в пункте 3.1, Пользователю не предоставляется и сохраняется за Правообладателями.

3.4. Без предварительного письменного согласия Правообладателей, за исключением случаев, прямо предусмотренных законом, запрещается любое использование Отчета или его частей (включая выводы, тексты, таблицы, графики, иллюстрации и данные), кроме предусмотренного пунктом 3.1, в частности:

а) копирование и воспроизведение (включая цифровое копирование, создание снимков экрана, распечатку, запись на любые электронные и иные носители) за пределами пункта 3.1;

б) распространение, публикация, размещение в сети Интернет (в том числе на сайтах, в социальных сетях, мессенджерах, облачных хранилищах и файлообменниках) и иное доведение до всеобщего сведения, а также передача Отчета или его частей третьим лицам, в том числе в составе иных материалов;

в) перепечатка, перевод, сокращение, адаптация, пересказ, изменение, компиляция, извлечение и повторное использование данных, таблиц, графиков и иных материалов Отчета, создание на их основе производных материалов;

г) публичный показ Отчета или его частей, включая использование в презентациях, выступлениях и публикациях;

д) удаление или изменение информации об авторском праве, знаков охраны, водяных знаков и индивидуальных меток, а также обход технических средств защиты Отчета;

е) автоматизированный сбор, копирование и анализ Отчета, его использование для обучения, дообучения, тестирования и настройки моделей машинного обучения и систем искусственного интеллекта, а также загрузка Отчета или его частей во внешние сервисы искусственного интеллекта, допускающие их хранение или использование оператором сервиса.

3.5. Использование Отчета, его частей, выводов и содержащихся в нем данных в коммерческих целях допускается только с предварительного письменного согласия Правообладателей. К коммерческим целям относятся, в частности, реклама и продвижение товаров, работ и услуг; маркетинговые, PR-, тендерные, презентационные и инвестиционные материалы; собственные исследования, аналитические обзоры и рейтинги; включение в состав собственных продуктов, услуг, программного обеспечения и баз данных; использование в качестве подтверждения или обоснования качества и эффективности собственных продуктов и услуг.

3.6. Не допускается создавать впечатление, что Правообладатели одобряют, рекомендуют, спонсируют либо иным образом связаны с Пользователем, его продуктами или услугами. Наименования и товарные знаки Правообладателей могут использоваться только в форме указания источника в соответствии с п. 3.7 Условий.

3.7. При любом допустимом (на основании закона или письменного согласия Правообладателей) распространении, воспроизведении, цитировании и упоминании Отчета, его фрагментов, выводов и содержащихся в нем данных обязательно указываются все Правообладатели, название Отчета, год выпуска и ссылка на источник.

Рекомендуемая форма: «Источник: Аналитический отчет. Исследование актуальных угроз мошенничества с использованием поддельных документов, 2026 год. ООО «Смарт Энджинс Сервис» и ООО «Агентство юридической безопасности ИНТЕЛЛЕКТ-С». Указание размещается рядом с используемыми материалами в читаемом виде.

3.8. Указание Правообладателей не заменяет письменного согласия там, где оно требуется в соответствии с настоящими Условиями.

4. Целевое назначение сведений

4.1. Сведения о способах мошенничества с использованием поддельных документов, содержащиеся в Отчете, предоставляются исключительно в информационных и аналитических целях, для повышения осведомленности и противодействия мошенничеству. Запрещается использовать Отчет и содержащиеся в нем сведения для изготовления, подделки, сбыта и использования поддельных документов, обхода систем идентификации, верификации и проверки документов, совершения мошенничества и иных противоправных действий, а также для содействия им.

4.2. Правообладатели не несут ответственности за использование Отчета Пользователем или иными лицами в противоправных целях.

5. Отказ от гарантий и ограничение ответственности

5.1. Отчет носит информационно-аналитический характер, предоставляется безвозмездно на условиях «как есть» и отражает информацию по состоянию на дату его подготовки на основании источников, методологии и допущений, указанных в Отчете. Отчет не является юридической, налоговой, финансовой, технической или иной консультацией, экспертным заключением, рекомендацией к принятию каких-либо решений или публичной офертой. Упоминание в Отчете продуктов, технологий и услуг носит информационный характер.

5.2. Правообладатели не дают гарантий и заверений относительно результатов использования Отчета, точности, полноты, достоверности и актуальности содержащихся в нем сведений, отсутствия ошибок, применимости Отчета к целям и потребностям Пользователя, а также отсутствия нарушений прав третьих лиц. Правообладатели не обязаны обновлять или исправлять Отчет либо уведомлять о таких изменениях.

5.3. Использование Отчета и содержащихся в нем сведений осуществляется исключительно на риск Пользователя, который самостоятельно проверяет сведения и несет ответственность за решения, принятые на их основе.

5.4. В максимальной степени, допускаемой применимым правом, Правообладатели лица не несут ответственности перед Пользователем и третьими лицами за любые убытки (включая упущенную выгоду, ущерб деловой репутации, потерю данных, штрафы и иные потери), возникшие в связи с использованием либо невозможностью использования Отчета или содержащихся в нем сведений, в том числе в связи с решениями, принятыми на их основе, и последствиями мошеннических действий.

5.5. Правообладатели не отвечают за содержание материалов третьих лиц и внешних ресурсов, на которые Отчет содержит ссылки, а также за копии Отчета, размещенные третьими лицами.

5.6. Если Пользователь использует Отчет в предпринимательской деятельности, он обязуется по требованию возместить Правообладателям имущественные потери, возникшие в связи с претензиями третьих лиц, вызванными использованием Пользователем Отчета с нарушением настоящих Условий.

6. Ответственность за нарушение Условий

6.1. Использование Отчета с нарушением настоящих Условий, в том числе за пределами прав, предоставленных пунктом 3.1, является нарушением исключительных прав Правообладателей и настоящих Условий. Правообладатели вправе требовать прекращения нарушения, удаления и уничтожения копий Отчета, публикации решения суда о допущенном нарушении, возмещения убытков либо (по выбору Правообладателей) выплаты компенсации, а также принимать иные меры защиты, включая обращение к информационным посредникам и ограничение доступа к незаконно размещенным копиям Отчета в порядке, установленном законодательством.

6.2. В случае нарушения настоящих Условий Правообладатели вправе отказаться от предоставленной Пользователю лицензии, направив ему уведомление. С момента получения уведомления Пользователь обязан прекратить использование Отчета и удалить все его копии.

7. Заключительные положения

7.1. К настоящим Условиям применяется право Российской Федерации.

7.2. Споры, не урегулированные в претензионном порядке в течение 30 дней, подлежат рассмотрению в суде по месту нахождения ООО «Смарт Энджинс Сервис».

Аннотация

Настоящий аналитический отчет посвящен исследованию актуальных угроз мошенничества с использованием поддельных документов в России в 2019-2025 годах. Его цель – сформировать целостное представление о масштабах проблемы, динамике преступлений, наиболее распространенных видах подделок, механизмах их создания и использования, а также связанных с ними финансовых, правовых и репутационных рисках для граждан, бизнеса и государства.

Исследование объединяет экспертизу компании Smart Engines и юридической фирмы INTELLECT и опирается на статистику МВД России и Судебного департамента при Верховном Суде РФ, материалы судебной практики, открытые государственные данные и другие источники. Особое внимание уделено трансформации мошеннических схем под влиянием цифровизации и генеративного ИИ, переходу от подделки отдельных документов к созданию фиктивных личностей, а также современным подходам к комплексной проверке документов и противодействию мошенничеству.

Авторы отчета



Smart Engines – научно-технологический лидер рынка систем распознавания и проверки подлинности документов. ИИ-решения компании лежат в основе критически важных процессов – идентификации, KYC, антифрода и автоматизированной обработки документов – и используются там, где цена ошибки особенно высока: на государственных границах, в банках, в телекоммуникационных компаниях, государственных структурах и крупнейших коммерческих организациях.



INTELLECT – независимая юридическая фирма с более чем 25-летним опытом в судебных спорах и правовом консультировании бизнеса и частных клиентов. Практики INTELLECT регулярно отмечаются ведущими российскими и международными юридическими рейтингами.

В подготовке отчета также приняли участие эксперты Национального совета финансового рынка (НСФР), компаний МТС KYC Платформа, Альфа-Деньги (А Деньги) и других. Их консультации позволили дополнить исследование взглядом организаций, которые на практике сталкиваются с рисками идентификации, цифрового мошенничества, кредитного скоринга и проверки документов.

Содержание

Введение	06
-----------------	-----------

Ключевые наблюдения актуального исследования	08
Научные консультанты отчета	10
Об авторах	12
Только цифры	18

Статистика преступлений с использованием поддельных документов	20
---	-----------

Статистика МВД РФ по выявленным и расследуемым преступлениям	21
Статистика по количеству осужденных	22
Распределение осужденных по частям статьи 327 УК РФ	23
Демографические и иные признаки осужденных за подделку документов	24
Наиболее распространенные виды поддельных документов	26

Финансовые последствия мошенничества с документами	28
---	-----------

Финансовый масштаб преступлений с поддельными документами	29
Невидимая цена подделки: ущерб, который не отражает статистика	30

Как устроено мошенничество с поддельными документами	32
---	-----------

Откуда мошенники берут данные для поддельных документов?	33
Как создается поддельный документ?	35

Правовые аспекты подделки и проверки документов

Кто несет ответственность за подделку документов	41
Кто несет ответственность за проверку документов	42
ЕСИА и ЕБС не снимают ответственность с бизнеса	44

Примеры из судебной практики

Противодействие мошенничеству

Как ловят мошенников в разных каналах	53
Как устроены антифрод-системы на базе ИИ	55
Возможности антифрод-систем на базе ИИ	57

Платформа антифрода документов «Шерлок»

Антифрод	60
Проверка подлинности	62
Выявление дипфейков, синтеза с помощью VLM	64
«Антифотошоп» и выявление коллажей	65
Выявление атак на предъявление с оценкой читаемости	66
Небиометрическая сверка лиц и проверка «живости»	68
Распознавание ДУЛ всех стран мира	70
Сканеры для документов А4	72
Как «Шерлок» работает на практике: карта внедрений и результаты	74

FAQ

Глоссарий

Контакты

Введение

Поддельные документы являются одним из ключевых инструментов современных мошеннических схем. Они позволяют злоумышленникам выдавать себя за других людей, подтверждать несуществующие права и обстоятельства и получать доступ к деньгам, имуществу и услугам. Цифровизация многократно усилила потенциальный ущерб одной подделки: документ, созданный для одного сценария, может использоваться снова и снова – в разных организациях, процессах и мошеннических схемах. Последствия таких злоупотреблений затрагивают одновременно граждан, бизнес и государство, превращая мошенничество в системную угрозу для экономики.

В рамках совместного исследования **Smart Engines и юридическая фирма INTELLECT** поставили перед собой задачу сформировать для рынка целостную и объективную картину угроз, связанных с мошенничеством с использованием поддельных документов. Исследование призвано показать масштаб проблемы, ключевые тенденции, наиболее распространенные сценарии мошенничества и связанные с ними риски для граждан и бизнеса.

В отчете представлена статистика по судебным делам, связанным с фальсификацией, изготовлением и оборотом поддельных документов, данные о том, ка-

кие документы подделывают чаще всего и как эта картина изменилась с 2024 по 2025 год, детальный анализ осужденных за подделку по демографическим и иным признакам, а также наиболее показательные примеры из судебной практики.

Результаты исследования показывают не только количественный рост мошеннических атак с использованием поддельных документов, но и принципиальное усложнение самой угрозы. Схемы становятся все более изощренными и многоэтапными, а их последствия – более масштабными. Ущерб от таких преступлений неуклонно растет, а в зону риска попадают одновременно граждане, компании и государство.

Это означает, что проверка документов должна становиться частью комплексной системы противодействия мошенничеству, а не отдельной формальной процедурой. Сегодня перед коммерческими и государственными организациями стоит задача выстроить защиту так, чтобы технологии, контрольные механизмы и бизнес-процессы работали как единая система. Только такой подход позволяет эффективно противостоять мошенничеству и формировать сквозное доверие между всеми участниками цифровой экономики в условиях постоянно меняющихся угроз.

Важно

Представленные в отчете 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).

Источники данных

В основу исследования легли данные из нескольких независимых источников:

- Статистические анализы МВД России «Состояние преступности в России» за 2019-2025 гг.;
- Статистическая отчетность Судебного департамента при Верховном Суде Российской Федерации;
- Сведения о результатах рассмотрения уголовных дел за 2019-2025 гг.;
- Официальная база судебных актов ГАС «Правосудие»;
- База судебных актов Sudact;
- Российский федеральный портал открытых данных;
- Банк судебной практики СПС «ГАРАНТ»;
- Материалы официальных государственных органов и СМИ.

Ключевые наблюдения актуального исследования

01 В 2025 году произошло резкое увеличение числа преступлений, связанных с подделкой документов

Число зарегистрированных МВД преступлений, связанных с фальсификацией, изготовлением и оборотом поддельных документов, выросло на 338% – с 397 до 1 739 случаев, достигнув максимума за последние семь лет.

02 Нелегальный рынок поддельных удостоверений личности исчисляется миллиардами рублей

По минимальным оценкам, в 2025 году объем этого рынка составил около 2,6 млрд рублей.

03 Реальная цена мошенничества с документами значительно выше, чем сумма прямого ущерба

Совокупный установленный судами материальный ущерб по исследованным делам в 2025 году оценивается примерно в 1,8 млрд рублей, однако счет, открытый по поддельному паспорту, может в том числе использоваться в дроп-схемах для переводов и обналичивания похищенных средств. Даже если банк напрямую не теряет деньги, такие случаи создают дополнительные расходы на расследования и проверки, а также повышают регуляторные и репутационные риски.

04 Злоумышленники переходят от подделки отдельных документов к созданию фиктивной личности

В сложных мошеннических схемах одновременно используются паспорта, водительские удостоверения, СНИЛС, доверенности и другие документы на вымышленное или чужое имя, позволяющие поддерживать одну легенду на нескольких этапах проверки.

05

Заметно участилась подделка документов, связанных с миграцией

Количество выявленных поддельных паспортов стран СНГ и видов на жительство выросло на 41% год к году, а их доля среди рассмотренных видов поддельных документов увеличилась с 12% в 2024 году до 18% в 2025 году.

06

Каждый второй из 10 942 осужденных по ст. 327 УК РФ в 2025 году был иностранцем

Из них 5 408 человек – граждане стран СНГ, еще 66 – граждане других государств. Двенадцать осужденных вообще не имели гражданства.

07

Мошенники научились получать доступ к чужим банковским счетам в обход проверки документа самим банком

В одном из рассмотренных дел поддельный паспорт предъявили оператору мобильной связи, где процедуры проверки были мягче. Получив по нему SIM-карту и привязав ее к банковскому счету потерпевшего, злоумышленники смогли восстановить доступ к интернет-банку и похитить 4,45 млн рублей.

08

Генеративный ИИ расширяет инструментарий подделки личности

Помимо классического редактирования изображений используются полностью синтетические документы, генеративная замена текста, фотографий, подписей и печатей, а также face swap, морфинг и синтетические селфи.

09

Современное мошенничество с документами подрывает доверие между гражданами и бизнесом и требует комплексного подхода к его восстановлению

Злоумышленники объединяют украденные персональные данные, поддельные документы, синтетические изображения и методы захвата учетных записей, обходя отдельные механизмы защиты. В этих условиях бизнесу необходимы системы, обеспечивающие доверие на всех этапах взаимодействия с клиентом: от проверки подлинности документов и верификации личности до защиты персональных данных от утечек и передачи третьим лицам.

Научные консультанты отчета

Настоящий отчет подготовлен при консультационной поддержке ведущих экспертов в области искусственного интеллекта, информационной безопасности, права и противодействия мошенничеству. Их профессиональная экспертиза помогла дополнить исследование отраслевой аналитикой, практическими наблюдениями и более комплексным взглядом на ключевые угрозы и меры противодействия.



Владимир Арлазаров

Основатель и генеральный директор Smart Engines, доктор технических наук, доцент. Ведущий ученый в области искусственного интеллекта, распознавания образов и компьютерного зрения. Под его руководством разработана первая промышленная система распознавания паспорта РФ.

Автор более 140 научных публикаций, 16 патентов США и 55 патентов РФ.



Дмитрий Николаев

Технический директор Smart Engines, доктор технических наук, доцент. Ведущий российский ученый в области обработки изображений, технического зрения и вычислительной томографии.

Автор более 400 научных работ, в том числе двух научных пособий, 15 патентов США и 33 патентов РФ.



Дмитрий Загайнов

Управляющий партнер и руководитель практики уголовного права INTELLECT, адвокат, медиатор. Специализируется на уголовном праве, экономических преступлениях и корпоративных расследованиях.

Почетный адвокат России. Отмечен российскими и международными юридическими рейтингами «Право-300», «Коммерсантъ» и Best Lawyers.



Александр Золоев

Советник INTELLECT, адвокат, член исполнительного комитета Свердловского регионального отделения общероссийской общественной организации Ассоциация юристов России.

Специализируется на банкротстве, антирейдерстве и защите по уголовным делам, связанным с экономическими и должностными преступлениями. Автор научных исследований.



Иван Кузьмин

Product Owner МТС КҮС Платформа, специалист по внедрению современных способов подтверждения личности. Эксперт в области цифровой идентификации, КҮС, биометрии и технологий противодействия мошенничеству.

Отвечает за развитие платформы МТС для автоматической проверки документов, идентификации пользователей и антифрод-задач.



Константин Дедюкиев

Руководитель направления антифрода в МКК Альфа-Деньги, эксперт в области кредитного антифрода с опытом работы более 15 лет в банках и МФО. Специализируется на выявлении и предотвращении мошенничества в розничном кредитовании и микрофинансировании.

Имеет профессиональный опыт построения антифрод-процессов и защиты дистанционных кредитных продуктов от мошеннических схем.



Smart Engines – ведущий российский разработчик систем распознавания и проверки подлинности документов. Компания создает ИИ-решения для распознавания паспорта РФ и документов всех стран мира, номеров телефонов, банковских карт и QR-кодов. Технологии Smart Engines пользуются 70% жи-

телей России и больше 275 млн человек по всему миру.

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

10 лет

на рынке

130+

сотрудников

1,6 млрд

распознаваний
продано за все время

220+

клиентов по всему миру

390+

научных статей опубликовано
сотрудниками Smart Engines

100+

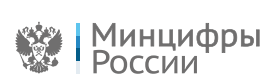
патентов и полезных моделей
получено к 2026 году

21

6 докторов наук
и 15 кандидатов наук в команде

50%

платежей по QR в России
обеспечивается ПО Smart Engines





Владимир Арлазаров

Генеральный директор Smart Engines, д.т.н.



Никогда прежде у мошенников не было такого мощного набора возможностей для создания фальсифицированных документов – и одновременно такого легкого доступа к ним. Генеративные модели искусственного интеллекта, фоторедакторы, нелегальные сервисы и другие инструменты делают создание цифровых и физических подделок все более массовым преступлением, что подтверждает статистика настоящего исследования.

Дополнительным ресурсом для злоумышленников служат многочисленные утечки персональных данных и изображений документов. Скомпрометированная информация используется не только для атак на ее владельцев, но и для обучения ИИ-моделей, с помощью которых мошенники создают все более правдоподобные подделки в значительных масштабах. В результате потенциальный объем фальсификаций многократно превышает количество документов и данных, попавших в открытый доступ.

В совокупности эти факторы привели к слоому доверия между гражданами и бизнесом. Главный вызов сегодняшнего дня – восстановить это доверие на фоне постоянно растущих рисков мошенничества и компрометации данных.

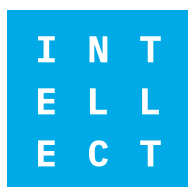
Ответом на этот вызов стала созданная нами платформа антифрода и проверки подлинности документов «Шерлок». Ее уникальная, технологически совершенная архитектура позволяет выстроить сквозное доверие между бизнесом и клиентом без посредников – от проверки документа до защиты персональных данных.

Для бизнеса «Шерлок» объединяет проверку подлинности физических и цифровых документов, комплексные сценарии идентификации и антифрода в физических и цифровых каналах. Платформа анализирует документы по множеству независимых признаков, выявляет следы подделки, генерации и цифрового вмешательства, сопоставляет данные из раз-

ных источников и проводит более 600 проверок для любых документов мира. При этом проверка выполняется внутри защищенного контура организации: чувствительные данные и изображения не передаются внешним сервисам, не сохраняются и не требуют сетевого соединения.

Для клиента это означает отсутствие сторонних сервисов, третьих лиц и операторов, получающих доступ к его персональным данным в процессе проверки. Это снижает риски компрометации и утечек информации и возвращает человеку контроль над собственными данными. Так выстраивается модель взаимного доверия: человек понимает, кому он передает свои данные и кто получает к ним доступ, а организация получает объективные основания доверять документу и клиенту и одновременно защищаться от мошенничества.

Мы убеждены: за таким доверием – будущее. Доверием, которое строится на проверяемых основаниях, прозрачных решениях и контроле над собственными данными.



INTELLECT

INTELLECT – независимая 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 (CA), Chambers Europe, Legal 500 EMEA, World Trademark Review 1000 (Великобритания), а также национальным рейтингом «Право.Ru-300».

25 лет

на рынке юридических и патентных услуг

5

офисов в России

Екатеринбург, Москва, Пермь, Санкт-Петербург, Челябинск

60+

общее количество сотрудников

40+

юристов, адвокатов и патентных поверенных в команде

25

отраслей экономики, в которых юристы сопровождают бизнес клиентов

18

юридических практик в специализации компании позволяют оказывать услуги клиентам по принципу Full Service

50%

юристов INTELLECT удостоены личной рекомендации международных и российских рейтингов юридических фирм

50%

сотрудников работают в компании более 10 лет





Дмитрий Загайнов



Управляющий партнер INTELLECT, почетный адвокат России

В ответ на развитие мошеннических схем ужесточаются требования к идентификации клиентов. Особенно заметны эти изменения в финансовом секторе, где риски противоправных действий традиционно высоки. Появляются новые законодательные требования к проведению отдельных операций и подтверждению личности клиентов, расширяются обязанности организаций по противодействию мошенничеству. Для бизнеса это означает необходимость пересматривать привычные подходы к проверке клиентов и выстраивать комплексную систему защиты, учитывающую риски на каждом этапе обслуживания.

Показательный пример – переводы без открытия банковского счета. С 30 мая 2025 года перевести таким способом по упрощенной идентификации можно не более 100 тыс. рублей. Для перевода большей суммы клиенту нужно пройти полную идентификацию либо воспользоваться своим банковским счетом. Сервисам денежных переводов, таким образом, приходится выстраивать разные сценарии проверки в зависимости от суммы операции.

Усиливается контроль и в микрофинансовом секторе. С сентября 2025 года при выдаче онлайн-займов МФО в предусмотренных случаях проверяют, принадлежат ли реквизиты для перечисления денег самому заемщику. С марта 2026 года микрофинансовые компании должны использовать Единую биометрическую систему при выдаче онлайн-займов; для микрокредитных компаний это требование вступит в силу в марте 2027 года.

Все эти нововведения – часть структурированной политики государства, направленной на усиление прозрачности и безопасности финансовой системы не только для компаний, но и простых граждан. Таким образом, все игроки выходят на новый уровень стандартов и качества, частью которого является эффективная идентификация пользователей финансо-

вых услуг.

При этом важно различать полноту идентификационных сведений и их достоверность. Совпадение имени заемщика с данными владельца счета само по себе не подтверждает подлинность предъявленного паспорта. Биометрическая проверка также не снимает вопроса о подлинности документа в тех процессах, где он используется. Если злоумышленник предъявил убедительную подделку, даже формальное соблюдение установленных процедур может создать ложное впечатление достоверности личности клиента.

Дополнительную сложность создают различия в способах предъявления и проверки документов в разных каналах обслуживания. При очном обслуживании можно исследовать физический документ и его защитные элементы; при дистанционном – организация часто работает с изображением. С юридической точки зрения важно, чтобы порядок проверки учитывал канал обращения, предусматривал действия при обнаружении противоречий и позволял восстановить основания принятого решения. Это помогает разбирать спорные случаи и совершенствовать саму процедуру.

Поэтому ужесточение требований к идентификации повышает значение технологий проверки подлинности документов. Надежная система должна оценивать множество независимых признаков: согласованность реквизитов, особенности бланка и защитных элементов, целостность изображения, следы цифрового вмешательства или генерации, соответствие документа сведениям о заявителе. Только такой подход позволит обеспечить надежную идентификацию клиентов, минимизировать риски мошенничества и выполнить требования законодательства.

**Иван Кузьмин**

Product Owner MTC KYC Платформа



Рост мошенничества с документами в последние годы перестал быть частным отраслевым явлением и превратился в системный вызов для всей экономики: угроза больше не ограничивается финансовым сектором или отдельными регулируемыми нишами, с ней сталкивается бизнес в самых разных индустриях. Сегодня ключевой вопрос сместился с «внедрять ли антифрод-технологии» на «какие именно технологии внедрять». Рынок уже осознал необходимость таких решений, но парадоксальным образом это создает новую ловушку: стремясь быстро закрыть комплаенс-требования, компании нередко выбирают примитивные или разрозненные инструменты, которые дают иллюзию защищенности, но на практике не выдерживают столкновения с реальными, постоянно изменяющимися схемами фрода.

Цена такой уязвимости складывается не только из прямых финансовых потерь. Миллионные убытки от конкретных инцидентов – самое очевидное последствие, но не менее ощутимы косвенные издержки: время и ресурсы на расследование каждого случая, штрафы со стороны регуляторов и – что часто недооценивается – репутационный урон. Доверие клиентов – хрупкий актив: если из-за уязвимости в KYC на человека оформляют десятки кредитов без его ведома (как это произошло с россиянкой, на которую оформили 60 кредитов), это не только оборачивается прямыми потерями, но и бьет по конверсии и клиентскому опыту – а такой ущерб бизнес чувствует куда дольше, чем сумму одного инцидента.

В этих условиях компании, которые полагаются на устаревшие методы проверки личности, оказываются в уязвимом положении – не потому, что не осознают риски, а потому, что скорость эволюции мошеннических схем опережает скорость модернизации таких систем. Именно поэтому принципиальное значение сегодня имеет доступность надеж-

ных антифрод-технологий для бизнеса любого масштаба – от крупных игроков до небольших компаний, у которых нет ресурсов на месяцы внедрения и собственную экспертизу в антифрод-технологиях, но есть та же потребность в защите. При этом сама технология должна быть устроена так, чтобы не создавать нового риска: не раскрывать данные пользователей мошенникам в процессе проверки и не становиться точкой утечки внутри самой системы.

Наконец, будущее эффективной защиты – не за отдельными точечными инструментами, а за комплексными платформами: от распознавания и верификации документов до детекции дипфейков и сверки лиц, работающими в единой связке. Мошеннические схемы становятся многоканальными и комбинированными, и ответом на это может быть только такая же многоуровневая, интегрированная система защиты – способная не только отражать распространенные атаки, но и предвосхищать новые угрозы по мере их изменения, оставаясь при этом доступной вне зависимости от размера бизнеса, который ее внедряет.



Константин Дедюкиев

Альфа Деньги

Руководитель направления антифрода, эксперт в области кредитного антифрода с опытом работы более 15 лет в банках и МФО

Для микрофинансового сектора мошенничество с документами – не абстрактный риск, а вполне измеримая статья потенциальных потерь. Как только злоумышленники находят слабое место в процессе проверки заявок, число попыток мошенничества с поддельными документами резко возрастает и может достигать нескольких сотен случаев с ущербом на десятки миллионов рублей. Именно поэтому сегодня недостаточно выявлять отдельные подозрительные заявки – важно оперативно закрывать обнаруженные уязвимости и постоянно адаптировать систему защиты к новым сценариям мошенничества.

Для розничного кредитования особенно опасны два сценария. Первый – кража личности, когда злоумышленник использует утекшие в сеть персональные данные жертвы и заполняет ими поддельный паспорт. С учетом количества и объемов утечек такие атаки быстро масштабируются: один мошенник может автоматически формировать большое количество заявок на разных людей. Второй сценарий – захват учетной записи благонадежного клиента. Получив доступ к устройству (смартфону) клиента, злоумышленник авторизуется в личном кабинете МФО и изменяет критичные данные – например, номер телефона или платежные реквизиты – и подтверждает изменения с помощью поддельного документа, сгенерированного ИИ. Риск здесь особенно высок, поскольку повторные клиенты часто имеют более высокие лимиты и проходят часть проверок по упрощенному сценарию.

При этом сами атаки становятся заметно разнообразнее. Мы видим шаблонные и полностью сгенерированные ИИ документы, которые создаются с помощью специализированных онлайн-сервисов или LLM/VLM-моделей. Для таких подделок характерны повторяющиеся фоны и обложки паспортов, одинаковые или схожие подписи, неестественно оформленные печати и штампы, различия в оттенках и начертании отдельных реквизитов. Нередко одни и те же элементы шаблона используются сразу в нескольких заявках, что позволяет выявлять серийный характер таких атак.

Отдельный класс мошеннических атак связан с подменой селфи. Вместо фотографии, сделанной в момент оформления заявки, злоумышленники могут использовать изображение из паспорта, фотографию из социальных сетей или один и тот же снимок в заявках разных клиентов. Все чаще встречаются синтетические селфи, полностью созданные с помощью генеративного ИИ: правдоподобность таких изображений постоянно растет, и визуально отличить сгенерированное селфи от настоящего становится все сложнее.

В этих условиях защита не может базироваться на одном источнике данных или антифрод-правиле. Для обоснованного принятия решений необходимо использовать комплекс сигналов: сведения бюро кредитных историй, данные телеком-операторов, специализированные антифрод-инструменты, характеристики устройства и интернет-сессии, историю поведения клиента и результаты проверки документов. Для заявок с повышенным чеком и сценариев, где идентификация строится по фотографии и/или скану документа, важным элементом такого контура защиты могут выступать антифрод-технологии Smart Engines. Они позволяют проверять документы и изображения на признаки цифрового вмешательства, пересъемки, подмены реквизитов, дипфейков и других видов фальсификации, дополняя поведенческие и транзакционные сигналы непосредственной проверкой самого документа.

Мошенники быстро адаптируются к новым механизмам контроля, генеративные модели становятся совершеннее, а приемы, которые еще вчера позволяли достаточно уверенно выявлять подделку, со временем теряют эффективность. Поэтому антифрод в МФО – это не отдельная проверка в процессе выдачи займа, а постоянно развивающаяся система, которая должна регулярно пересматриваться вместе с изменением самого профиля угроз. И без качественных технологий проверки подлинности документов выстроить действительно надежную комплексную защиту сегодня просто невозможно.

Только цифры

Рост числа преступлений

Зарегистрированных МВД
по ст. 327 УК РФ¹
в период с 2024 по 2025 гг.

+338%

Общее число осужденных

По ст. 327 УК РФ за последние семь лет
– в период с 2019 по 2025 гг.

69 221

Потери только банков

От внешнего мошенничества
в 2025 году по оценке Т1²

≈ 28,6 млрд
руб.

Доля иностранцев среди осужденных

За подделку документов в 2025 году

50%

¹ Статья 327 УК РФ: подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков

² Оценка рассчитана на основе данных Т1 о доле внешнего мошенничества в структуре операционных потерь банков за 2025 год

Количество новых преступлений

Зарегистрированных МВД
по ст. 327 УК РФ

397 → 1 739
2024 год 2025 год

Количество осужденных

По ст. 327 УК РФ

10 877 → 10 942
2024 год 2025 год

Объем рынка поддельных удостоверений личности

Минимальная оценка
за 2025 год

≈ 2,6 млрд
руб.

Рост числа поддельных документов мигрантов

Паспортов стран СНГ и видов
на жительство – с 2024 по 2025 гг.

+41%

Статистика преступлений с использованием поддельных документов

Статистика МВД РФ по выявленным и расследуемым преступлениям по ст. 327 УК РФ

397

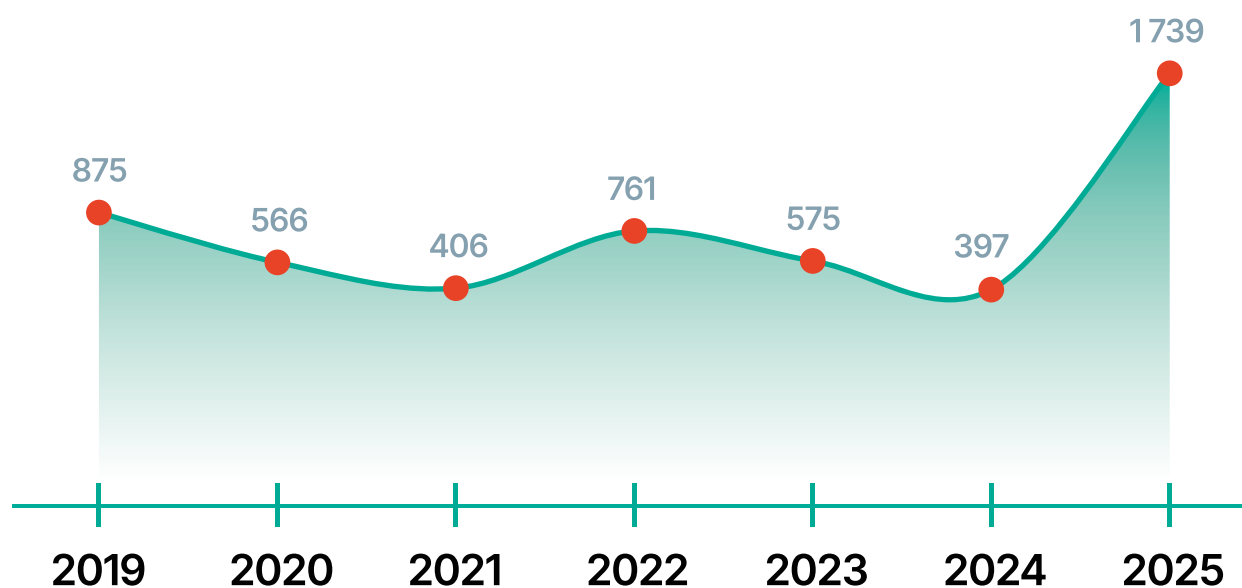
Новые преступления по ст. 327 УК РФ согласно данным МВД в 2024 году

1 739

Новые преступления по ст. 327 УК РФ согласно данным МВД в 2025 году

+338%

В 2025 году количество новых зарегистрированных МВД преступлений по ст. 327 УК РФ **выросло на рекордные 338%** по сравнению с 2024 годом и **составило 1 739 случаев. Это самый высокий показатель за последние семь лет.**



Количество преступлений по ст. 327 УК РФ, статистика МВД

Для оценки динамики из статистики МВД учитывался только показатель **новых преступлений, зарегистрированных в каждом отчетном году**. Такой подход позволяет исключить влияние преступлений прошлых лет, в том числе ранее нераскрытых, и сопоставить именно количество новых зарегистрированных случаев за одинаковые периоды.

Данные МВД отражают общую динамику преступлений, квалифицируемых по ст. 327 УК РФ. Помимо подделки и оборота паспортов, удостоверений и других официальных документов, статья охватывает ряд смежных предметов – в частности, государственные награды, медицинские книжки и др. В настоящем исследовании эти категории отдельно не рассматриваются.

Статистика по количеству осужденных по ст. 327 УК РФ

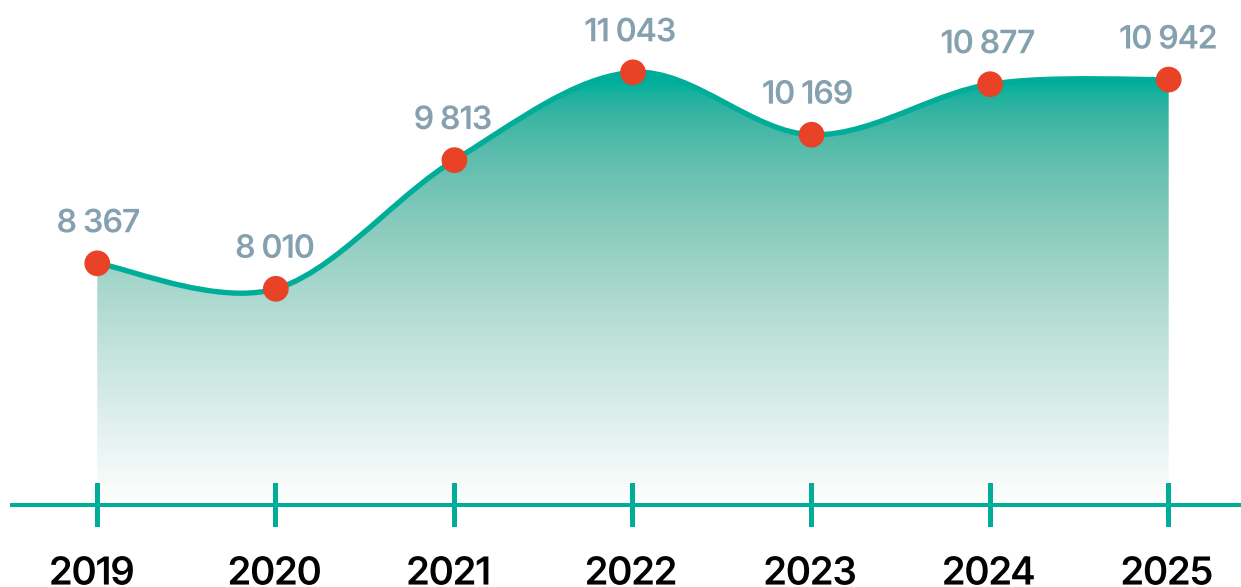
10 877

Количество осужденных
по ст. 327 УК РФ в 2024 году

+0,6%
10 942

Количество осужденных
по ст. 327 УК РФ в 2025 году

В 2025 году количество осужденных по ст. 327 УК РФ **увеличилось на 0,6%** по сравнению с 2024 годом и **составило 10 942 человека**. Положительная динамика показателя **сохраняется уже третий год подряд**. За семь лет, с 2019 по 2025 год, **совокупное число осужденных превысило 69 тыс. человек**.



Число осужденных по ст. 327 УК РФ, расчеты авторов на основе данных
ГАС «Правосудие»

Резкий рост количества преступлений в сфере подделки в 2025 году можно охарактеризовать как бум, при этом количество осужденных судами осталось на прежнем уровне. Это означает, что система юстиции еще не отреагировала на всплеск преступлений в сфере подделки документов. Таким образом, рост числа осужденных вслед за зафиксированным МВД бумом подделок может проявиться уже в статистике следующих лет.

Распределение осужденных по частям статьи 327 УК РФ



Третья часть статьи 327 УК РФ по-прежнему остается наиболее массовой: на нее приходится около 7 тыс. осужденных, тогда как по большинству других частей статьи их число измеряется сотнями.

Такой разрыв во многом объясняется самой конструкцией нормы. Часть 3

предусматривает ответственность не за изготовление подделки, а прежде всего за ее приобретение, хранение, перевозку и использование – то есть охватывает широкий круг конечных пользователей поддельных паспортов, удостоверений и других официальных документов.

Справка по частям статьи 327 УК РФ

Часть 1: подделка официальных документов, предоставляющих права или освобождающих от обязанностей, а также государственных наград, штампов, печатей и бланков в целях использования или их сбыта.

Часть 2: подделка паспорта гражданина или удостоверения, предоставляющего права или освобождающего от обязанностей, в целях использования или сбыта.

Часть 3: приобретение, хранение и перевозка в целях использования или сбыта, а также использование заведомо поддельных паспортов, удостоверений и иных официальных документов, предоставляющих права или освобождающих от обязанностей.

Часть 4: деяния, предусмотренные частями 1-3, совершенные группой лиц по предварительному сговору или организованной группой либо в целях совершения преступления на территории РФ, сокрытия другого преступления или облегчения его совершения.

Часть 5: использование заведомо подложных документов, не подпадающее под часть 3.

Демографические и иные признаки осужденных за подделку документов в 2025 году

В 2025 году количество уголовных дел, в которых фигурировали поддельные документы (ст. 327 УК РФ), составило 3 023. Всего по ст. 327 УК РФ было осуждено 10 942 человека. Чтобы понять, кто чаще всего оказывается фигурантом таких дел, рассмотрим основные характеристики осужденных: **гражданство, пол, возраст, место жительства, уровень образования, а также число участников преступления.**

Гражданство

Из общего числа осужденных около половины являются иностранными гражданами (5 408 – лица из стран СНГ, 66 – из иных государств), 12 – лица без гражданства.

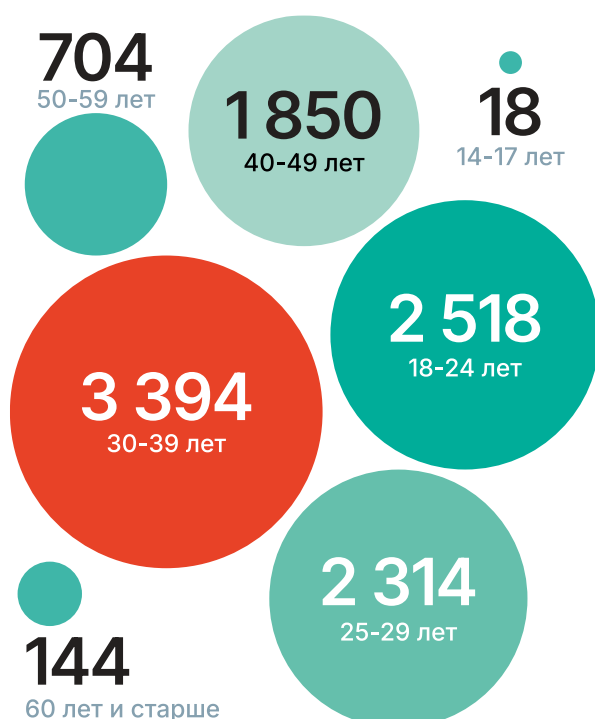


Половая принадлежность

Среди всех осужденных абсолютное большинство – мужчины (85,6%). Женщин, уличенных в подделке документов, на порядок меньше: 1 578 или 14,4%.

Возраст осужденных лиц на момент совершения преступления

В 52,2% случаев лица, подделывающие документы, находились в возрасте от 25 до 39 лет. Однако встречаются преступники как значительно моложе, так и значительно старше. «Поддельщики» были даже среди несовершеннолетних: 18 лиц (около 0,2%). В возрасте от 60 лет включительно находилось 144 лица (1,3%).



Регистрация по месту жительства

Большинство осужденных – 60,2% (6 584 лица) – являлись постоянными жителями местности, где было совершено преступление. Еще 38,2% (4 178 лиц) не имели постоянной регистрации в этой местности. 1,2% (138 лиц) составляли лица без определенного места жительства, а 0,4% (42 лица) – беженцы и вынужденные переселенцы.



Уровень образования осужденных

У 48,3% осужденных (5 284 лица) было только среднее общее образование. Еще у 10,4% (1 136 лиц) его не было вовсе либо было начальное/основное общее. Средним профессиональным (31,2%) и высшим (10,1%) образованием обладали 3 418 и 1 104 лица соответственно.

Число участников преступления

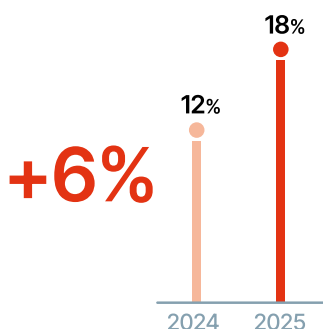
Осужденные по ст. 327 УК РФ в 98,1% случаев действовали единолично – таких лиц было 10 734. Оставшиеся 1,9% (208 лиц) совершили преступление в группе, из них 2 лица – в составе организованной преступной группы.



Наиболее распространенные виды поддельных документов

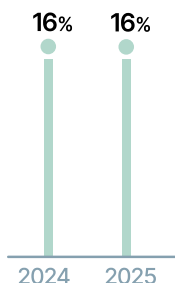
Наибольшую долю среди поддельных документов по-прежнему составляют водительские удостоверения. При этом в 2025 году существенно выросла доля документов, связанных с миграцией, в том числе паспортов стран СНГ и видов на жительство: их количество увеличилось на 41% год к году.

Паспорта стран СНГ и виды на жительство



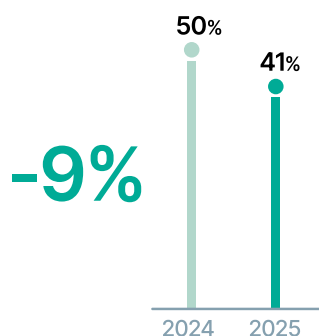
Поддельные паспорта стран СНГ используются прежде всего в схемах, связанных с легализацией пребывания иностранных граждан в России: при постановке на миграционный учет, оформлении регистрации и получении других документов, подтверждающих право на пребывание и работу в стране. Характерная особенность выявляемых случаев – относительно простые способы фальсификации, в том числе замена или переклейка фотографии в подлинном документе.

Паспорта РФ



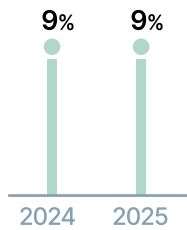
Поддельный паспорт гражданина РФ позволяет злоумышленникам действовать от имени другого человека и получать доступ к услугам и юридически значимым операциям, требующим подтверждения личности. Его могут использовать для получения кредитов и других финансовых услуг, оформления сим-карт, покупки билетов на самолет или поезд и совершения иных мошеннических действий. Чуть реже – для вступления в наследство или для проникновения в закрытые административно-территориальные образования (ЗАТО).

Водительские удостоверения



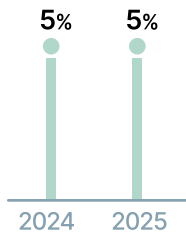
Водительские удостоверения уже несколько лет подряд остаются самым распространенным видом поддельных документов: в 2025 году на них приходится практически каждая вторая выявленная фальсификация. Судебная практика показывает типичный сценарий: поддельные права заказывают дистанционно, передавая изготовителю фотографию и персональные данные, оплачивают переводом, а готовый документ получают по почте или через службу доставки. В рассмотренных судами делах стоимость таких «прав» составляла, например, 30-80 тыс. рублей.

Служебные и военные удостоверения



Служебные и военные удостоверения подделывают прежде всего ради получения прав или освобождения от обязанностей, связанных с соответствующим статусом. Поддельное служебное удостоверение позволяет выдать себя за сотрудника государственного или правоохранительного органа, воспользоваться связанными с должностью полномочиями либо оказать давление на других лиц. Военные билеты, в свою очередь, могут подделываться для создания ложных сведений о воинском статусе и уклонения от призыва на военную службу. Однако важно понимать, что подобное нарушение будет рассматриваться уже как дезертирство и повлечет за собой более строгую ответственность.

Судебные приказы и нотариальные доверенности



Несмотря на то, что количество уголовных дел, связанных с подделкой этих типов документов, крайне невелико, в действительности они несут высокий риск и максимальный ущерб. Во-первых, это связано с большим объемом подделок. Так, в одном деле, где фигурирует подделка судебных приказов, может идти речь об обороте десятков, сотен и даже тысяч фальшивок. Во-вторых, поддельные судебные приказы и нотариальные доверенности могут наносить прямой ущерб физическим лицам. Граждане вовлекаются в незаконные операции с недвижимостью и страдают от взыскания несуществующих задолженностей.

Заграничные паспорта граждан РФ



Заграничные паспорта граждан РФ подделывают прежде всего для поездок под чужим именем: прохождения пограничного контроля, въезда и выезда из страны, покупки авиабилетов и перемещения между государствами. Поддельный документ также позволяет скрыть настоящие установочные данные человека – например, при нахождении в розыске или попытке избежать идентификации правоохранительными органами.

Финансовые последствия мошенничества с документами

Финансовый масштаб преступлений с поддельными документами

Подделка документов влечет не только правовые, но и значительные финансовые последствия. Анализ судебной практики позволяет оценить масштаб нелегального оборота подделок и ущерба от преступлений, совершенных с их использованием.

≈ 28,6 млрд руб.

Показатель: Оценка потерь только банков от внешнего мошенничества в 2025 году.

Методика расчета: Показатель рассчитан на основе данных Т1 о доле внешнего мошенничества в структуре операционных потерь банков за 2025 год.

≈ 2,6 млрд руб.*

Показатель: Ориентировочная минимальная сумма оборота черного рынка поддельных удостоверений личности в 2025 году.

Методика расчета: Показатель рассчитан на основе судебных дел, в которых была указана стоимость приобретения поддельных документов либо доход от их изготовления и сбыта. На основе выявленных сумм рассчитано среднее значение по одному делу. В выборку вошли только дела, содержащие соответствующие финансовые данные.

≈ 1,8 млрд руб.*

Показатель: Примерный совокупный установленный судами ущерб от преступлений, связанных с подделкой удостоверений личности.

Методика расчета: Показатель рассчитан как сумма материального ущерба, установленного судами по исследованным делам, связанным с использованием поддельных документов. Учитывались только дела, в которых размер причиненного ущерба был определен судом.

≈ 1,4 млн руб.*

Показатель: Средний ущерб по одному делу с установленным материальным ущербом в 2025 году.

Методика расчета: Показатель рассчитан на основе совокупного установленного ущерба и количества дел, в которых его размер был определен судом. Показатель позволяет оценить средний финансовый масштаб одного такого дела.

* Финансовые показатели рассчитаны на основе анализа судебной практики за 2025 год и носят оценочный характер. В расчет совокупного и среднего ущерба включены только дела, в которых размер причиненного ущерба был установлен судом.

Невидимая цена подделки: ущерб, который не отражает статистика

Что остается за пределами прямого ущерба?

Мошенничество с использованием поддельных документов наносит бизнесу не только прямой финансовый ущерб. Успешная подмена личности может стать отправной точкой для целой цепочки противоправных действий, последствия которых проявляются спустя месяцы и даже годы после первоначальной проверки документа. При этом отсутствие зафиксированных хищений не означает, что организация не понесла дополнительных расходов.

Особенно актуальна эта проблема для банковского сектора. Счет, открытый по поддельному паспорту, может в том чис-

ле использоваться в дроп-схемах для переводов и обналичивания похищенных средств. Подобные операции создают для банка дополнительные риски в области противодействия легализации (отмыванию) доходов и финансированию терроризма (ПОД/ФТ). Даже когда кредитной организации удастся избежать непосредственного материального ущерба, она вынуждена нести существенные расходы на расследование и урегулирование претензий пострадавших, а также сталкиваться с регуляторными последствиями.

Четыре составляющие реальной цены мошенничества с документами

1. Прямые финансовые потери

Кредитные убытки, хищения, возмещение ущерба

3. Операционные расходы

Расследования, обработка запросов, юридическое сопровождение

2. Регуляторные последствия

Предписания, штрафы, ограничения операций

4. Репутационные издержки

Жалобы клиентов, публичные претензии, снижение доверия

Эти компоненты могут возникать независимо друг от друга или одновременно, увеличивая совокупные издержки каждого инцидента.

1. Прямые финансовые потери

Поддельные документы могут использоваться для оформления кредитов, кредитных карт и овердрафтов на чужое имя, а также для получения доступа к счетам действующих клиентов и хищения денежных средств. В предусмотренных законом случаях банк обязан возместить клиенту средства, похищенные в результате операций без его добровольного согласия. В частности, ст. 9 Закона № 161-ФЗ

«О национальной платежной системе» устанавливает случаи и порядок такого возмещения.

Когда проявляется: при возникновении просроченной задолженности, выявлении хищения или поступлении претензии от настоящего владельца документа – иногда спустя месяцы после первоначальной идентификации.

2. Регуляторные последствия

Открытие счета по поддельному паспорту может также свидетельствовать об уязвимости процедур идентификации клиента. При выявлении нарушений Банк России вправе потребовать их устранения, ограничить проведение отдельных банковских операций на срок до шести месяцев, а за нарушение требований ПОД/ФТ – взыскать штраф в размере до 0,1% собственных средств кредитной организации. Если предписание регулятора не исполнено либо нарушение создает реальную угрозу интересам кредиторов или вкладчиков, возможны более стро-

гие меры, включая запрет на отдельные банковские операции на срок до одного года.

При неоднократном в течение одного года нарушении установленных законом требований и нормативных актов Банка России регулятор также вправе отозвать банковскую лицензию в соответствии с п. 6.1 ч. 1 ст. 20 Федерального закона № 395-1 «О банках и банковской деятельности».

Когда проявляется: при выявлении нарушений Банком России в рамках надзорных мероприятий.

3. Операционные расходы

После обнаружения счета, открытого по поддельному документу, может потребоваться участие сразу нескольких подразделений банка. Службы безопасности и антифрода устанавливают обстоятельства подмены личности, анализируют движение денежных средств и проверяют связанные операции. Подразделение ПОД/ФТ оценивает выявленную активность в рамках внутреннего контроля и при наличии установленных законом оснований направляет сведения в Росфинмониторинг. Юридическая служба работает с претензиями пострадавших и судебными разбирательствами.

Затраты в то же время могут возникнуть при обработке запросов Банка Рос-

сии и правоохранительных органов, дополнительной проверке и актуализации сведений о клиентах, а также устранении выявленных недостатков внутреннего контроля. Даже если инцидент не привел к непосредственным финансовым потерям банка, его расследование требует рабочего времени сотрудников и дополнительных организационных ресурсов.

Когда проявляется: с момента выявления инцидента и на протяжении его расследования и устранения последствий. Если счета банка регулярно оказываются задействованы в мошеннических схемах, связанные с этим расходы перестают быть разовыми и превращаются в постоянную операционную нагрузку.

4. Репутационные издержки

Публичная информация о повторяющихся случаях мошенничества, жалобы и претензии пострадавших негативно сказываются на доверии к кредитной организации со стороны клиентов и деловых партнеров. Особую опасность представляют случаи, когда на добросовестного клиента оформляются финансовые обязательства или злоумышленники получают доступ к его денежным средствам.

Помимо расследования самого инцидента, банку может потребоваться урегулировать претензии пострадавших и предпринять дополнительные меры для сохранения доверия клиентов.

Когда проявляется: как правило, накопительно – по мере повторения мошеннических инцидентов, появления публичных претензий и распространения информации о них.



Как устроено
мошенничество
с поддельными
документами

Откуда мошенники берут данные для поддельных документов?

Утечки и взломы информационных систем

В результате компрометации компаний и государственных организаций в распоряжении злоумышленников оказываются массивы персональных данных: ФИО, телефоны, адреса, учетные данные, реквизиты документов и другая информация. Один набор данных может неоднократно перепродаваться и дополняться сведениями из других источников.

4,5 млрд

записей персональных данных утекло в России за 2023-2025 гг.

По данным исследования ГК InfoWatch.

Инфостилеры и компрометация устройств

Вредоносные программы извлекают из зараженных устройств сохраненные пароли, cookies, данные автозаполнения, платежную и другую персональную информацию. Полученные массивы затем используются самими злоумышленниками или продаются на криминальных площадках.

83%

вредоносных рассылок содержат шпионские ПО и инфостилеры.

По данным исследования Центра кибербезопасности Ф6.

Социальные сети и OSINT (разведка по открытым источникам)

ФИО, фотографии, даты рождения, контакты, места работы, родственники и другие публично доступные сведения позволяют дополнить украденный набор данных и сформировать более полный цифровой профиль человека.

30%

россиян публиковали в социальных сетях личную информацию – в том числе номер телефона или место работы.

По данным опроса «Лаборатории Касперского».

Теневые рынки и брокеры украденных данных

На даркнет-площадках, форумах, в закрытых каналах и специализированных магазинах продаются как отдельные сведения, так и готовые наборы данных – fullz. Помимо анкетных данных, на теневом рынке встречаются фотографии и сканы паспортов, ID-карт и водительских удостоверений, учетные записи и финансовая информация.

225

ранее не опубликованных украденных баз данных обнаружено в Telegram-каналах и на даркнет-площадках в 2025 году.

По данным исследования Центра кибербезопасности Ф6.

Публичные и государственные источники

Корпоративные реестры, судебные решения, кадастровые и другие открытые базы могут содержать сведения, позволяющие подтвердить или дополнить уже имеющиеся данные о человеке. Объем доступной информации зависит от страны и установленного режима доступа.

138 млн

обращений к открытому банку данных исполнительных производств зарегистрировано в 2025 году.

По данным Федеральной службы судебных приставов.

Фишинг и социальная инженерия

Поддельные сайты, письма, сообщения и звонки используются, чтобы убедить человека самостоятельно передать персональные данные, реквизиты документов, учетные данные или их копии.

43%

интернет-ресурсов, по которым ЦБ РФ инициировал меры в 2025 году, были фишинговыми сайтами.

По данным Банка России.

Данные из разных источников могут объединяться: например, сведения из утечки дополняются фотографиями из социальных сетей, копией документа из скомпрометированного аккаунта и актуальными контактами из другой базы. Так из разрозненных фрагментов формируется цифровой профиль, достаточный для создания поддельного документа или использования чужой личности.

Как создается поддельный документ?

Условно подделки можно разделить на две большие группы: **физические**, связанные с изготовлением или изменением материального носителя, и **цифровые**. Последние, в свою очередь, могут создаваться с помощью классических инструментов редактирования изображений или технологий генеративного ИИ. При этом на практике эти методы могут сочетаться в рамках одной подделки.

Физическая подделка документов

Физические подделки предполагают вмешательство непосредственно в материальный носитель. Мошенник может изготовить документ целиком, незаконно персонализировать настоящий незаполненный бланк или изменить уже выданный документ – заменить фотографию, персональные данные, отдельные страницы или элементы защиты.

Контрафакт (Counterfeit)

Полное изготовление поддельного документа с имитацией бланка, печати, материалов и защитных элементов.

Муляж (Pseudo / Fantasy)

Документ, внешне похожий на официальный, но не существующий или не признаваемый официальным документом.

Украденный бланк (Stolen blank)

Незаконная персонализация подлинного незаполненного бланка.

Подделка (Forgery)

Замена фотографии, замена листа, наложение (overlay), Подделка отдельных элементов, вмешательство в защитный слой.

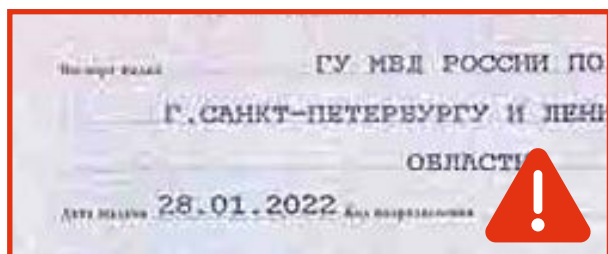
Цифровая подделка документов

Фоторедакторы

Самый доступный способ создать цифровую подделку – изменить изображение документа в фоторедакторе. Для этого не требуется изготавливать новый физический носитель: мошенник работает с фотографией или сканом настоящего документа, заменяя отдельные данные – фотографию владельца, ФИО, дату рождения, номер документа или другие поля.

Перекодирование и компрессионные уловки

Повторное JPEG-сохранение.



Вмешательство в метаданные и происхождение

Правка/очистка EXIF/XMP.



Локальный монтаж

Замена фотографии.



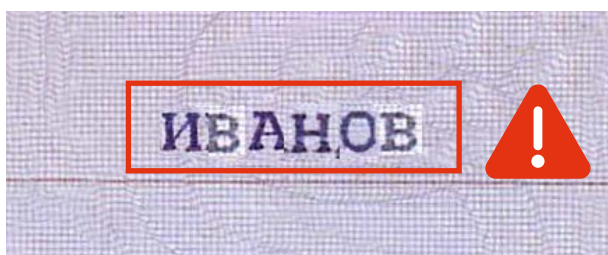
Локальный монтаж

Перерисовка текста и цифр.



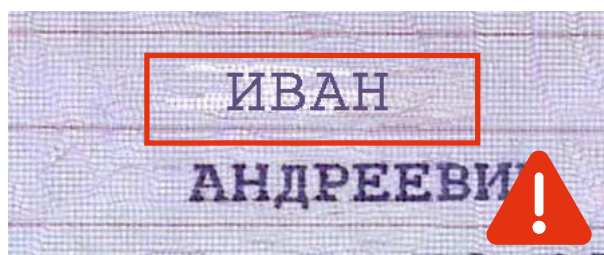
Локальный монтаж

Модификация изображения методом вставки (splicing, copy-move, inpainting).



Локальный монтаж

Erase-fill (стирание с заполнением).



Генеративный ИИ

Генеративный ИИ позволяет создавать поддельные изображения документов без ручной работы с каждым отдельным элементом. С помощью генеративных моделей можно изменить отдельные области существующего изображения – например, фотографию или текстовые поля – либо синтезировать изображение документа целиком. При этом модель не просто копирует исходные пиксели, а генерирует новое содержимое, стараясь сохранить окружающую текстуру, освещение и общий визуальный стиль документа.

Полная генерация документа по заданным параметрам

Создание синтетического изображения документа целиком.



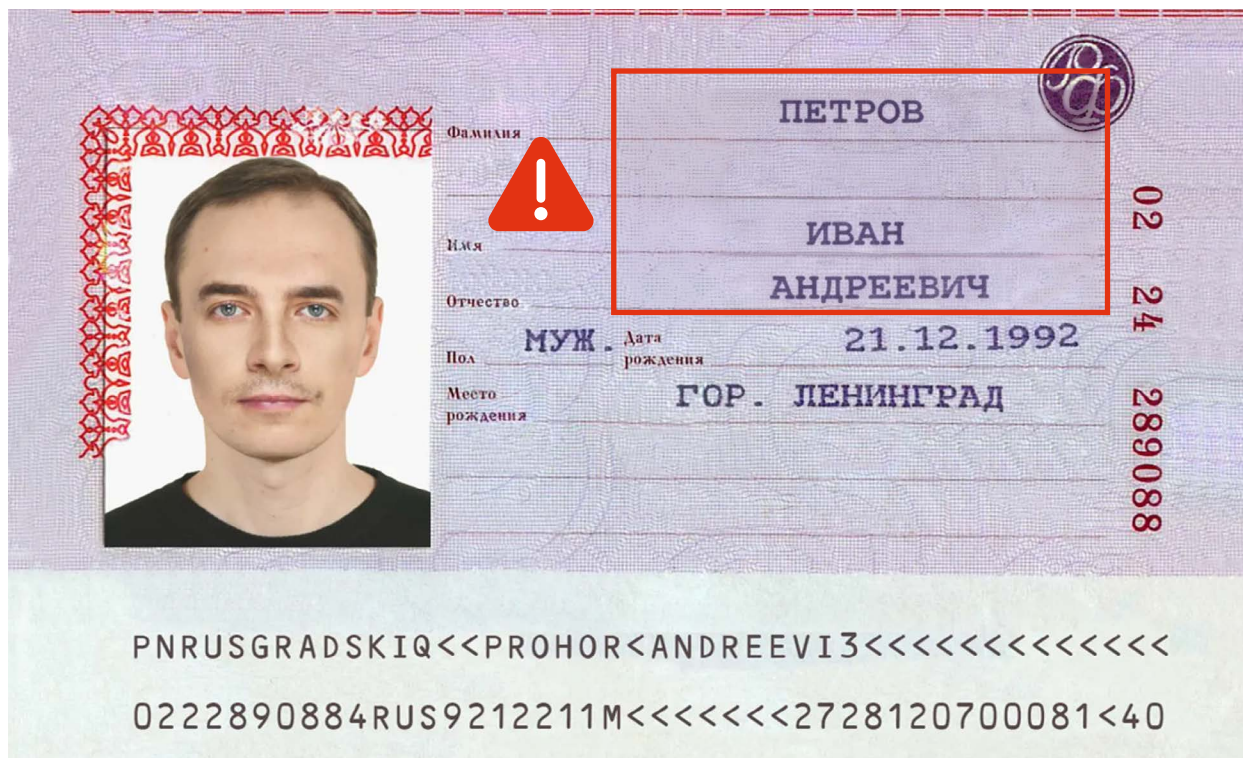
Генерация отдельных элементов

Синтез фотографий, подписей, печатей, рукописного текста, логотипов, штрихкодов и других элементов с последующей вставкой в документ.



Generative fill / Inpainting

Перегенерация выбранной области документа с сохранением окружающего фона, текстуры и визуального стиля.



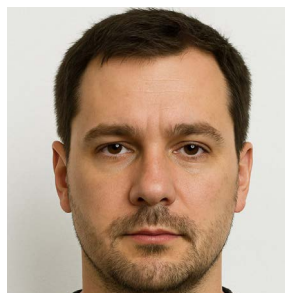
Генеративная замена текста

Создание новых ФИО, дат, номеров и других текстовых полей с воспроизведением шрифта, положения и оформления.



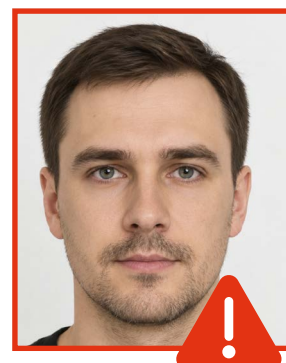
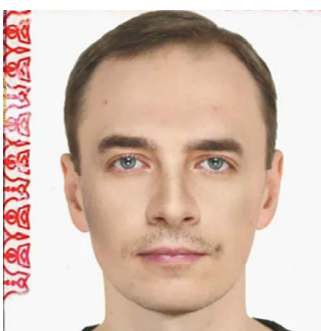
Deepfake / Face swap

Замена лица владельца документа
на лицо другого человека.



Морфинг

Создание среднего портрета из изображений двух и более людей.



Синтетическая личность

Синтетическая личность – это искусственно созданный цифровой профиль человека, сформированный из сфабрикованных данных. Синтетические профили объединяют согласованные между собой биографические сведения, данные из документов, контактные данные, изображение лица и цифровую историю. Мошенники используют такие профили для прохождения процедур идентификации и верификации клиентов (KYC – Know Your Customer) на различных платформах.

Что включает синтетическая личность?

Биографические сведения

Формируется набор персональных данных: имя и фамилия, дата рождения, пол, место проживания и другие сведения. Эти данные подбираются так, чтобы формировать правдоподобную и непротиворечивую биографию вымышленного человека.

Контактные данные

К профилю привязывается номер телефона, адрес электронной почты и другие контактные данные, благодаря которым синтетическая личность может существовать в различных онлайн-сервисах как самостоятельный пользователь.

Синтетический портрет

С применением генеративных моделей искусственного интеллекта создается изображение несуществующего человека. В результате у фиктивного профиля появляется собственное визуальное представление.

Поддельные документы

Для подтверждения вымышленной личности создаются физические или цифровые подделки документов. Таким образом, описанные ранее методы подделки становятся частью более крупной схемы – создания фиктивного человека.

Цифровой след

Для вымышленного человека формируется цифровая история: учетные записи, профили в социальных сетях и другие связанные с ним записи в онлайн-сервисах. Такой цифровой след повышает правдоподобность профиля и затрудняет его выявление при автоматизированных проверках.

История взаимодействий

Синтетическая личность может использоваться продолжительное время, постепенно накапливая историю взаимодействий с различными организациями. В финансовой сфере такие профили способны месяцами или даже годами выглядеть как обычные клиенты.

Синтетические личности могут применяться мошенниками для открытия счетов и получения финансовых продуктов, мошенничества с государственными выплатами и других схем, связанных с прохождением процедур идентификации.

Правовые аспекты подделки и проверки документов

Ответственность за подделку документов несут:

изготовители, пособники и предъявители поддельных документов

В соответствии со статьей 327 УК РФ

Подделка официального документа, предоставляющего права или освобождающего от обязанностей, в целях его использования или сбыт такого документа либо изготовление в тех же целях или сбыт поддельных государственных наград Российской Федерации, РСФСР, СССР, штампов, печатей или бланков.

Наказание

- Ограничение свободы на срок до 2 лет;
- Принудительные работы на срок до 2 лет;
- Лишение свободы на срок до 2 лет;
- Арест на срок до 6 месяцев.

Подделка паспорта гражданина или удостоверения, предоставляющего права или освобождающего от обязанностей, в целях их использования или сбыт таких документов.

Наказание

- Ограничение свободы на срок до 3 лет;
- Принудительные работы на срок до 3 лет;
- Лишение свободы на срок до 3 лет.

Приобретение, хранение, перевозка в целях использования или сбыта либо использование заведомо поддельного паспорта гражданина, удостоверения или иного официального документа, предоставляющего права или освобождающего от обязанностей, штампов, печатей или бланков.

Наказание

- Ограничение свободы на срок до 1 года;
- Принудительные работы на срок до 1 года;
- Лишение свободы на срок до 1 года.

Деяния, предусмотренные частями 1-3 статьи 327 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой, а также деяния в целях совершения преступления на территории РФ либо с целью скрыть другое преступление или облегчить его совершение.

Наказание

- Лишение свободы на срок от 2 до 6 лет со штрафом в размере до 500 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет либо без такового и с ограничением свободы на срок до 1 года либо без такового.

Использование заведомо подложного документа, за исключением случаев, предусмотренных частью третьей настоящей статьи.

Наказание

- Штраф в размере до 80 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 6 месяцев;
- Обязательные работы на срок до 480 часов;
- Исправительные работы на срок до 2 лет;
- Арест на срок до 6 месяцев.

Ответственность за проверку документов несут:

Банки и банковские сотрудники

По какому закону?

- Ст. 7 Закона № 115-ФЗ;
- Положение Банка России № 499-П;
- Ст. 74 Закона № 86-ФЗ;
- Ст. 7 Закона № 353-ФЗ;
- Ст. 241, 243 ТК РФ.

Что входит в обязанности?

Идентифицировать клиента и проверять предусмотренные законом сведения о нем, в том числе данные документа, удостоверяющего личность.

Что грозит за нарушение?

Банку: штраф до **0,1% капитала**, но не менее 100 тысяч рублей, предписание устранить нарушение, ограничение отдельных банковских операций на срок **до 6 месяцев**.

Виновному сотруднику: банк может предъявить требование о возмещении причиненного ущерба; обычно – в пределах среднего месячного заработка, а в предусмотренных законом случаях – полностью.

МФО

По какому закону?

- Ст. 7 Закона № 115-ФЗ;
- Положение Банка России № 444-П;
- Ст. 7 Закона № 353-ФЗ;
- Ст. 15.27 КоАП РФ.

Что входит в обязанности?

Идентифицировать заемщика и подтверждать достоверность установленных законом сведений, в том числе сведений документа, удостоверяющего личность.

Что грозит за нарушение?

За нарушение требований ПОД/ФТ – предупреждение или штраф **10-30 тысяч рублей** для должностных лиц и **50-100 тысяч рублей** для юридических лиц. В зависимости от конкретного состава нарушения штраф для юридического лица может достигать **1 млн рублей**, также возможно административное приостановление деятельности на срок **до 90 суток**.

Нотариусы

По какому закону?

- Ст. 42 Основ законодательства РФ о нотариате;
- Ст. 17 Основ законодательства РФ о нотариате.

Что входит в обязанности?

Устанавливать личность обратившегося по паспорту или иному документу; использовать доступные государственные информационные ресурсы, а при наличии – специальные технические средства для проверки подлинности представленных документов.

Что грозит за нарушение?

Если из-за ошибки нотариуса человеку или компании причинен ущерб, его должны возместить. За частного нотариуса ущерб возмещается за счет страхования, а если его недостаточно – **за счет имущества нотариуса** и компенсационного фонда. За государственного нотариуса ущерб возмещает государство. Также нотариус может получить дисциплинарное взыскание.

Страховые компании

По какому закону?

- Ст. 7 Закона № 115-ФЗ;
- Положение Банка России № 444-П;
- Ст. 15.27 КоАП РФ.

Что входит в обязанности?

Идентифицировать клиента, представителя, выгодоприобретателя и бенефициарного владельца в предусмотренных законом случаях.

Что грозит за нарушение?

За нарушение требований ПОД/ФТ – предупреждение или штраф **10-30 тысяч рублей** для должностных лиц и **50-100 тысяч рублей** для юридических лиц. В зависимости от конкретного состава нарушения штраф для юридического лица может достигать **1 млн рублей**, также возможно административное приостановление деятельности на срок до **90 суток**.

Сотрудники МФЦ

По какому закону?

- Ст. 16 Закона № 210-ФЗ;
- Ст. 5.63 КоАП РФ.

Что входит в обязанности?

При приеме заявления и выдаче документов устанавливать личность заявителя по паспорту или иному документу и проверять соответствие незаверенных копий их оригиналам.

Что грозит за нарушение?

Если нарушение порядка предоставления госуслуги повлекло ее непредоставление либо нарушение срока – штраф для работника МФЦ **1-1,5 тысячи рублей**. За требование не предусмотренных законом документов или платы – **1,5-3 тысячи рублей**. За повторное аналогичное нарушение – **3-5 тысяч рублей** или дисквалификация на срок до **6 месяцев**.

Операторы связи

По какому закону?

- Ст. 44 Закона № 126-ФЗ;
- Ч. 5 ст. 13.29 КоАП РФ.

Что входит в обязанности?

До начала оказания услуг проверять достоверность сведений об абоненте: ФИО, дату рождения, реквизиты документа, удостоверяющего личность, гражданство и др.

Что грозит за нарушение?

За неосуществление проверки или несоблюдение порядка – **30-50 тысяч рублей** для должностных лиц и **300-500 тысяч рублей** для юридических лиц.

Судебные приставы-исполнители

По какому закону?

- Ст. 12 Закона № 118-ФЗ;
- Ст. 13, 31 Закона № 229-ФЗ;
- Ст. 48 Закона № 328-ФЗ;
- Ст. 293 УК РФ.

Что входит в обязанности?

При совершении исполнительных действий вправе проверять документы, удостоверяющие личность, у участников исполнительного производства. При возбуждении исполнительного производства пристав также проверяет соответствие

исполнительного документа установленным законом требованиям.

Что грозит за нарушение?

За нарушение служебной дисциплины возможно замечание, выговор, строгий выговор, предупреждение о неполном служебном соответствии или увольнение со службы. Если ненадлежащее исполнение обязанностей образует состав преступления, возможна уголовная ответственность, в частности, за халатность по ст. 293 УК РФ.

ЕСИА и ЕБС не снимают ответственность с бизнеса

По данным юридического заключения
Национального совета финансового рынка.



В ряде случаев при дистанционной идентификации пользователей компании обязаны использовать государственные системы ЕСИА¹ и ЕБС². Для бизнеса это удобный способ подтвердить сведения о клиенте через его аккаунт на Госуслугах и дополнительно сверить его биометрические данные с единой базой.

Но теперь представим ситуацию: финансовая организация получает из ЕСИА подтвержденные сведения о клиенте, завершает дистанционную идентификацию и принимает его на обслуживание. Позднее выясняется, что операцию совершал мошенник. Паспорт оказался утраченным, изображение документа – отредактированным, а доступ к учетной записи – скомпрометированным.

Может показаться, что в этом случае финансовая организация не виновата. Однако на деле ответственность распределена и значительная ее доля **лежит на бизнесе**.

Оператор ЕСИА или ЕБС

За что отвечает?

За функционирование и защищенность системы, а также целостность и неизменность передаваемых через нее данных. При этом операторы ЕСИА и ЕБС **не гарантируют фактическую достоверность всей информации**, размещенной другими участниками взаимодействия.

- Подп. «б» п. 4.2 Положения, утв. Приказом Минкомсвязи России от 13.04.2012 № 107;
- Подп. «е» п. 11 Положения, утв. Постановлением Правительства РФ от 08.06.2011 № 451.

Лицо, разместившее сведения в ЕСИА или ЕБС

За что отвечает?

В предусмотренных законодательством случаях несет ответственность за достоверность размещенных им сведений.

- Ч. 3 ст. 20 Закона № 572-ФЗ.

Бизнес

За что отвечает?

Отвечает за итоговое решение о приеме клиента на обслуживание или проведении операции. Получение сведений из ЕСИА или ЕБС само по себе не освобождает от ответственности.

- Ч. 1 ст. 15.27 КоАП РФ.

Таким образом, государственная система не является универсальной гарантией того, что перед организацией находится именно тот человек, за которого он себя выдает, а предъявленный в конкретной сессии документ является подлинным.

В каких случаях ЕСИА и ЕБС обязательны?

Обязанность использовать государственные системы возникает не для любого КҮС-процесса, а в случаях, прямо предусмотренных законодательством³.

Если использование ЕСИА и ЕБС прямо предписано законом, организация обязана применять установленный государственный маршрут, а собственные технологии могут дополнять его, но не заменять. К таким случаям относятся, в частности, предусмотренные законом сценарии дистанционной идентификации клиентов микрофинансовыми организациями, а также отдельные процедуры обслуживания иностранных граждан и лиц без гражданства операторами связи.

Если прямого требования использовать ЕСИА или ЕБС нет, финансовая организация вправе применять иные предусмотренные законом источники и собственные средства проверки. Это могут быть технологии распознавания и проверки подлинности удостоверений личности, сверки лица предъявителя с фотографией в документе и другие антифрод-решения.

Вывод

Вне зависимости от обращения к ЕСИА и ЕБС организации необходимо сформировать собственный набор проверяемых оснований для принятия КҮС-решения и убедиться, что:

- Предъявленный в конкретной сессии документ подлинный, а не отредактированное, сгенерированное или переснятое изображение;
- Реквизиты документа действительны, согласованы друг с другом и не противоречат сведениям из доступных источников;
- Онбординг действительно проходит предъявитель документа, а не злоумышленник, получивший доступ к чужой учетной записи или персональным данным;
- Итоговое решение основано на совокупности проверяемых данных и может быть впоследствии обосновано перед регулятором.

Государственные системы остаются важным элементом КҮС, но **не заменяют собственную систему управления рисками** мошенничества. Поскольку итоговое решение принимает сама организация и ответственность за него остается на ней, надежная идентификация должна строиться сразу на нескольких независимых источниках – государственных сведениях, результатах анализа предъявленного документа и других внутренних проверок.

¹ Единая система идентификации и аутентификации

² Единая биометрическая система

³ Закон № 115-ФЗ, Закон № 126-ФЗ



**Примеры
из судебной практики**

Хищение средств со счетов путем подмены личности

Апелляционное определение Московского городского суда №01-0182/2025 от 02.12.2025.

Фабула:

Организованная группа получила информацию о наличии у клиента ПАО «Банк Уралсиб» значительной суммы на трех банковских счетах. Для хищения денег преступники организовали изготовление поддельного паспорта на имя владельца счетов. В паспорт была помещена фотография непосредственного исполнителя, внешне похожего на потерпевшего.

Затем один из участников группы заранее связался с сотрудниками банка, представился представителем клиента и сообщил, что тот намерен снять крупную сумму наличными. Деньги были предва-

рительно заказаны в банке. 1 марта 2024 года исполнитель приехал в офис Банка Уралсиб вместе с другим участником группы, предъявил поддельный паспорт на имя владельца счетов и после проверки документов получил в кассе банка денежные средства с трех счетов потерпевшего.

После получения денег участники вышли из банка и передали наличные другим членам группы. Один из участников, обеспечивавший проведение операции в банке, впоследствии получил 4,5 млн руб. в качестве своей доли.



Какие документы подделывали:

Подделан был паспорт гражданина РФ.

Сотрудники Банка Уралсиб при проверке паспорта не выявили признаков подделки. Внешность предъявителя соответствовала фотографии в паспорте, а детектор не выявил подозрительных признаков бланка. Впоследствии экспертиза установила, что паспорт не был изготовлен Гознаком и содержал признаки подделки: изображение и реквизиты были нанесены способом цветной электрофотографии и струйной печати.



Фактический размер причиненного ущерба:

Всего из кассы было выдано 27 782 510 руб.



Размер и вид назначенного наказания:

Суд квалифицировал действия преимущественно по ч. 4 ст. 159 УК РФ – мошенничество, совершенное группой лиц по предварительному сговору в особо крупном размере. Максимальный срок, назначенный организатору преступной схемы – 3,5 года лишения свободы.

Ипотека на чужое имя по поддельным документам

Приговор №1-10/2025 от 10.02.2025 Первомайского районного суда г. Ижевска.

Фабула:

В 2022 году в Удмуртии действовала группа лиц, организовавшая серию мошенничеств при получении кредитов в банках и МФО. Глава преступной группы подыскивала лиц, готовых за вознаграждение выступать в банках под именами других граждан, обеспечивала их поддельными документами и координировала оформление кредитов.

В частности, по эпизоду с ПАО «Банк Уралсиб» один из участников выступил покупателем квартиры, выдавая себя за другое лицо, а другой – представителем продавца. С использованием поддельных документов и нотариальной доверенности они оформили ипотечную сделку и получили из кассы банка 5 млн руб.,

которые были переданы организаторам и распределены между участниками.

По эпизоду с ПАО «Совкомбанк» участники использовали поддельные паспорта для оформления ипотечного кредита на 19,5 млн руб. Однако служба безопасности банка выявила несоответствия в представленных документах, поэтому выдача кредита была заблокирована. Таким образом, этот эпизод остался на стадии покушения на мошенничество.

Всего приговор охватывает несколько эпизодов в отношении Банка ЗЕНИТ, Руснаробанка, АТБ, ОТП Финанс, Банка Уралсиб и Совкомбанка.



Какие документы подделывали:

Суд установил использование довольно широкого набора поддельных документов. В материалах дела прямо указаны:

- Паспорта граждан РФ на имена реальных граждан;
- Водительские удостоверения;
- СНИЛС;
- Нотариальные доверенности.

Например, для оформления автокредита в Банке ЗЕНИТ был приобретен поддельный паспорт, водительское удостоверение и СНИЛС на имя другого гражданина. В эпизоде с Совкомбанком при задержании у участников были обнаружены поддельные паспорта. В эпизоде с Банком Уралсиб дополнительно использовалась поддельная нотариальная доверенность, позволявшая одному из участников представляться продавцом

квартиры и распоряжаться денежными средствами на счете, открытом на имя собственника.

Таким образом, подделка документов носила комплексный характер: преступники создавали целый пакет документов под вымышленную либо чужую личность, достаточный для прохождения банковской проверки.

**Фактический размер причиненного ущерба:****Общая сумма ущерба 9 889 151,29 руб.****2 522 637,29 руб.**

ПАО «Банк ЗЕНИТ»

4 918 017,63 руб.

ПАО «Банк Уралсиб»

2 272 244,37 руб.

АО КБ «Руснарбанк»

176 252 руб.

ООО МФК «ОТП Финанс»

**Размер и вид назначенного наказания:**

Суд квалифицировал действия преимущественно по ч. 4 ст. 159 УК РФ – мошенничество, совершенное группой лиц по предварительному сговору в особо крупном размере; по незавершенным эпизодам применена также ч. 3 ст. 30 УК РФ – покушение на преступление. Максимальный срок, назначенный организатору преступной схемы – 6 лет лишения свободы.

Перевыпуск SIM-карты по поддельному паспорту для получения доступа к банковскому аккаунту

Апелляционное определение Красноярского краевого суда № 33-992/2026 от 26.01.2026.

Фабула:

Владелец счета в АО «Райффайзен-банк» находился под стражей в СИЗО, поэтому физически не мог пользоваться своим мобильным телефоном и банковским приложением. В это время организованная группа получила доступ к его банковскому счету.

Для этого один из участников приехал в Красноярск и в салоне ПАО «МТС» предъявил поддельный паспорт на имя клиента банка. Сотрудник оператора, не распознав подделку, перевыпустил SIM-карту с телефонным номером потерпевшего. Получив контроль над номером,

преступники смогли использовать SMS-коды банка для восстановления доступа к системе «Райффайзен-Онлайн».

Затем злоумышленники связались с банком, представившись владельцем счета, и изменили привязанный к интернет-банку адрес электронной почты. После получения доступа к онлайн-банку с другого мобильного устройства со счета потерпевшего было перечислено 4,45 млн руб. на счет другого клиента Райффайзенбанка. Следствие установило, что этим счетом фактически пользовался организатор преступной группы.



Какие документы подделывали:

Подделан был паспорт гражданина РФ.

Кейс интересен тем, что поддельный паспорт был предъявлен не в банк, а оператору мобильной связи, где процедуры проверки намного мягче, чем в банке. Благодаря получению таким образом SIM-карты и ее привязки к банковскому счету потерпевшего удалось похитить денежные средства.



Фактический размер причиненного ущерба:

Всего из кассы было выдано 4 450 000 руб.



Размер и вид назначенного наказания:

Первая инстанция взыскала с Райффайзенбанка в пользу клиента 4,45 млн руб., поскольку банк не доказал отсутствие своей вины в проведении операции. Красноярский краевой суд согласился с этим выводом.

Особенно важным суд посчитал то, что у банка одновременно имелось несколько признаков потенциально мошеннической операции:

- Незадолго до перевода была заменена SIM-карта клиента;
- Банк был уведомлен оператором связи о замене SIM-карты;
- Изменился адрес электронной почты, связанный с интернет-банком;
- Вход в «Райффайзен-Онлайн» произошел с нового мобильного устройства;
- Была совершена единичная крупная операция на 4,45 млн руб., тогда как обычный оборот клиента составлял примерно 300-600 тыс. руб. в месяц.

По мнению апелляционной коллегии, совокупность этих обстоятельств должна была заставить банк распознать операцию как соответствующую признакам

перевода денежных средств без согласия клиента и принять предусмотренные законом меры для ее приостановления.

Истец предъявлял требования и к ПАО «МТС», поскольку именно сотруднику МТС был предъявлен поддельный паспорт и именно после этого была перевыпущена SIM-карта.

Однако суд отказался взыскивать деньги с оператора связи. Логика суда следующая: сотрудник МТС видел паспорт с реальными персональными данными клиента, совпадающими с информацией в базе оператора. У оператора не было биометрической информации клиента, а проверка технической подлинности паспорта требует специальных знаний.

Подобный подход означает, что банк должен усиливать механизмы аутентификации и распознавания сомнительных операций, компенсируя слабость проверки на стороне мобильных операторов. В будущем, однако, существует возможность, что обязанность по строгой проверке подлинности удостоверений личности и ответственность за халатность при проверке будет распространена и на операторов связи.



Противодействие
мошенничеству

Как ловят мошенников в разных каналах

Чтобы защититься от мошенничества при оказании финансовых и других услуг, важно проводить предварительную идентификацию и аутентификацию клиента. Это требование закреплено действующими нормативными актами.

При этом современные финансовые организации и другие компании используют несколько каналов для взаимодей-

ствия с клиентами и оказания услуг. В зависимости от формата обслуживания их можно разделить на три основные группы: **традиционные** – через отделения, **полудистанционные** – с выездом сотрудника и **дистанционные**. Рассмотрим каждый из этих каналов с точки зрения применяемых методов антифрода и необходимости использования систем на базе ИИ.

Оказание финансовых услуг в отделениях

Клиент приходит лично с физическими документами.

Риски

- Человеческий фактор (невнимательность, халатность сотрудников);
- Сговор сотрудника отделения и мошенника;
- Отсутствие полноты информации о способе проверки документов.

Системы антифрода на базе ИИ, работающие с мультиспектральными данными, полностью исключают человеческий фактор и связанные с ним риски.

Методы защиты

- Физическая проверка подлинности предъявляемых документов (в том числе с помощью мультиспектральных считывателей документов, ультрафиолетовых детекторов, цифровых увеличителей и др.);
- Проверка целостности (не рваный, не надорванный и т. п.) и валидности документа (срок действия и пр.);
- Сверка лица клиента с его фотографией в документе;
- Использование сервисов и баз недействительных документов;
- Двойное подтверждение (дополнительная проверка старшим специалистом) при совершении значимых операций.

Полудистанционное оказание услуг

Выездной сотрудник передает клиенту банковскую карту или забирает заявление на открытие счета.

Риски

- «Полевые условия» – выездной сотрудник не имеет при себе стационарных средств контроля подлинности документов (УФ/ИК, лупы/считывателя);
- Дефицит времени – выездное обслуживание и KPI на скорость подталкивают к поверхностному проведению проверок;
- Человеческий фактор – невнимательность, усталость и недостаточность квалификации.

Методы защиты

- Фотографирование удостоверения личности;
- Фотографирование клиента с паспортом;
- Фотофиксация процесса оказания услуги;
- Проверка подлинности документа по инструкциям банка;
- Проверка по базам и сервисам;
- Сверка лица клиента с фотографией в документе.

В данном случае роль ИИ – упорядочить и упростить процесс идентификации и аутентификации клиента за счет технологий распознавания и проверки подлинности, а также обеспечить ускорение процесса оказания услуги.

Дистанционное оказание услуг

Объектом проверки выступает изображение документа (скан или фотография) или видеопоследовательность.

Риски

- Трудновывяляемость подделок – даже квалифицированным специалистам требуется время, чтобы выявить вмешательство в изображение или видеопоток;
- Эффект «time pressure» в условиях конкуренции: в пиковых нагрузках время на проверку сокращается.

Методы защиты

- Первый этап – проверка на фрод. Необходимо убедиться, что объект аутентичный и не был подвержен редактированию;
- Далее – все так же, как в полудистанционном режиме.

ИИ может осуществлять проверку документов по десяткам и сотням признаков «на лету», поэтому для дистанционного формата оказания услуг он фактически незаменим.

Как устроены антифрод-системы на базе ИИ

Какие атаки детектируют, как оценивать качество работы

Антифрод-системы принципиально отличаются от базовых систем распознавания. Они предполагают глубокий комплексный анализ физических документов, изображений и видеопоследовательностей, а также работу с редкими событиями. Возможность проверки подлинности подразумевает особенно высокие требования к качеству распознавания документов.

01

Большее число операций. В отличие от систем распознавания документов антифрод-системы устроены сложнее на всех уровнях. Необходимо не только найти документ, но и выявить аномалии внутри и вне его. На уровне шаблона – не просто определить тип, а проверить ключевые защитные признаки; на уровне символов – не только распознать букву, но и оценить шрифт и способ нанесения. Все это делает разработку технологий антифрода существенно более сложной задачей.

02

Анализ обширного объема данных. На входе антифрод-система получает разнородные данные: пакеты изображений в различных спектрах, результаты распознавания с метаданными документа и его атрибутов, а также отклики специализированных модулей проверки. Лишь согласованный и комплексный анализ позволяет вынести корректное заключение.

03

Комплексный вывод. На выходе антифрод-система формирует перечень обнаруженных признаков подделки. По каждому признаку указываются как минимум два параметра: достаточность данных для его надежного выявления и вероятность наличия признака на анализируемых материалах. Дополнительно система может возвращать оценку уверенности в подлинности документа – рассчитанную либо по детерминированным правилам (взвешивание отдельных признаков), либо с помощью предобученных моделей ИИ.

04

Видит то, что не видит человек. Антифрод-системы фиксируют признаки, которые трудно заметить даже опытному сотруднику: от аномалий в распределении шума до неоднородностей фактуры печати. Такие тонкие паттерны надежно детектируются алгоритмами и служат основаниями для вывода.

Требования к качеству работы. Это ключевое отличие классического распознавания от антифрода. В первом случае часто достаточно одной метрики – ассигасы или точности (доля правильно распознанных символов/слов). В антифроде все сложнее: система сталкивается и с подлинными, и с поддельными документами, а стоимость ошибок различна.

Поэтому качество работы таких систем измеряют путем вычисления двух показателей:

- Ошибка первого рода («ложноположительное» заключение, обозначается α) – когда антифрод-система неверно «признала» подлинный документ за подделку;
- Ошибка второго рода («ложноотрицательное» заключение, обозначается β) – когда антифрод-система неверно «пропустила» подделку.

Будучи «дополнительным щитом» от мошенничества, антифрод-системы не должны мешать прохождению подлинных документов. Поэтому доля ложных срабатываний (когда подлинный документ ошибочно признается подделкой) должна быть минимальной. Современные антифрод-системы на базе искусственного интеллекта гарантируют значение ошибки первого рода на уровне не выше 0.1%, то есть ошибаются на подлинных документах не чаще одного раза на тысячу.

Почему так важно минимизировать ошибки на подлинных документах? Представим систему, которая одинаково ошибается и на подлинных, и на поддельных документах – например, с вероятностью 1% (то есть $\alpha = \beta = 0.01$). Пусть при этом подделки в потоке встречаются редко, всего в 1% случаев (примерно соответствует реальности). Возникает вопрос: какова вероятность того, что документ действительно поддельный, если система пометила его как фальшивый? Интуитивно кажется, что почти 99%.

Но на практике все иначе. Обратимся 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%.

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

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

Возможности антифрод-систем на базе ИИ

- Контроль действительности документа в части присутствующих дат;
- Контроль соответствия данных документа (например, контроль соответствия данных визуально контролируемой зоны машиночитаемой зоне);
- Проверка контрольных сумм заданного набора целевых полей;
- Контроль целостности данных (соответствия присутствующих в документе атрибутов требованиям стандартов);
- Контроль наличия обязательных атрибутов в документе (в том числе печатей и подписей);
- Детализированная проверка бланка документа на предмет правильности оформления;
- Проверка цветности документа в целом и отдельных атрибутов;
- Контроль подлинности используемых шрифтов при оформлении документа;
- Проверка динамически изменяемых элементов (например, голограмм) при распознавании в видеопотоке;
- Сверка фото в документе с лицом владельца;
- Распознавание уникальных атрибутов в графических реквизитах (например, распознавание печати в документе);
- Контроль наличия на документе защитных элементов в мультиспектральном режиме (элементов защищенной полиграфии);
- Выявление аномалий захвата изображения (в том числе выявление «пересъемки с экрана»);
- Выявление физического вмешательства в документ (переклейки фотографии, исправления реквизитов и т. д.);
- Выявление вмешательства в изображение с помощью фоторедакторов;
- Выявление синтезированных изображений, в том числе выполненных с применением методов глубокого обучения;
- Проверка документа 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 модифицированных документов**;
- Случаи предъявления **документов с истекшим сроком действия**;
- **Цифровой фрод**.

Платформа антифрода документов «Шерлок»

«Шерлок» – флагманская платформа антифрода и проверки подлинности документов компании Smart Engines, предназначенная для выявления широкого спектра мошеннических атак во всех каналах обслуживания клиентов: от отделений и точек продаж до мобильных приложений и веб-страниц.

«Шерлок» анализирует **более 600 признаков подлинности** и поддерживает **более 5 000 шаблонов документов**, включая паспорта и удостоверения личности граждан России, документы мигрантов, ДУЛ стран СНГ, БРИКС и других регионов мира. Все проверки выполняются локально: система не передает данные и изображения на обработку третьим лицам, не сохраняет их и не требует сетевого соединения. Решения строятся на принципах объяснимого ИИ, поэтому система позволяет понять, **что именно, где и почему** вызвало подозрение.

Как устроена платформа антифрода «Шерлок»?

Основу платформы составляет ядро «Шерлока» – набор базовых антифрод-технологий, необходимых для комплексной проверки документа. Оно объединяет анализ признаков подлинности, проверку NFC-чипа и голограмм, выявление пересъемки с экрана, копий и распечаток, следов графического редактирования и монтажа, генеративных подделок и атак на предъявление. Для инструментальной проверки физических документов ядро также поддерживает мультиспектральный анализ в видимом, ИК- и УФ-диапазонах.

Под конкретные задачи бизнеса возможности ядра можно расширять дополнительными модулями. Они добавляют распознавание удостоверяющих личность документов всех стран мира, небιοметрическую сверку лица предъявителя с фотографией в документе и проверку «живости», поддержку альтернативных моделей сканеров, а также работу со сканерами формата А4 для проверки доверенностей, свидетельств, справок, лицензий и других документов. Таким образом, заказчик получает не набор разрозненных решений, а единую платформу, которую можно конфигурировать под конкретный канал обслуживания, тип документов и уровень требуемой проверки.

Модули расширения функциональности

Распознавание ДУЛ всех стран мира

3 000+ типов и 5 000+ шаблонов.

Небиометрическая сверка лиц и проверка «живости»

Сверка лиц без выделения биометрических признаков, детекция атак на предъявление, кооперативная проверка «живости», выявление дипфейков.

Ядро платформы

**Антифрод и проверка подлинности документов,
удостоверяющих личность: РФ, ЕАЭС, СНГ, БРИКС**

Антифрод

Чтение и проверка чипа (NFC), проверка голограмм, выявление пересъемки с экрана, ксерокопий и распечатанных документов.

Проверка подлинности

Мультиспектральная проверка подлинности документов с помощью специализированных сканеров (ИНТЕК).

Выявление дипфейков и синтеза с помощью VLM

Обнаружение признаков вмешательства с помощью генеративного ИИ.

Выявление атак на предъявление с оценкой читаемости

Обнаружение случаев перекрытия данных пальцами, бликами, голограммами.

«Антифотешоп» и выявление коллажей

Выявление признаков графической обработки и монтажа.

Сканеры для документов формата А4

Проверка подлинности и распознавание доверенностей, свидетельств, справок, лицензий и других документов.

Альтернативные сканеры

Инструментальная проверка подлинности документов с помощью пользовательских моделей сканеров.

Модули расширения функциональности

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ГУ МВД РОССИИ ПО
Г. САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ
ОБЛАСТИ
780-011
28.01.2022

ГРАДСКИЙ

ПРОХОР

АНДРЕЕВИЧ

21.12.1992

МУЖ.

ГОР. ЛЕНИНГРАД

08 21 280088

PNRUSGRADSKIQ<<PROHOR<ANDREEVI3<<<<<<<<<<<<<<<<

0222890884RUS9212211M<<<<<<<<<<<<<4220128780011<40

11:52 rus.passport.national

-
- check_00000000000001 passed
- check_00000000000002 passed
- check_00000000000003 passed
- check_00000000000004 passed
- check_0000000001001 failed
- check_0000000001002 passed
- check_0000643000001 undefined
- check_0000643000002 undefined
- check_0000643000003 passed
- check_0000643000004 passed
- check_0000643000005 passed
- check_1000000002001 passed
- check_1000000004001 passed
- check_1000000004002 passed
- check_1000000005001 passed
- Готово
- Еще раз

Ещё раз

Ядро платформы «Шерлок»

Антифрод

Чтение и проверка чипа (NFC), проверка голограмм, выявление пересъемки с экрана, ксерокопий и распечатанных документов.

«Шерлок» проверяет документ как единую систему взаимосвязанных признаков – от правильности бланка и способа нанесения реквизитов до данных машиночитаемой зоны, штрихкодов и электронного чипа. Такой подход позволяет убедиться, что системе предъявлен именно подлинный документ, а не его копия, распечатка, изображение на экране или документ с замененными реквизитами и фотографией.

Платформа одновременно анализирует структуру и оформление документа, специальные визуальные элементы, шрифты, способы печати, фотографию владельца, печати и штампы, формат и

логику заполнения полей. Полученные данные сопоставляются между собой: информация визуальной зоны (VIZ) проверяется на соответствие MRZ, штрихкоду и данным NFC/RFID-чипа. Если один и тот же реквизит представлен в нескольких источниках, «Шерлок» выполняет их кросс-валидацию и выявляет расхождения, которые могут свидетельствовать о подмене или фальсификации.

«Шерлок» работает без обязательного использования специализированного сканера и поэтому подходит в том числе для мобильных и дистанционных сценариев.

Возможности:

- Проверка соответствия документа заявленному типу и эталонному шаблону;
- Проверка специальных визуальных элементов и особенностей дизайна бланка;
- Контроль способов нанесения и печати персональных данных и других реквизитов;
- Проверка гарнитур, начертаний и параметров шрифтов;
- Выявление признаков переклейки и замены фотографии владельца;
- Проверка наличия и характеристик печатей и штампов;
- Контроль срока действия документа;
- Сквозная проверка данных лицевой и оборотной сторон документа;
- Проверка контрольных разрядов, формата и правил заполнения реквизитов;
- Анализ логической согласованности реквизитов документа;
- Кросс-валидация данных между визуальной зоной (VIZ), MRZ, NFC/RFID-чипом и штрихкодами;
- Чтение данных электронного чипа паспорта и ID-карты через NFC, включая DG1 и DG2;
- Сопоставление фотографии владельца в документе с изображением, записанным в электронном чипе;
- Выявление пересъемки документа с экрана;
- Обнаружение ксерокопий, сканов и распечатанных документов;
- Проверка визуальных защитных элементов, включая голографические признаки;
- Выявление противоречий между отдельными реквизитами и источниками данных документа.



**Настольный
считыватель документов**



**Настольный считыватель
со встроенным ИИ**



**Встраиваемый считыватель
для киосков, банкоматов
и умных терминалов**

Ядро платформы «Шерлок»

Проверка подлинности

Мультиспектральная проверка подлинности документов с помощью специализированных сканеров ИНТЕК для отделений, офисов и точек продаж.

С помощью специализированного считывателя «Шерлок» обеспечивает проверку подлинности и действительности в трех спектральных диапазонах – видимом, инфракрасном (~870 нм) и ультрафиолетовом (~365 нм). Такой охват позволяет анализировать элементы, недоступные человеческому глазу – от УФ-люминесцентных волокон и красок до ИК-метамерных элементов. Комплексный анализ с помощью сканера для ввода и проверки подлинности углубляет контроль и снижает риск пропуска под-

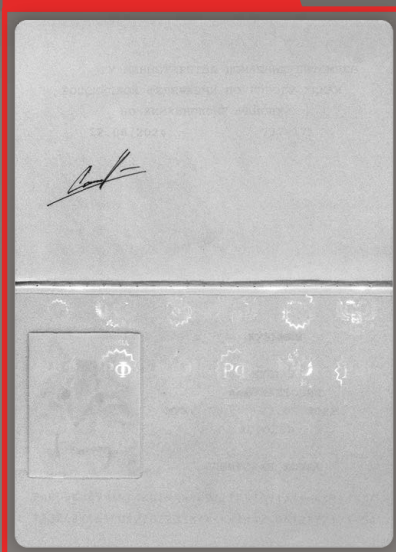
делок при поточном обслуживании. На весь процесс сканирования и проверки уходит несколько секунд.

Система позволяет проверять на подлинность документы РФ, национальные удостоверения Азербайджана, Армении, Беларуси, Казахстана, Кыргызстана, Молдавии, Таджикистана, Узбекистана, Туркменистана, а также паспорта и документы всего мира.

Видимый диапазон



Инфракрасный диапазон



Ультрафиолетовый диапазон



Возможности:

- Контроль люминесценции бланка документа в УФ-диапазоне;
- Контроль бланка и реквизитов документа в ближнем ИК-диапазоне;
- Контроль наличия, целостности и отсутствия люминесцирующих волокон и других объектов защищенной полиграфии;
- Выявление клеевых пятен и следов изменения данных, затертых областей;
- Многостраничный анализ документа;
- Выявление разрывов и надрывов документа;
- Проверка действительности документа;
- Комплексное обнаружение переклейки фотографий;
- Кросс-валидация данных основного разворота с данными машиночитаемой зоны (MRZ), RFID-чипа.

Ядро платформы «Шерлок»

Выявление дипфейков и синтеза с помощью VLM

Обнаружение признаков вмешательства, реализованных с помощью генеративного ИИ.

«Шерлок» выявляет изображения документов, полностью или частично созданные с помощью современных генеративных моделей. Система детектирует вмешательства, выполненные с использованием NanoBanana, ChatGPT, Grok, Qwen, Midjourney, Stable Diffusion, Flux и более 20 других моделей искусственного интеллекта.

В основе технологии лежит анализ микрофрагментов изображения. Вместо того чтобы искать только смысловые ошибки – например, нелогичные детали или визуальные несоответствия – «Шерлок» исследует низкоуровневую структуру изображения и выявляет статистические аномалии и характерные артефакты генерации и редактирования, которые могут быть незаметны человеческому глазу.

Это обеспечивает одинаково высокую глубину проверки вне зависимости от реалистичности дипфейка и сохраняет эффективность технологии по мере развития генеративных моделей.

Возможности:

- Выявление полностью сгенерированных изображений документов;
- Обнаружение частичных изменений реквизитов, включая точечную замену отдельных символов;
- Анализ микрофрагментов изображения для поиска статистических аномалий и артефактов генерации;
- Анализ низкоуровневых паттернов, не зависящих от смыслового содержания изображения;
- Сохранение эффективности проверки при развитии генеративных моделей за счет анализа микроструктуры изображения, а не только семантических несоответствий;
- Детекция вмешательств, выполненных с использованием NanoBanana, ChatGPT, Grok и более 20 других моделей искусственного интеллекта.



Ядро платформы «Шерлок»

«Антифотошоп» и выявление коллажей

Создано
при поддержке

Выявление признаков графической обработки и монтажа.

«Шерлок» выявляет цифровое вмешательство в изображение документа – от точечной подмены фотографии или отдельных реквизитов до создания коллажа из фрагментов нескольких изображений. Система анализирует не только содержимое документа, но и структуру самого файла: проверяет метаданные, ищет следы многократного сжатия и другие признаки, возникающие после обработки в графических редакторах.

Для обнаружения монтажа платформа выявляет вставленные и скопированные области изображения – в том числе операции **copy-move**, **copy-paste** и **splicing** – а также участки, где исходные данные

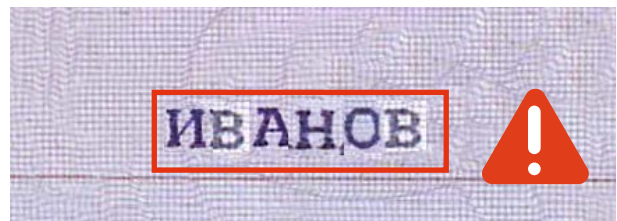
были затерты или замаскированы. Это позволяет находить коллажи и локальные изменения даже тогда, когда визуально подделка выглядит цельной и аккуратно выполненной.

Особенность технологии – возможность не просто зафиксировать факт вмешательства, но и локализовать подозрительную область. Алгоритмы анализируют цифровой «почерк» разных участков изображения и обнаруживают статистические различия между исходными и измененными фрагментами, превращая результат проверки в объяснимое основание для антифрод-решения.

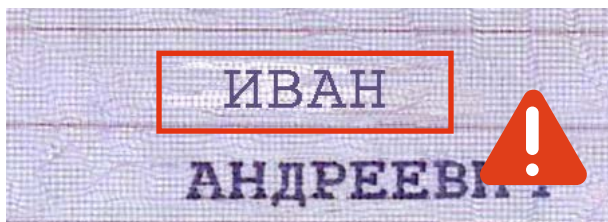
Возможности:



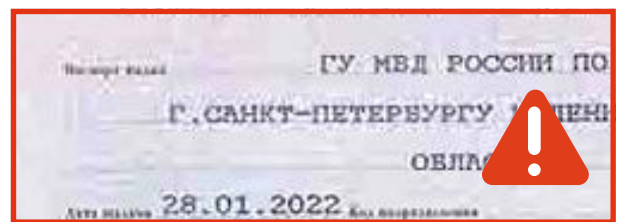
Поиск цифрового вмешательства в изображение документа.



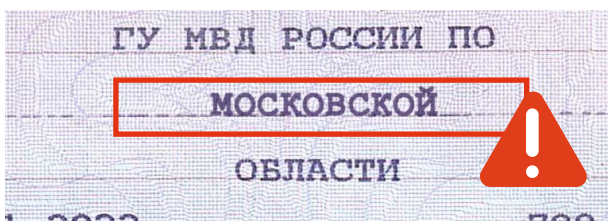
Поиск модификаций в изображении методом вставки (copy-move, copy-paste, splicing).



Обнаружение областей изображения с затертыми данными (erase-fill).



Выявление многократного сжатия изображения документа.



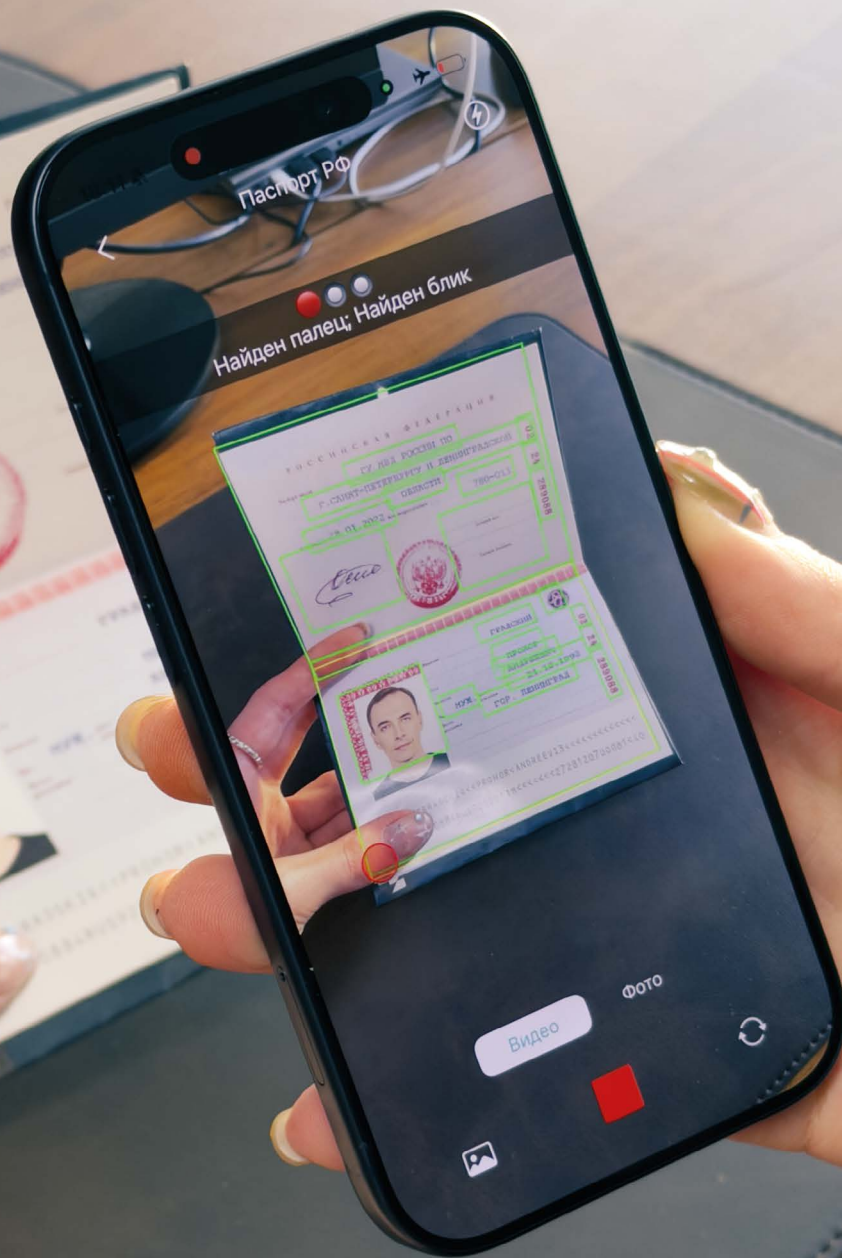
Поиск модификаций текстовых атрибутов в документе, выполненных с помощью графических редакторов.

```

"Software": "Adobe Photoshop 25.2 (Windows)",
"DateTimeOriginal": "2025:09:16 10:42:31",
"ExposureTime": "1/250",
"FNumber": "f/1.85",
"ISO": 64,
"FocalLength": "5.81 mm"
},
"IPTC": {
  "Creator": "Имя фотографа",
  "CopyrightNotice": "© 2025"
}

```

Проверка метаданных и структуры файла с изображением.



Ядро платформы «Шерлок»

Выявление атак на предъявление с оценкой читаемости

Обнаружение случаев перекрытия данных пальцами, бликами, голограммами.

«Шерлок» оценивает, насколько хорошо видны и читаемы данные документа в момент его предъявления. Для каждого кадра система размечает помехи и формирует объективную оценку читаемости полей, выявляя блики, пальцы, посторонние предметы, частичное перекрытие реквизитов и неполное попадание документа в кадр. В реальном времени платформа подсказывает пользователю, что необходимо исправить, чтобы документ соответствовал требованиям проверки.

Отдельная задача – выявление намеренных атак на предъявление. Злоумышленник может специально закрыть фотографию или отдельные поля паспорта, чтобы нарушить целостность процесса идентификации. «Шерлок» автоматически обнаруживает такие случаи, локализует перекрытые области и учитывает их при оценке каждого кадра. Благодаря этому система не просто извлекает данные, но и позволяет проверить, насколько надежными были условия, в которых они были получены.

Такой механизм особенно важен в дистанционных сценариях – при открытии счетов, оформлении продуктов, возрастной верификации и других процедурах, где пользователь самостоятельно показывает документ в камеру смартфона или компьютера.

Возможности:

- Оценка читаемости полей для каждого кадра видеопоследовательности;
- Разметка помех и перекрытий, влияющих на распознавание документа;
- Выявление бликов, пальцев, посторонних предметов и неполного попадания документа в кадр;
- Обнаружение намеренных атак на предъявление с перекрытием фотографии или отдельных реквизитов;
- Локализация проблемных областей изображения;
- Формирование подсказок пользователю в реальном времени о том, что необходимо исправить для корректного предъявления документа.



Модули расширения функциональности «Шерлок»

Небиометрическая сверка лиц и проверка «живости»

Сверка лиц без выделения биометрических признаков, детекция атак на предъявление, кооперативная проверка «живости», выявление дипфейков.

Система сверки лиц – полностью безопасный способ удаленной верификации личности без необходимости регистрировать биометрию или обращаться во внешние базы данных. Уникальный нейросетевой комплекс мгновенно сравнивает фото в документе клиента с его селфи. В качестве ответа система выдает процент уверенности, насколько два лица похожи.

Технология небиометрической сверки лиц может использоваться ровно в тех же сценариях, что и биометрические решения – начиная от удаленного открытия банковского счета, оформления страховых и заканчивая получением шеринговых услуг.

Возможности:

Устойчивость к любым условиям съемки

ИИ способен осуществлять сверку лиц как по одной фотографии человека с документом, так и по видеоселфи. Это позволяет достичь высочайшей точности распознавания за счет межкадровой интеграции векторов в латентном пространстве нейросети, возникающих при распознавании отдельных кадров. Кроме того, система автоматически устраняет aberrации камеры и распознает документ, даже если он отзеркален или снят в низком разрешении.

Проверка «живости» лица

Модуль проверки «живости» подтверждает, что перед камерой находится реальный человек, а не фотография, видеозапись, маска или другой способ имитации присутствия. Такая проверка защищает дистанционную идентификацию от атак на предъявление и дополняет небιοметрическую сверку лиц: система устанавливает не только сходство с фотографией в документе, но и сам факт присутствия живого предъявителя.

Полная конфиденциальность и безопасность

Верификация не требует наличия интернета и выполняется изолированно на смартфоне без передачи изображений на обработку на внешние серверы, в облако или сторонние сервисы. Данные остаются в контуре – такой подход гарантирует максимальную безопасность как для пользователей, так и для организаций.

Отсутствие дискриминации

ИИ устойчив к расе, полу, этнической принадлежности, макияжу, наличию усов, бороды и очков и одинаково успешно справляется с задачей сверки лиц граждан всех возрастов и стран мира.

Без биометрии = нет предмета применения 572-ФЗ, 152-ФЗ

В процессе работы модуль не использует биометрические шаблоны и не анализирует антропометрические точки, по которым вычисляются индивидуальные характеристики: форма носа, разрез глаз, расстояние между ними и др. Возникновению биометрических признаков в скрытых пространствах препятствует специальный метод обучения сквозных нейросетевых моделей.

Модули расширения функциональности «Шерлок»

Распознавание ДУЛ всех стран мира

Поддержка более 3 000 типов и 5 000 шаблонов документов.

«Шерлок» помогает организациям удостоверять личность не только граждан своей страны, но и иностранных клиентов: туристов, мигрантов, сотрудников, пассажиров, абонентов и пользователей цифровых сервисов. Система распознает паспорта, ID-карты, визы, виды на жительство, разрешения на работу и другие удостоверяющие документы разных стран, проверяет их подлинность и передает структурированные данные в KYC-, AML-, CDD- и клиентские системы.

ИИ Smart Engines распознает данные документов на английском и более чем 100 национальных языках мира. Система работает с кириллицей, латиницей, арабским письмом, ивритом, урду, фарси, китайской, японской, корейской письменностью и другими сложными графическими системами. Это позволяет автоматизировать обработку иностранных документов без ручного выбора языка и без отдельной настройки под каждый алфавит или страну. В общей сложности «Шерлок» обеспечивает распознавание данных из более чем 3 000 типов и 5 000 шаблонов документов.

Архитектура Smart Engines помогает выстраивать процессы удостоверения личности с учетом требований GDPR, CCPA, PIPL, LGPD, PDPL, DPDP Act, HIPAA и других нормативных актов в области защиты персональных данных. Обработка выполняется локально, без передачи изображений и реквизитов во внешние облачные сервисы, а подтверждение принадлежности документа предъявителю может выполняться с помощью сверки лиц без биометрии.

Возможности:

- Распознавание всего комплекта документов иностранцев: паспортов, ID-карт, виз, миграционных карт, уведомлений о прибытии, патентов, разрешений на работу, РВП, ВНЖ и др.;
- Распознавание документов 210+ стран и юрисдикций на 100+ языках;
- Автоматическое определение типа документа и его шаблона без предварительного выбора страны или языка;
- Работа с изображениями низкого разрешения, бликами, изгибами, перспективными искажениями, недостаточным освещением и неполным попаданием документа в кадр;
- Распознавание документов на смартфонах, планшетах, рабочих станциях, серверах и терминалах самообслуживания;
- Локальная обработка персональных данных без передачи изображений документов во внешние облачные сервисы;
- Поддержка нескольких поколений и вариантов оформления одного типа документа;
- Добавление новых шаблонов документов без перестройки клиентского процесса.

[illegible][illegible]

A stack of green and white ID cards. The top card is white with a green border. It features a small photo of a man in a military-style uniform. To the right of the photo is a small circular emblem. Below the photo and emblem are several fields for personal information, including 'Name', 'Date of Birth', 'Sex', 'Blood Type', 'Religion', 'Marital Status', 'Occupation', 'Address', 'Phone Number', and 'Signature'. The card also has a long alphanumeric code at the bottom. The stack of cards is placed on a green, textured surface, possibly a tablecloth.

565918
18/
ALID AL SUWAIDI
b.Emirates
990
HABI

country: *Armenia*
 surname: *Arakyan*
 surname: *Arakyan*
 given_names: *Arakyan*
 full_name: *Arakyan*
 full_name: *Arakyan*
 full_name: *Arakyan*
 date_of_birth: 15.03.1992
 place_of_birth_eng: Bishkek
 place_of_birth: БИШКЕК
 date_of_issue: 10.09.2020
 date_of_expiry: 10.09.2030
 issuing_authority_code: BK
 personal_number: 92031519920056
 address_eng: Manatka 45, u. 12, Bishkek
 address_yr: Манатка 45, к. 12, Бишкек
 license_number: 000154672
 vehicle_categories: A, B, BE, C, CE, D,
 category_restrictions: B(III) RH.

The image shows a stack of Pakistani passports. The top passport is open, displaying its data page. The passport is green and white, with the Pakistani coat of arms and the text 'ISLAMIC REPUBLIC OF PAKISTAN' and 'PASSPORT'. The data page includes fields for name, date of birth, sex, date of issue, date of expiry, and place of issue. The passport number is visible at the bottom.



Модули расширения функциональности «Шерлок»

Сканеры для документов А4

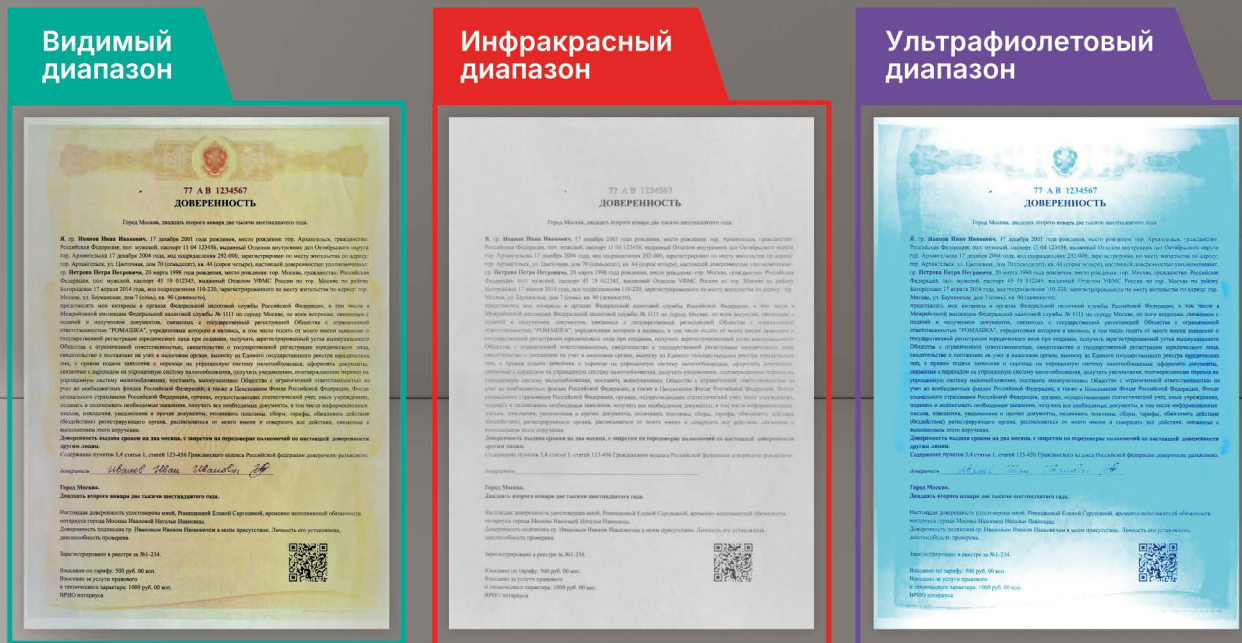
Распознавание и проверка подлинности доверенностей, свидетельств, справок, лицензий и других документов формата А4.

Модуль позволяет автоматизировать распознавание и проверку подлинности документов формата А4. Система работает с нотариальными доверенностями, судебными приказами, свидетельствами о рождении и браке, дипломами, ПТС, справками и другими защищенными документами, где важно не только извлечь данные, но и подтвердить подлинность самого бланка.

Программно-аппаратный комплекс объединяет технологии Smart Engines со специализированным мультиспектральным сканером. Система распознает данные документа и одновременно анализирует его в видимом, ультрафиолетовом и инфракрасном диапазонах. Это позволяет проверить защитные элементы, которые невозможно надежно оценить при обычном визуальном контроле: флуорес-

центные волокна и краски, особенности защищенной бумаги, ИК-признаки и другие элементы полиграфической защиты. На весь процесс сканирования, распознавания и проверки требуется несколько секунд.

ИИ анализирует не только оригинальность бланка, но и признаки вмешательства в сам документ. Система выявляет механические исправления, перепечатку реквизитов, переклейки, повреждения и другие изменения, которые могут свидетельствовать о фальсификации. Такой подход позволяет автоматизировать проверку документов, которые традиционно требуют ручного контроля специалиста, и использовать единый сценарий распознавания и антифрода в государственных структурах, банках, нотариате, HR-службах и других организациях.



Возможности:

- Распознавание и проверка подлинности документов формата А4;
- Распознавание нотариальных доверенностей, судебных приказов, свидетельств ЗАГС, дипломов, ПТС, лицензий, справок и других документов;
- Мультиспектральная проверка в видимом, ультрафиолетовом и инфракрасном диапазонах;
- Контроль оригинальности и защищенности бланка документа;
- Проверка флуоресцентных волокон, красок и других элементов защищенной полиграфии;
- Контроль свойств бумаги и особенностей печати;
- Выявление механических исправлений и следов изменения данных;
- Выявление переклеек, перепечатки и других способов физического вмешательства;
- Проверка целостности документа и отдельных его элементов;
- Одновременное распознавание данных и проверка подлинности за один цикл;
- Извлечение структурированных данных для передачи в корпоративные информационные системы.

Платформа «Шерлок» Доверие в каждом сегменте

Защита от мошенничества, антифрод и проверка подлинности документов в ключевых отраслях по всей России и за ее пределами.



Государственные границы

В международных аэропортах Шереметьево, Внуково и Кольцово «Шерлок» в составе АСПК «Сапсан» обеспечивает мгновенную проверку паспортов для бесконтактного прохождения границы.



ФЕДЕРАЛЬНАЯ
НАЛОГОВАЯ
СЛУЖБА

Государственные ведомства

«Шерлок» выявляет поддельные паспорта при выдаче электронной подписи руководителям юридических лиц и ИП в отделениях Федеральной налоговой службы (ФНС России).



Юридическая сфера

«Шерлок» используют более 7 тысяч пользователей нотариальной системы «Экспресс» по всей России для защиты делопроизводства от мошеннических атак с поддельными документами.



Бизнес

Компании из разных сфер выстраивают комплексные антифрод-сценарии для защиты от мошенничества благодаря платформе «Шерлок» при поддержке партнеров Smart Engines.



Банки

РНКО «Металлург» и «Металлинвестбанк» используют «Шерлок» при обслуживании клиентов в отделениях. Платформа автоматизирует ввод паспортных данных и проверяет подлинность документов, помогая банкам ускорить онбординг и снизить риск ошибок.



Финансовые сервисы

«Шерлок» защищает банковские и финансовые организации по всей России от открытия счетов и оформления кредитов по поддельным документам в отделениях, кассах и при дистанционном обслуживании.



Фармацевтика и розничная торговля

Платформа «Шерлок» в составе роботизированного аптечного киоска распознает и проверяет документы для подтверждения возраста при бесконтактной продаже лекарств в любое время суток.



Транспорт и логистика

«Шерлок» применяется при продаже билетов в кассах РЖД, а также в автоматических бюро для выдачи пропусков на объекты транспортной инфраструктуры, включая морские и речные порты.

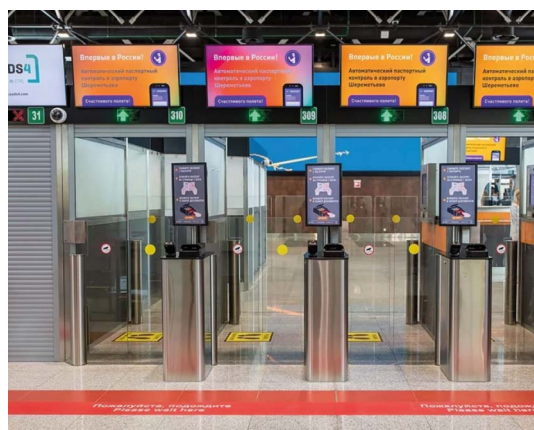
Как это работает на практике

внедрения и результаты

Бесконтактное прохождение границы за 40 секунд

Шереметьево, Внуково, Кольцово

Модули АСПК «Сапсан» с интегрированной платформой «Шерлок» от Smart Engines помогают сократить время пограничного контроля до 40 секунд и выявлять попытки предъявления поддельных документов при прохождении границы Российской Федерации. «Шерлок» за 3 секунды распознает и проверяет подлинность заграничных паспортов, обеспечивая быстрое и комфортное прохождение границы, не снижая требований к безопасности.



Оформление билетов в 6 раз быстрее

Кассы продажи билетов РЖД

Программно-аппаратный комплекс с интегрированной платформой «Шерлок» автоматически распознает реквизиты паспорта пассажира и вносит их в форму продажи билета, сокращая время ввода данных в 6 раз. Решение экономит оператору до 44 часов рабочего времени в месяц, а извлечение и анализ данных ведутся в локальной оперативной памяти – сведения о пассажире не сохраняются и не передаются в сторонние сервисы.



10 000 предотвращенных мошеннических атак МФК «Займер»

Платформа «Шерлок» надежно защищает МФК «Займер» от мошеннических атак и уже помогла предотвратить более 10 000 попыток получения займа по поддельным документам. Технология в реальном времени распознает и проверяет подлинность документов, обеспечивая непрерывную защиту сервиса и его клиентов без снижения скорости обслуживания добросовестных заемщиков.



Более 7 000 нотариусов по всей стране Система «Экспресс»

Система нотариального делопроизводства «Экспресс» благодаря платформе «Шерлок» выявляет поддельные паспорта и проводит безопасную небиометрическую сверку лица с фото в документе для предотвращения преступлений с недвижимостью, наследственными делами и незаконным переоформлением компаний. Решение используется более чем 7 000 нотариусами по всей России и обеспечивает системную защиту интересов граждан и бизнеса при совершении нотариальных действий в масштабах всей страны.



100% качество ввода данных в РКО РНКО «Металлург»

Более 10 лет РНКО «Металлург» использует платформу Smart Engines в расчетно-кассовом обслуживании. По оценкам компании, система со 100% качеством вводит данные из паспортов РФ, включая рукописные поля, и помогает ускорить расчетно-кассовое обслуживание, избавляя кассиров от риска ошибок при работе с сотнями тысяч клиентов. Сотрудник получает обоснованный результат, банк – единый стандарт контроля, а клиент проходит проверку без лишнего ожидания.



КУС и обслуживание клиентов из любых стран

Альфа-Деньги

«Шерлок» обеспечивает финансовому сервису Альфа-Деньги многоуровневую защиту от мошеннических атак при обслуживании граждан Узбекистана, Кыргызстана и Таджикистана. Платформа распознает и проверяет документы, а также проводит небиометрическую сверку лиц в мобильном приложении и веб-версии сервиса. Обработка осуществляется во внутреннем контуре Альфа-Деньги, а изображения не передаются в сторонние сервисы и облачным верификаторам, что обеспечивает безопасность персональных данных клиентов.



Мгновенная идентификация в терминалах и СКУД

«Конверста»

Компания «Конверста» применяет платформу Smart Engines в составе автоматических бюро для выдачи пропусков на объекты транспортной инфраструктуры – морские и речные порты, аэропорты. Система мгновенно извлекает необходимую информацию из документа и вносит ее в заявление на посещение. Пользователю остается только подтвердить корректность данных и получить магнитную карточку или бумажный пропуск.



Проверка паспорта при обслуживании юрлиц и ИП

Федеральная налоговая служба (ФНС России)

«Шерлок» проверяет подлинность паспортов при выдаче электронной подписи руководителям юридических лиц и ИП во всех отделениях Федеральной налоговой службы. Мультиспектральный сканер с технологиями Smart Engines анализирует изображения документа в трех диапазонах и выявляет более 80 признаков фальсификации – от механических вмешательств до переклейки фотографии, снимая нагрузку с сотрудника и исключая риски человеческого фактора.



Круглосуточная продажа лекарств без продавца

Аптечный робот, Минск-Пассажирский

Платформа Smart Engines применяется в первом роботизированном аптечном киоске на вокзале Минск-Пассажирский. В комплексе с мультиспектральным сканером технология позволяет автоматически распознавать паспорта и другие документы РФ, Беларуси и других стран СНГ и безопасно контролировать возраст покупателя при продаже лекарств – без очередей, перерывов и участия человека.



Проверка документов при обслуживании в отделениях банка

«Металлинвестбанк»

«Металлинвестбанк» применяет платформу Smart Engines для проверки подлинности документов при обслуживании в отделениях по всей России. Сотруднику банка достаточно положить паспорт на считывающую поверхность – данные автоматически распознаются, документ проверяется на подлинность в трех диапазонах, а информация передается в учетную систему, избавляя от рисков ошибок и ускоряя обслуживание клиентов при любых банковских операциях, требующих предъявления паспорта.



FAQ

10 вопросов, на которые бизнес должен знать ответ

01 Каков масштаб проблемы с поддельными документами?

Мошенничество с использованием поддельных документов уже давно представляет системную угрозу для граждан, бизнеса и государства, однако в последние годы проблема заметно обострилась. С 2024 по 2025 год число новых зарегистрированных МВД России преступлений по ст. 327 УК РФ (фальсификация, распространение и оборот поддельных документов) выросло на **338% – с 397 до 1 739 случаев**. Всего за 2025 год по этой статье было осуждено **10 942 человека**.

Финансовый масштаб проблемы исчисляется миллиардами рублей. По минимальным оценкам, объем неле-

гального рынка поддельных удостоверений личности в 2025 году составил около **2,6 млрд рублей**, а совокупный материальный ущерб, установленный судами по исследованным делам, – порядка **1,8 млрд рублей**.

При этом статистика отражает лишь часть реального масштаба проблемы: поддельный документ нередко становится только одним из элементов более сложных преступных схем, квалифицирующихся по другим статьям УК РФ. За пределами статистики также остаются невыявленные подделки и множество предотвращенных попыток мошенничества.

02 Какие документы подделывают чаще всего и для чего их используют?

По данным анализа судебной практики, наиболее распространенным видом поддельных документов в 2025 году стали **водительские удостоверения** – их доля составила 41% от общего объема подделок. Права приобретают прежде всего для управления транспортными средствами, в частности, лица, ранее лишенные водительского удостоверения.

На втором месте находятся **паспорта стран СНГ и виды на жительство** – их доля составила 18%. При этом с 2024 по 2025 год количество поддельных документов этой категории увеличилось на 41%. Фальсифицированные

паспорта стран СНГ, как правило, используются для подтверждения личности, постановки на миграционный учет, оформления регистрации и других процедур, связанных с правом на пребывание и работу в России.

Паспорта граждан РФ составили 16% выявленных подделок. Их мошенники используют, чтобы выдавать себя за другого человека, получать кредиты и другие финансовые услуги, оформлять SIM-карты, проводить операции с денежными средствами и совершать иные действия, требующие подтверждения личности.

03 Откуда мошенники получают персональные данные для создания подделок?

Основным источником данных для создания поддельных документов становятся утечки и взломы информационных систем, теневые рынки украденных данных, фишинг, вредоносные программы и открытые источники. В распоряжении злоумышленников могут оказаться ФИО, дата рождения, адрес, телефон, паспортные реквизиты, фотографии и сканы документов, учетные данные и другая персональная информация.

Полученные сведения обычно не используются по отдельности. Мошенники объединяют данные из разных источников: например, сведения

из утечки дополняют фотографиями из социальных сетей, копией паспорта из скомпрометированного аккаунта и актуальными контактами из другой базы. Так формируется цифровой профиль человека, достаточный для создания **целого пакета поддельных документов**.

Отдельную роль играет социальная инженерия. Поддельные сайты, письма, сообщения и звонки позволяют убедить человека самостоятельно передать персональные данные, реквизиты документов или их копии, которые затем могут использоваться в дальнейших мошеннических схемах.

04 Как генеративный ИИ изменил технологии подделки документов?

Генеративный ИИ **значительно снизил порог входа** для создания цифровых подделок и расширил набор доступных мошенникам инструментов. Если раньше для изменения паспортных реквизитов, фотографии или других элементов документа требовались навыки работы с графическими редакторами, то сегодня многие такие операции можно выполнять с помощью генеративных моделей.

С их помощью злоумышленники могут создавать полностью синтетические изображения документов, изменять отдельные реквизиты, генерировать новые фотографии, подписи и печати, подменять лица на изображениях и создавать морфированные портреты. Современная антифрод-система должна уметь выявлять все перечисленные типы вмешательства и обнаруживать даже незаметные человеческому глазу следы генерации.

05 Из чего складывается ущерб от мошенничества с документами?

Ущерб от мошенничества с поддельными документами не ограничивается похищенными средствами. Для бизнеса реальная цена одного инцидента складывается сразу из **четырёх компонентов**: прямых финансовых потерь, регуляторных последствий, операционных расходов и репутационных издержек.

Прямые потери возникают, например, при оформлении кредитов на чужое имя или получении доступа к счетам действующих клиентов. Дополнительно организация может столкнуться с требованиями регулятора, штрафами и ограничениями, а также нести расходы на внутренние рассле-

дования, работу служб безопасности, антифрода, ПОД/ФТ и юристов, обработку запросов государственных органов и устранение выявленных недостатков.

Даже если мошенничество не привело к непосредственной потере денег, последствия могут сохраняться длительное время. Повторяющиеся инциденты, жалобы пострадавших и публичная информация о случаях мошенничества способны снижать доверие клиентов и деловых партнеров. Поэтому фактический ущерб от одной подделки может быть значительно выше суммы, непосредственно похищенной злоумышленниками.

06 Могут ли мошенники получить доступ к счету, не проходя идентификацию в банке?

Да. Мошенники могут атаковать не сам банк, а другую организацию, через которую впоследствии получают доступ к банковскому аккаунту. В одном из рассмотренных дел злоумышленники предъявили поддельный паспорт оператору мобильной связи и добились перевыпуска SIM-карты. С помощью полученного номера преступники восстановили доступ к интернет-банку и похитили со счета **4,45 млн рублей**.

Этот инцидент доказывает, что на-

дежные технологии проверки документов на подлинность необходимы не только банкам и другим кредитным организациям. **Мошенники зачастую атакуют самое слабое звено в цепочке идентификации**, поэтому антифрод-технология должна применяться везде, где подтверждение личности может стать ключом к дальнейшему доступу к счетам и учетным записям клиентов.

07 Какую ответственность несет бизнес за проверку документов?

Требования к проверке документов зависят от отрасли и конкретного сценария обслуживания. Банки, МФО, страховые компании, операторы связи и другие организации обязаны устанавливать личность клиента и проверять предусмотренные законом сведения, в том числе данные удостоверяющего личность документа.

Последствия нарушения могут быть существенными. Например, для банков возможно ограничение отдельных операций на срок до шести ме-

сяцев и штраф **до 0,1% собственных средств кредитной организации**. Для МФО и страховых компаний за отдельные нарушения требований ПОД/ФТ предусмотрены штрафы, достигающие **1 млн рублей**, а также административное приостановление деятельности до 90 суток. Для операторов связи нарушение порядка проверки сведений об абоненте может повлечь штраф **до 500 тысяч рублей**.

08 Можно ли выявить качественную подделку при обычной визуальной проверке?

Далеко не всегда. Современные подделки могут быть выполнены настолько качественно, что их практически невозможно обнаружить на глаз. Показательный пример содержится в одном из рассмотренных в исследовании уголовных дел. Мошенник предъявил в отделение банка поддельный паспорт на имя владельца счета. Сотрудники проверили документ, однако не выявили никаких признаков подделки. Позднее экспертиза установила, что паспорт не был изготовлен Гознаком, а изображе-

ния и реквизиты были нанесены с помощью цветной электрофотографии и струйной печати.

Поэтому визуальный осмотр не должен быть единственным уровнем защиты. Для надежной проверки необходимо одновременно анализировать соответствие документа эталонному шаблону, способы нанесения реквизитов, защитные элементы, фотографию владельца, согласованность данных и сотни других признаков возможной фальсификации.

09 Можно ли не проверять документ, если данные клиента подтверждены через ЕСИА или ЕБС?

Нет. Получение подтвержденных сведений о клиенте через ЕСИА или ЕБС **не освобождает организацию от ответственности** за итоговое решение о его идентификации и приеме на обслуживание. Операторы государственных систем отвечают за их функционирование, защищенность и неизменность передаваемых данных, но **не гарантируют фактическую достоверность** всей информации, размещенной другими участниками.

Поэтому даже при использовании ЕСИА и ЕБС бизнесу необходимо сформировать собственный набор оснований для принятия KYC-решения: убедиться, что предъявленный в конкретной сессии документ не был подделан, отредактирован или сгенерирован, его реквизиты действительны и согласованы между собой, а идентификацию действительно проходит владелец документа.

10 Как проверить клиента и не создать лишних рисков для его персональных данных?

Безопасная идентификация должна быть устроена так, чтобы для проверки клиента не требовалось передавать изображения его документов и персональные данные лишним участникам процесса. Чем больше внешних сервисов, посредников и точек хранения задействовано в проверке, тем выше риск компрометации чувствительной информации.

Снизить этот риск позволяет ло-

кальная обработка: распознавание документов и проверка их подлинности могут выполняться **на устройстве клиента или внутри защищенного контура организации**, без передачи изображений и реквизитов во внешние сервисы. Такой подход позволяет бизнесу одновременно проверить подлинность документа и сохранить полный контроль над персональными данными клиента.

Глоссарий

Глоссарий Smart Engines – справочник по ключевым терминам в области распознавания и проверки документов на подлинность, компьютерного зрения и цифровой идентификации. Здесь собраны определения технологий и процедур, типов документов, а также требований законодательства, связанных с защитой персональных данных.

Антифрод

Комплекс технологий и методов, предназначенных для выявления и пресечения мошеннических действий. При проверке удостоверений личности антифрод позволяет обнаруживать признаки манипуляций с документами – антифрод-система «Шерлок Зо» от Smart Engines выявляет более 600 таких признаков, включая дипфейки. Система одновременно анализирует изображения документов в разных спектрах, видеопоследовательности, текстовые поля, данные NFC-чипа, штрихкоды, метаданные и сигнатуры.

Паспорт РФ

Основной документ, удостоверяющий личность гражданина Российской Федерации, и ключевой источник данных для идентификации клиентов при оказании финансовых, государственных и других услуг. Система распознавания паспорта Smart Engines извлекает информацию со всех страниц документа, включая рукописные и печатные реквизиты, и возвращает данные в структурированном виде, помогая автоматизировать KYC и исключить ручной ввод данных.

ВНЖ

Вид на жительство – документ, подтверждающий право иностранного гражданина или лица без гражданства постоянно проживать на территории определенного государства. Технологии Smart Engines распознают ВНЖ России, СНГ, БРИКС и других стран мира на более чем 100 языках, а также выявляют признаки подделки как в физических, так и в цифровых каналах обслуживания.

ПОД/ФТ

Противодействие отмыванию доходов и финансированию терроризма – комплекс мер по выявлению и пресечению операций, связанных с легализацией преступных доходов и финансированием терроризма. На территории РФ требования в этой сфере закреплены в Федеральном законе № 115-ФЗ. Технологии Smart Engines автоматизируют распознавание и проверку документов при идентификации клиентов, помогая финансовым организациям выполнять требования ПОД/ФТ.

РВП

Разрешение на временное проживание – документ, подтверждающий право иностранного гражданина временно проживать на территории определенного государства. РВП часто используется для идентификации при трудоустройстве, получении финансовых, государственных и других видов услуг. Технологии Smart Engines выполняют распознавание документов мигрантов, включая РВП, автоматически извлекают необходимые сведения и помогают ускорить обслуживание или трудоустройство иностранных граждан.

API

Application Programming Interface – программный интерфейс, который позволяет разным приложениям и системам обмениваться данными и командами по заранее установленным правилам. API упрощает интеграцию программных продуктов и помогает автоматизировать обмен информацией между ними. Например, через API система распознавания документов может получать изображения из мобильного или веб-приложения и возвращать извлеченные и структурированные данные: имя, дату рождения, номер документа и другие.

HTR

Handwritten Text Recognition – технология автоматического распознавания рукописного текста и преобразования его в редактируемый формат. HTR позволяет автоматизировать обработку документов, в которых часть значимых сведений заполняется от руки, и сократить объем ручного ввода. В программных продуктах Smart Engines используется HTR для извлечения рукописных и рукопечатных данных паспортов, анкет, заявлений, форм и других документов.

Форензика

Совокупность методов анализа документов, данных и изображений для выявления следов изменения, подделки или другого вмешательства. Антифрод-система «Шерлок Зо» оснащена технологиями форензики для выявления поддельных удостоверений личности в физических и цифровых каналах обслуживания. Система обнаруживает отредактированные реквизиты, замененные фотографии, коллажи, следы генерации, нарушения структуры и защитных элементов документа, а также другие признаки манипуляций.

GDPR

General Data Protection Regulation – регламент Европейского союза, устанавливающий требования к сбору, обработке, хранению и защите персональных данных физических лиц. За наиболее серьезные нарушения GDPR предусматривает штрафы до 20 млн евро или 4% годового оборота компании. Технологии Smart Engines помогают бизнесу выполнять требования GDPR, так как данные документов распознаются локально на устройстве пользователя или в защищенном контуре организации и не передаются во внешние сервисы.

ICAO Doc 9303

Стандарт Международной организации гражданской авиации (ICAO), устанавливающий требования к машиночитаемым проездным документам, включая паспорта, визы и ID-карты, а также к структуре MRZ и электронным чипам. Унификация форматов и структуры данных позволяет упростить распознавание и проверку документов независимо от страны их выдачи. «Шерлок» поддерживает документы, соответствующие ICAO Doc 9303, извлекает данные визуальной и машиночитаемой зон и сопоставляет их с информацией из NFC-чипа.

ICR

Intelligent Character Recognition – технология интеллектуального распознавания документов, позволяющая расширить функциональность классических систем для извлечения текста. ICR используется для автоматического определения типа документа, поиска значимых полей, проверки структуры и взаимного расположения реквизитов, а также для преобразования извлеченной информации в набор структурированных данных.

ID-карта

Удостоверение личности в формате пластиковой карты, содержащее персональные данные владельца, фотографию и другие значимые сведения. Наряду с паспортом ID-карта используется для идентификации клиентов при оказании финансовых, государственных и других услуг. Технологии Smart Engines распознают ID-карты всех европейских стран, США и других государств, извлекают данные из визуальной и машиночитаемой зон, штрихкодов и электронных чипов.

ISO/ICAO

Свод международных стандартов, устанавливающих требования к машиночитаемым удостоверяющим и проездным документам, включая их формат, расположение данных, структуру MRZ и электронные компоненты. Технологии Smart Engines распознают документы, оформленные в соответствии со стандартами ISO/ICAO, определяют их тип и извлекают сведения из визуальной и машиночитаемой зон, а также RFID/NFC чипа.

KYB

Know Your Business – процедура проверки юридического лица или индивидуального предпринимателя перед началом деловых отношений, включающая подтверждение регистрационных данных, структуры собственности, бенефициаров и других сведений о компании. Технологии Smart Engines помогают автоматизировать KYB за счет мгновенного распознавания паспортов и комплектов регистрационных, учредительных и других корпоративных документов.

KYC

Know Your Customer – обязательная для банков, МФО, финтех-сервисов и других финансовых организаций процедура проверки личности клиента. Технологии Smart Engines позволяют автоматизировать процесс KYC: распознать удостоверение личности, проверить его подлинность и сопоставить фотографию в документе с селфи пользователя без выделения биометрических дескрипторов.

MRZ

Machine-readable zone – машиночитаемая зона документа, в которой основные сведения о владельце и самом документе записаны в стандартизированном формате с использованием специального шрифта OCR-B. «Шерлок» распознает MRZ в паспортах, ID-картах, визах и других удостоверениях личности и сопоставляет содержащиеся в ней сведения с данными визуальной зоны для выявления расхождений.

OCR

Optical Character Recognition – технология оптического распознавания символов, которая преобразует текст на фотографиях и сканах документов в редактируемый формат. Технология OCR Smart Engines выполняет распознавание паспортов и удостоверений личности, а также других документов всех типов и полнотекстовое распознавание. Система поддерживает более 100 языков и работает с изображениями, полученными в сложных условиях съемки – при бликах, перекосах, размытии и неравномерном освещении.

SDK

Software Development Kit – набор программных компонентов, помогающих разработчикам встраивать готовую технологию в приложение или информационную систему. SDK Smart Engines включает библиотеки, API, документацию, примеры кода и инструменты для настройки, тестирования и запуска решения. С помощью него разработчики могут интегрировать распознавание и проверку подлинности паспортов, ID-карт и других документов непосредственно в мобильные, серверные и веб-приложения, а также в мини-приложения мессенджеров.

115-ФЗ

Федеральный закон РФ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», обязывающий организации идентифицировать клиентов, проверять и актуализировать сведения о них. За нарушения требований ПОД/ФТ предусмотрены штрафы до 1 млн рублей или приостановление деятельности на срок до 90 суток. Технологии Smart Engines помогают компаниям выполнять требования 115-ФЗ, автоматизируя проверку документов физических лиц, ИП, компаний и их бенефициарных владельцев при процедурах KYC и KYB.

QR-код

Двумерный штрихкод, в котором может быть закодирована платежная или другая информация для быстрого считывания камерой устройства. Технология Smart Code Engine распознает QR-коды, используемые для оплаты товаров и услуг, и автоматически извлекает из них платежные реквизиты, упрощая проведение безналичных операций как в мобильных приложениях, так и в браузере.

WASM

WebAssembly – технология, позволяющая запускать скомпилированный программный код непосредственно в веб-браузере с производительностью, близкой к нативным приложениям. Smart Engines использует WASM для распознавания документов в браузере (Google Chrome, Safari, Яндекс Браузер и др.) и мини-приложениях мессенджеров Telegram и MAX, а также для чтения QR-кодов и банковских карт без установки отдельного приложения и передачи данных во внешние сервисы.

152-ФЗ

Федеральный закон РФ «О персональных данных», регулирующий их обработку и защиту. За нарушения предусмотрены штрафы до 20 млн рублей, при повторных утечках – оборотные штрафы до 500 млн рублей, а в наиболее тяжких случаях – лишение свободы до 10 лет. Технологии Smart Engines помогают компаниям соблюдать требования 152-ФЗ: данные документов извлекаются локально и не передаются во внешние сервисы, а при сверке лиц система не создает и не сохраняет биометрические шаблоны.



Smart Engines

Узнать больше:
smartengines.ru

+7 (495) 649 82 60

Для запросов коммерческих
предложений

sales@smartengines.ru

Для связи с PR-службой и
запросов от СМИ

pr@smartengines.ru

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



INTELLECT



INTELLECT

Узнать больше:
intellectpro.ru

8 (800) 555-67-05

Для запросов коммерческих
предложений

mail@intellectpro.ru

г. Екатеринбург, Первомайская
улица, д. 15, 11 этаж

г. Москва, ул. Неверовского, д. 10,
стр. 3А, 3 этаж

