# Системы верификации и авторизации по верифицированным данным

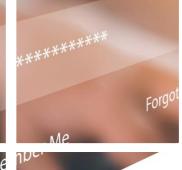
Обзор российского рынка



2024 год

















#### Оглавление

- 1. Введение
- 2. Терминология
- 3. Структура рынка
- 4. Государственные системы
- 5. <u>Банковские системы</u>
- 6. Другие игроки
- 7. <u>Тренды</u>
- 8. Приложение. Гайд по терминологии
- 9. O Data Insight

### Введение

С развитием цифровизации общества лавинообразно растет число сервисов, требующих авторизации. Пользователи устают от большого количества аккаунтов, паролей и логинов. Цифровизация также приводит в онлайн уязвимые категории граждан, которые легко могут стать жертвами мошенников. Одновременно бурно растет количество инструментов для мошенничества. С другой стороны, использование сложных методов защиты от мошенничества и многоступенчатых проверок приводит к снижению конверсии.

Перед бизнесом стоит сложная задача: с одной стороны, обеспечить безопасность пользователей и избежать мошенничества, а с другой - сократить количество аккаунтов и проверок, сделать необходимые проверки максимально незаметными для клиентов.

Поэтому растет важность систем верификации (проверки) личности и систем внешней авторизации (входа на сайт), использующих верифицированные данные. Такие системы позволяют входить на множество сайтов, используя одну учетную запись, а также верифицировать клиентов и пользователей сайтов, создавая простую, понятную и доверенную среду.

# Об обзоре

Предметом данного обзора являются поставщики услуг в области верификации личности и авторизации по верифицированным данным.

Настоящий обзор содержит описание терминологии и структуры рынка, описывает основные типы игроков. Для каждого типа определены особенности, даны описания конкретных поставщиков услуг, их специализация и особенности позиционирования. Кроме того, в обзоре представлены несколько кейсов успешного внедрения, иллюстрирующие применение решений от игроков рынка разного типа.

# Кратко о терминологии

**Верификация** - это процедура проверки данных пользователя. Например, проверка соответствия данных, которые он предоставил, документам или данным, содержащимся в базе.

**Авторизация** - это разрешение на совершение каких-либо действий (например, на вход на сайт) на основе проверки подлинности пользователя (например, при помощи пароля или СМС).

Проверка, выполняемая внешним провайдером, называется «внешней авторизацией».

Подробнее о других терминах (аутентификации, идентификации) и о пересечении их значений вы можете прочитать в нашем «Гайде по терминологии» в приложении к исследованию.

# Какие задачи решает верификация?

# eCommerce (1)

Верификация пользователей, прежде всего, предотвращает все виды проблем, связанные с использованием ботов и фейковых аккаунтов.

**Сбои статистики и накрутки трафика.** Боты могут посещать разделы интернет-магазина и карточки товаров, класть товары в корзину. Запросы от ботов могут полностью искажать аналитику на сайте.

**Сбор информации.** Боты могут собирать информацию о ценах и товарном ассортименте интернетмагазина и использовать ее для переманивания клиентов.

**Замедление работы магазина.** Активность ботов может повысить нагрузку на менеджеров магазина и привести к задержкам в обслуживании реальных клиентов.

**Мошенничество на скидках и акциях.** Мошенники могут использовать ботов для скупки ценных товаров на распродажах и акциях, регистрировать фейковые аккаунты для получения приветственных бонусов, кэшбеков. Часто при этом совершаются мелкие заказы, большое количество которых создает дополнительную нагрузку на логистику.



# eCommerce (2)

**Манипуляции с резервированием.** Фейковые аккаунты могут складывать сотни товаров в корзину. Если у интернет-магазина стоит автоматическое резервирование, это может привести к невозможности купить товар для настоящих клиентов. Другой пример: реселлеры могут совершать множество покупок с постоплатой с фейковых аккаунтов, но выкупать только те, которые им уже удалось перепродать. Таким образом, маркетплейс используется как склад, создается нагрузка на логистику, снижается доступность товара для реальных покупателей. Подобными схемами могут пользоваться и конкуренты.

**Ложные заказы.** Мошенники могут указывать данные реальных пользователей, например, номера телефонов. Это приведет к обзвону пользователей, которые не совершали заказ, и к репутационным потерям.

Фейковые отзывы. Проблема особенно актуальна для маркетплейсов. Фальшивые отзывы стимулируют покупку некачественных товаров и несут большие репутационные риски для маркетплейса.



# Другие сферы

**Классифайды.** Фальшивые аккаунты могут использоваться для распространения спама, мошеннических схем, отмывания денег.

**Кардинг.** Боты и фейковые аккаунты могут использоваться для проверок номеров украденных карт через транзакции на вашем портале. На украденные карты могут совершаться и крупные покупки. Это ведет не только к репутационным, но и к реальным финансовым потерям.

**Рекламный фрод.** Боты, фермы устройств или фейковые аккаунты могут симулировать бурную активность внутри приложения или сайта (фейковые установки, клики, запросы). Это снижает эффективность рекламы, портит таргетинг. В некоторых случаях это может делаться по заказу конкурентов.

# Типы внешней авторизации

Части сервисов не нужно знать о клиенте ничего, кроме логина, адреса электронной почты, или номера телефона. Но есть компании, которым нужны подтвержденные (верифицированные) данные о пользователях.

Разным запросам соответствуют два разных типа поставщиков внешней авторизации:

- 1. Социальная авторизация. Это авторизация через социальные сети и почтовые сервисы (зрелый и популярный метод, использующийся с 2010-х годов). В России самыми популярными провайдерами социальной авторизации являются VK, Одноклассники и Яндекс. Они имеют преимущество широкой аудитории и простоты использования, однако, они не могут рассказать о большинстве пользователей ничего, кроме того, что те сами о себе рассказали. Указанные в профилях личные данные не полны или не проверены.
- 2. **Авторизация по верифицированным данным.** Другие игроки имеют доступ к верифицированным данным или специализируются на верификации данных. Верифицированные данные обычно появляются у таких игроков как результат их деятельности. Это могут быть данные о клиентах банка, сотового оператора, данные потребителей государственных услуг.

#### Классификация по источнику верифицированных данных

Игроки рынка также делятся на два типа в зависимости от источника верифицированных данных:

- компании, обладающие собственными базами верифицированных пользователей, которые образовались в результате их основной деятельности (банки, государственные системы, операторы связи);
- компании, не обладающие такими базами, но верифицирующие пользователей на основе алгоритмов, открытых баз данных и других источников.

Первый тип компаний может называться в разных контекстах «системами идентификации» (ID) (когда речь идет о самой базе идентифицированных пользователей), «системами внешней авторизации» или «провайдерами идентификации» (когда речь идет о применении этих систем сторонними компаниями). Второй тип компаний в настоящем отчете мы называем «специализированными компаниями».

#### Использование верифицированных данных. Авторизация

Верифицированные данные могут использоваться как для авторизации, так и для верификации.

- 1. Вход на сайты или в приложения.
- **Регистрация**. Данные, идентифицирующие клиента, поступают от поставщика услуги владельцу сайта или приложения. На основании этих данных заводится профиль нового пользователя. *Пример: регистрация на Ozon.ru при помощи портала Госуслуги.*
- **Авторизация**. При первом входе данные поставщика связываются с существующим профилем пользователя на сайте. В последующем пользователь может входить на сайт, используя учетную запись в системе поставщика. *Пример: вход на сайт S7 при помощи Tinkoff ID.*

#### Использование верифицированных данных. Верификация

- 2. Подтверждение личности или данных.
- Верификация пользователя. Личные данные, указанные клиентом, подтверждаются и обогащаются дополнительными данными от поставщика; статус пользователя на сайте меняется. Пример: подтверждение личности на портале Mos.ru возможно через Госуслуги (ЕСИА), банковские ID (Сбер ID, Тинькофф ID, Alfa ID, ВТБ ID) и через личное посещение.
- **Разовая верификация** данных для отдельных операций или действий. При повторе операции данные верифицируются вновь, если пользователь не согласился на сохранение данных. Пример: проверка данных через Госуслуги при кроссбордерных заказах на Ozon.ru.

### Системы авторизации в закрытых экосистемах

Системы авторизации могут существовать и в закрытых экосистемах.

Например, экосистема МТС в данный момент закрыта для внешних партнеров, однако, в экосистеме существует идентификатор клиентов МТС ID, который и служит провайдером авторизации по отношению к сервисам экосистемы. Подобные системы существуют у других компаний, например Ozon ID, Газпром ID.

Когда экосистема открывается, ее внутренняя система авторизации становится доступной для внешних партнеров и превращается в одного из игроков рынка внешней авторизации.

По этому пути эволюционировали многие из банковских систем, описанные в соответствующем разделе, а в перспективе могут эволюционировать и некоторые из ныне закрытых экосистем.

# Требования закона к идентификации клиентов

Процедуру и требования к идентификации в России регулирует Федеральный закон 115-ФЗ.

**Полностью идентифицировать** своих клиентов обязаны банки, страховщики и другие профессиональные финансовые организации.

Полная идентификация производится путем проверки необходимых документов **при личном присутствии** клиента или его доверенного лица. Такие требования закона обеспечивают высокий уровень достоверности базы идентифицированных клиентов у банков.

Закон также предусматривает вариант упрощенной идентификации (УПРИД), которую можно провести удаленно. Она доступна при небольших операциях: переводы без открытия счета, кредиты до 15 тыс. рублей и так далее. Проводить ее имеют право, например, кредитные организации, МФО, страховые компании. УПРИД проводится путем простой проверки полученных от клиента данных (ФИО, номер паспорта) в государственных базах данных на действительность и не требует никаких процедур реальной проверки личности (свои ли данные предоставляет клиент).

Компании, использующие УПРИД, для достоверной верификации клиентов вынуждены обращаться за дополнительной проверкой к специализированным компаниям или в компании, уже владеющие базами полностью идентифицированных клиентов, например, в банки и государственные системы.

#### Провайдеры верификации и внешней авторизации



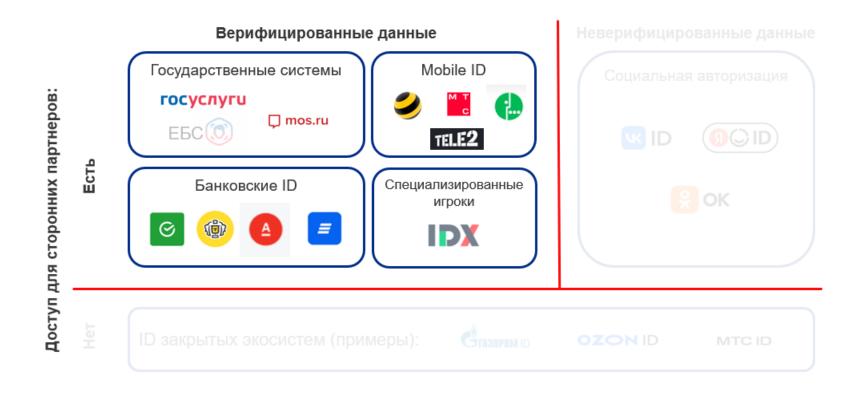
# Границы обзора

В настоящем обзоре мы рассмотрим только российские системы удаленной верификации и внешней авторизации, работающие с верифицированными личными данными и открытые для подключения внешних партнеров.

- Мы не будем рассматривать провайдеров социальной авторизации, которые по умолчанию работают с данными, предоставленными самим пользователем (хотя многие из них и стараются нарастить долю пользователей с подтвержденными личными данными).
- Закрытые системы идентификации, корпоративные или рассчитанные только на участников собственной экосистемы, также не включены в данный обзор.
- Мы также не будем рассматривать непосредственные технические решения для аутентификации, в частности, биометрию (включая Touch ID, Face ID, голос) и сервисы по отправке одноразовых кодов через SMS, мессенджеры и звонки.

# Границы обзора: схема

Предмет обзора - Российские системы удаленной верификации и внешней авторизации, работающие с верифицированными личными данными и открытые для подключения внешних партнеров



# Государственные системы

### О сегменте государственных систем

Государственные системы создавались на основе порталов государственных услуг, как общероссийских, так и региональных. Поскольку доступ к государственным услугам необходим подавляющему большинству граждан, такие системы имеют преимущество высокого проникновения и огромной аудитории верифицированных пользователей.

Изначально государственные системы идентификации использовались на соответствующих порталах и сайтах государственных органов. Однако постепенно такие системы открываются по отношению к коммерческим компаниям: сначала для ограниченного списка или в рамках пилотных проектов, но в перспективе они могут стать доступны всем потребителям.



# ЕСИА (Госуслуги)

ЕСИА (Единая система идентификации и аутентификации) существует с 2011 года.

Первоначально ЕСИА использовалась только для доступа к порталу Госуслуги. Так как для полноценного использования портала необходимо подтвердить свою учетную запись путем личного посещения МФЦ\*, большинство пользователей ЕСИА являются достоверно верифицированными.

**Число верифицированных пользователей:** 103 миллиона (август 2023 года) - самая большая база верифицированных граждан в стране.

**Статистика:** 8 800 подключенных систем (сюда включены, в том числе, и государственные органы, и информационные системы компаний, не использующих ЕСИА с целью верификации или авторизации).

Для партнеров: <a href="https://partners.gosuslugi.ru/catalog/esia">https://partners.gosuslugi.ru/catalog/esia</a>

Руководство пользователя ЕСИА: <a href="https://digital.gov.ru/ru/documents/6182/">https://digital.gov.ru/ru/documents/6182/</a>

Методические рекомендации по использованию ЕСИА: <a href="https://digital.gov.ru/ru/documents/6186/">https://digital.gov.ru/ru/documents/6186/</a>

<sup>\*</sup> Или воспользоваться для подтверждения Tinkoff ID, Сбер ID или интернет-банком Почта Банка.





#### Кто может пользоваться ЕСИА?

Помимо государственных органов, интегрироваться с ЕСИА имеют право только коммерческие компании из следующего списка:

- медицинские учреждения;
- банки и МФО, страховщики, брокеры и финансовые управляющие, негосударственные пенсионные фонды;
- операторы связи.

В соответствии с правилами, вступившими в силу с 1 сентября 2023 года, медицинские учреждения, предоставляющие платные услуги, также смогут использовать ЕСИА для идентификации клиента при дистанционном подписании договоров.

С марта 2023 года обеспечить интеграцию с ЕСИА также обязаны сайты объявлений (классифайды). В июле 2023 года Роскомнадзор опубликовал список из 12 сервисов, которые подпадают под данную норму.

Компании из других сфер также могут подать заявку на интеграцию с ЕСИА в качестве пилотного проекта. По такой схеме с ЕСИА уже работают: VK, Циан, Auto.ru, Авито, HeadHunter, Ozon и другие компании.



#### ECИA: Pros & Cons

**Охват.** Самая большая база верифицированных пользователей в России.

**Данные.** Вероятно, самый большой набор данных о пользователе. Однако большинство коммерческих организаций не имеют доступа к этим данным.

Перспективы. Полноценное использование биометрии расширит возможности ЕСИА в сфере удаленного предоставления услуг (см. слайд о ЕБС в заключительной части обзора).

**Законодательные ограничения.** ЕСИА могут использовать только компании из списка, определенного законом, и некоторые другие компании в рамках индивидуальных «пилотных» проектов.

**Сложность интеграции.** Согласование и интеграция занимают больше времени по сравнению с коммерческими решениями. От нескольких недель до месяцев.

**Аудитории**. Среди клиентов высока доля людей с низким уровнем цифровизации, использующих Госуслуги не чаще нескольких раз в год.

**Восприятие**. Система, связанная с документами, воспринимается пользователями как нечто, с чем нужно обращаться с осторожностью. Они опасаются использовать систему в простых ежедневных операциях.

**Технические ограничения.** Короткоживущие сессии вынуждают пользователей часто вводить пароль.



#### 🗖 mos.ru

#### Mos.ID

Mos.ID – учетная запись на портале Mos.ru. Доступ к системе для бизнеса открыт в 2019 году.

**Число пользователей:** 15,1 миллионов пользователей портала (нет данных о числе подтвержденных пользователей).

На сайте возможна регистрация при помощи сторонних провайдеров авторизации, в том числе и социальных. Однако статус подтвержденной учетной записи можно получить только при помощи ЕСИА и банковских ID (Сбер ID, Tinkoff ID, Alfa ID, BTБ ID).

Число интеграций: более 150 в 2022 году, в основном городские ресурсы.

**Примеры коммерческих интеграций:** МГТС, авторизация, 2019 год. Верификация данных (собственности на квартиру) на Яндекс.Недвижимость – кейс объявлен в 2022 году. О других интеграциях в открытых источниках информации нет.

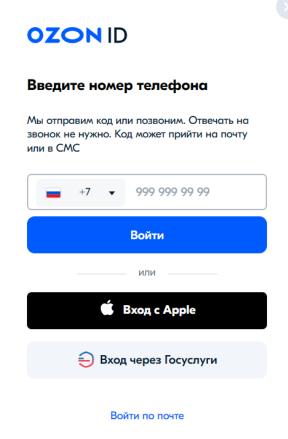
Документация: <a href="https://login.mos.ru/support/">https://login.mos.ru/support/</a>.



# Авторизация и получение верифицированных данных маркетплейсом Ozon из ЕСИА

**Задача.** Перед маркетплейсом Ozon стояла задача расширения выбора способов авторизации на сайте. Пользователи могут предпочитать разные способы авторизации, и расширение выбора повышает удобство сайта. Дополнительно стояла задача получения верифицированных данных о покупателях, необходимых для продажи некоторых категорий товаров и проведения отдельных операций.

**Выбор.** При этом Ozon не хотел пользоваться услугами банковских ID и социальных провайдеров авторизации, рассматривая их как конкурентов, а во втором случае также и потому, что социальные провайдеры не предоставляют верифицированные данные. Поэтому в качестве провайдера была выбрана некоммерческая система ЕСИА (Госуслуги).





# Авторизация и получение верифицированных данных маркетплейсом Ozon из ЕСИА

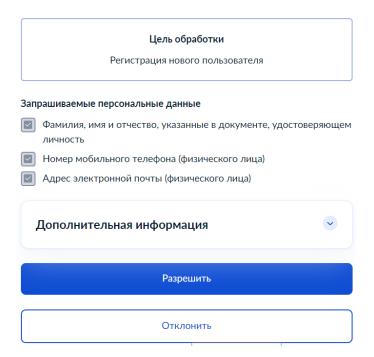
**Процесс.** Так как Ozon стал одним из первых маркетплейсов, где используется это государственное решение, внедрение заняло больше времени, чем обычно занимает интеграция коммерческих систем. Кроме того, в ЕСИА существуют определенные требования к оборудованию в случае, если клиент собирается хранить персональные данные, получаемые из системы.

Для пользователя. При первом входе через Госуслуги происходит процедура связывания аккаунтов. В редких случаях возникает ситуация, когда на получаемые от ЕСИА email и телефон на Ozon зарегистрированы два разных аккаунта. В таком случае клиенту предлагается выбрать аккаунт, с которым будет связан профиль на Госуслугах. Привязка аккаунтов полностью добровольна, пользователь имеет возможность в любой момент ее отменить.

#### госуслуги

#### ООО "ИНТЕРНЕТ РЕШЕНИЯ" запрашивает ваше согласие на обработку персональных данных

Адрес: 123112, Г.Москва, НАБ. ПРЕСНЕНСКАЯ, д. Д. 10, кв. ПОМЕЩ. I ЭТ 41 КОМН 6





# Авторизация и получение верифицированных данных маркетплейсом Ozon из ЕСИА

**Плюсы.** Дополнительным плюсом интеграции ЕСИА для Ozon стала возможность получать верифицированные данные покупателей. Компании не нужно верифицировать их самостоятельно. Например, в будущем Ozon сможет получать из ЕСИА верифицированный возраст, что может использоваться при продаже отдельных категорий товаров. А при кроссбордерных заказах Ozon уже сейчас предлагает покупателям возможность загрузить из Госуслуг верифицированные данные, необходимые для прохождения таможни, чтобы не вводить их вручную (все получаемые данные хранятся и обрабатываются маркетплейсом строго в соответствии с законом «О персональных данных»).

Основным способом авторизации для Ozon по-прежнему является авторизация по телефону (SMS, звонок), но внедрение ЕСИА дополнительно позволило оптимизировать затраты на услуги мобильных операторов. На данный момент решение полностью функционально и активно используется покупателями. Решение внедрено только на сайте маркетплейса и пока не применяется в приложении.

# Банковские системы

#### О сегменте банковских ID

Как и Госуслуги, банки обладают большой **базой уже идентифицированных клиентов**. Одновременно у большинства банков уже есть **опыт создания систем единой авторизации** в своих внутренних сервисах (экосистемах).

Поэтому логично, что банки с большой розничной аудиторией и развитой собственной экосистемой первыми заметили возможности рынка. Первые банковские системы идентификации выросли из больших внутренних экосистем: Сбер ID и Tinkoff ID. Однако сейчас появляются и ID банков, не имеющих заметных экосистем, но обладающих большой аудиторией розничных клиентов (Alfa ID, BTБ ID).

# Общие особенности игроков сегмента

- Аудитория банков меньше, чем у ЕСИА, однако она более активная и лояльная.
- Конверсия клиентов выше за счет восприятия банковских ID как коммерческих продуктов для ежедневного использования (в противоположность ЕСИА, государственной системе для важных документов).
- Быстрая и простая для клиента интеграция. Подробная и понятная документация, порталы для разработчиков.
- Банковские решения доступны всем партнерам, их применение не ограничено законодательством.
- Яркий маркетинг, который имеет как общие тезисы

(легкий и беспарольный вход, интеграция с финансовыми сервисами банка, проверенные данные),

так и фокус на преимуществах отдельных банков, например:

на ценности собственной экосистемы, или на богатстве возможностей для партнеров, или на удобстве и надежности данных.

• Несмотря на схожий функционал, банковские ID имеют разное проникновение и по-разному позиционируются на рынке.

# Сбер ID





Запущена в 2020 году.

**Количество интеграций:** 165 (июнь 2023 года), в том числе **8 интернет-магазинов из Топ-1000**\*.

Заметные интеграции: Циан, InSales, Mos.ru, Рамблер, VK.

Статистика: 63,6 млн пользователей системы (июнь 2023).

Для пользователей: <a href="http://www.sberbank.ru/ru/person/dist\_services/sberid">http://www.sberbank.ru/ru/person/dist\_services/sberid</a>

Для девелоперов: <a href="https://api.developer.sber.ru/product/SberbankID">https://api.developer.sber.ru/product/SberbankID</a>

Документация: <a href="https://developers.sber.ru/docs/ru/sberid/overview">https://developers.sber.ru/docs/ru/sberid/overview</a>

<sup>\*</sup> Рейтинг российских интернет-магазинов Топ-1000, 2022, Data Insight, <a href="https://datainsight.ru/index\_top100\_2023">https://datainsight.ru/index\_top100\_2023</a>.



# Позиционирование для пользователей





Среди преимуществ подчеркиваются удобство и возможности экосистемы Сбера:

- Бесплатный вход на сервисы и сайты;
- Несколько удобных способов входа (номер телефона, QR-код, логин);
- Доступ к возможностям экосистемы Сбера;
- Преимущества в экосистеме Сбера, скидки;
- Автозаполнение форм;
- Системой могут пользоваться и не клиенты банка;
- Можно использовать карты других банков;
- Финансовые данные не передаются сторонним партнерам.

# Позиционирование для партнеров





В отличие от других банков, у Сбер ID нет отдельной страницы, описывающей преимущества решения для партнеров. Компании переадресуются в раздел с документацией и на портал для разработчиков.

Сбер ID больше сфокусирован на пользователях, чем на партнерах. Потенциальным пользователям рекламируется в большей степени собственная экосистема, чем большой выбор сторонних партнеров. Подчеркивается открытость клиентам других банков (возможность добавления чужих карт, возможность использования не клиентами банка), что также больше направлено на завлечение клиента в экосистему, чем на расширение экосистемы.

В качестве основного преимущества для партнеров называется большая аудитория и активная вовлеченность аудитории в собственную экосистему Сбера (а, значит, ежедневное использование Сбер ID).

# Сбер ID: Pros & Cons





Охват - самый большой из банков. У Сбербанка больше 100 млн розничных клиентов.

**Развитая экосистема** собственных сервисов увеличивает вероятность использования Сбер ID на сайтах партнеров.

Особенности аудитории. Среди клиентов доля людей старшего возраста, с низким уровнем цифровизации – выше средней. Это может нивелировать преимущество большой базы.

**Фокус** больше на вовлечение аудитории в собственную экосистему, чем на расширение экосистемы.

# Тинькофф ID





Запущена в июле 2022 года.

**Количество интеграций**: более 200, в том числе **более 100 партнеров из Топ-1000\* в сегменте large enterprise.** 

Заметные интеграции: Циан, Авито, VK, Mos.ru, HeadHunter, СДЭК, S7, Финуслуги.

**Статистика:** 36 млн клиентов экосистемы, более 1 млрд авторизаций в месяц, ежемесячный рост числа авторизаций – 20% (июнь 2023 года).

Для пользователей: <a href="https://www.tinkoff.ru/tinkoff-id/">https://www.tinkoff.ru/tinkoff-id/</a>

Для партнеров: <a href="https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/">https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/</a>

Документация и стайл-гайды: <a href="https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/integration/">https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/integration/</a>

Рекомендации по интеграции: https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/integration/instruction/

<sup>\*</sup> Рейтинг российских интернет-магазинов Топ-1000, 2022, Data Insight, <a href="https://datainsight.ru/index\_top100\_2023">https://datainsight.ru/index\_top100\_2023</a>.



### Позиционирование для пользователей





Есть два раздела, описывающих преимущества **авторизации** (входа на сайты) и **верификации** (подтверждение профилей). Среди преимуществ для пользователя указаны:

- Доступ к сайтам и приложениям в пару кликов;
- Безопасный вход без логинов и паролей + платформа Тинькофф Защита на стороне банка;
- Современное шифрование;
- Передача данных только с согласия пользователя;
- Автозаполнение форм и анкет;
- Простой старт для клиентов Tinkoff;
- Удобное подтверждение профилей в соцсетях, на сайтах объявлений и у других партнеров.

Есть конкретные **кейсы** того, что можно сделать, использовав авторизацию (заказать товары и услуги, устроиться на работу, записаться к врачу и т. д.) или верификацию от Tinkoff ID (финансовые услуги и микрозаймы, сайты объявлений, соцсети, службы доставки, госсервисы).

Есть **список партнеров** Tinkoff ID по авторизации (25) и верификации (10).



#### Позиционирование для партнеров





Tinkoff описывает разнообразный набор преимуществ для партнеров:

- Увеличение конверсии благодаря легкому входу и автозаполнению форм;
- Подробные и актуальные данные о пользователе могут помочь с маркетингом;
- Система детектирования бот активности предотвратит попытки атак на партнёра;
- Антифрод-платформа Тинькофф Защита не пропустит пользователей, которые могут злоупотреблять сервисами партнёра или вводить в заблуждение других пользователей;
- Многоуровневая идентификация гарантирует подлинность данных пользователя;
- Большой охват (36 млн пользователей экосистемы);
- Большой опыт компании в финтехе;
- Интеграция с финансовыми продуктами Tinkoff.

Предоставлена информация о стоимости решения, сроках и сложности интеграции, а также о возможностях использования системы в b2b-кейсах.

### Тинькофф ID: Pros & Cons





**Аудитория.** Тинькофф – первый цифровой банк. Его аудитория молода и восприимчива к новым технологиям.

**Лояльность бренду**. Аудитория банка лояльна бренду, частота использования услуг банка выше средней.

**Развитая экосистема** также положительно влияет на конверсию.

Фокус на партнерах и расширении экосистемы за счет партнеров. Сайт имеет подробный раздел для партнеров. Дан большой список успешных кейсов.

**Охват**. Размер аудитории банка ниже, чем у Сбербанка, что ограничивает возможность использовать Тинькофф ID в качестве единственного решения.

**Экосистема меньше**, чем у Сбербанка, и включает меньше видов сервисов.

#### Alfa ID

<u>А</u> Войти по Альфа ID

A

Запущена для физических лиц в конце 2022 года.

Количество интеграций: нет данных (десятки).

Нет интеграций среди интернет-магазинов Топ-1000\*.

Заметные интеграции: Mos.ru, Superjob, VK.

Число пользователей: нет данных.

Для пользователей: <a href="https://alfabank.ru/everyday/alfa-id/">https://alfabank.ru/everyday/alfa-id/</a>

Для партнеров: <a href="https://alfabank.ru/sme/alfaid/">https://alfabank.ru/sme/alfaid/</a>

Для девелоперов: <a href="https://developers.alfabank.ru/products/alfa-id">https://developers.alfabank.ru/products/alfa-id</a>

<sup>\*</sup> Рейтинг российских интернет-магазинов Топ-1000, 2022, Data Insight, <a href="https://datainsight.ru/index\_top100\_2023">https://datainsight.ru/index\_top100\_2023</a>.



### Позиционирование для пользователей Войти по Альфа 10



На пользовательской странице Alfa ID описывает только преимущества удобной авторизации, не упоминая верификацию данных:

- Безопасный способ получить доступ ко множеству сервисов;
- Три доступных способа входа: по номеру телефона, QR-коду и через приложение;
- Авторизация без логина и пароля;
- Автозаполнение анкет и форм;
- Работает на компьютере и смартфоне;
- Самое современное шифрование;
- «Мы никогда не передаем информацию о ваших финансах».

### Позиционирование для партнеров

В позиционировании для партнеров **Alfa ID фокусируется на клиентском опыте, качестве и составе данных**:

- Единая учетная запись для множества продуктов и сервисов;
- Бесшовный клиентский опыт, быстро и удобно для пользователя;
- Источник проверенных качественных данных; только реальные клиенты, никаких вымышленных данных;
- Легитимная передача данных о пользователе;
- Расширенный профиль клиента;
- Высокие стандарты безопасности и защиты данных;
- Повышение конверсии за счет автозаполнения;
- Расширение функционала сайта за счет доступа к банковским сервисам.

#### Alfa ID: Pros & Cons



**Аудитория.** Альфа-Банк – один из крупнейших розничных банков.

**Подробная информация** о продукте как для пользователей, так и для партнеров.

Фокус на партнерах. Не имея большой собственной экосистемы, Альфа-Банк прилагает дополнительные усилия для привлечения партнеров.

**Охват**. Размер аудитории банка ниже, чем у конкурентов, что не позволяет использовать его в качестве единственного решения.

**Экосистема.** Экосистема Альфа-Банка менее развита, что снижает частоту использования ID и конверсию.

**Новизна**. Система запущена позже других и еще не стала привычной.

#### BTE ID





Система открылась для партнеров в 2023 году.

Количество интеграций: более ста (?\*\*).

Нет интеграций среди интернет-магазинов Топ-1000\*.

Заметные интеграции: Mos.ru.

Статистика: 700 тыс. клиентов ежемесячно.

Для пользователей: <a href="https://www.vtb.ru/personal/online-servisy/vtb-id/">https://www.vtb.ru/personal/online-servisy/vtb-id/</a>

Для партнеров: <a href="https://www.vtb.ru/malyj-biznes/vtb-id/">https://www.vtb.ru/malyj-biznes/vtb-id/</a>

Документация: <a href="https://www.vtb.ru/malyj-biznes/vtb-id/integraciya/">https://www.vtb.ru/malyj-biznes/vtb-id/integraciya/</a>

<sup>\*\*</sup> Такое число указано в сентябрьском пресс-релизе компании, однако не ясно, включает ли оно части собственной экосистемы ВТБ - <a href="https://www.vbr.ru/banki/vtb/press/klienti-vtb-smogyt-ispolzovat-edinii-vhod-vtb-id-bolee-cem-na-100-resyrsah/">https://www.vbr.ru/banki/vtb/press/klienti-vtb-smogyt-ispolzovat-edinii-vhod-vtb-id-bolee-cem-na-100-resyrsah/</a>.



<sup>\*</sup> Рейтинг российских интернет-магазинов Топ-1000, 2022, Data Insight, <a href="https://datainsight.ru/index\_top100\_2023">https://datainsight.ru/index\_top100\_2023</a>.

### Позиционирование для партнеров





#### Преимущества для клиентов:

- Не нужно запоминать много паролей и логинов;
- Безопасность данных;
- Легкий старт для клиентов банка.

Для партнеров ВТБ ID позиционируется как **простой дополнительный способ повысить конверсию**:

- Повышение конверсии за счет размера банка и числа розничных клиентов;
- Простая интеграция;
- Типовая форма договора;
- Сопровождение банка;
- Дополнительный способ авторизации, удобный для пользователей.

#### BTБ ID: Pros & Cons





Аудитория. Крупный розничный банк.

**Простота подключения.** Типовые договоры, простая интеграция, сопровождение.

**Охват**. Размер аудитории банка ниже, чем у конкурентов, что не позволяет использовать его в качестве единственного решения.

Экосистема. Экосистема банка менее развита.

**Новизна**. Система запущена совсем недавно и мало понятна. Нет понятных кейсов применения.

## Другие банки



Газпромбанк развивает собственную экосистему услуг для малого бизнеса – ГПБ Бизнес-онлайн, в рамках которой существует и **ГПБ Бизнес ID**, которая описывается как «Единая учетная запись для работы с продуктами и сервисами, предоставляемыми группой Газпромбанка и партнерами».

Однако на данный момент нет никакой четкой информации о том, как партнерам подключиться к системе, открыта ли она для партнеров, и, если нет, то когда будет открыта.



Почта Банк много лет позволяет своим клиентам подтверждать онлайн свою учетную запись на Госуслугах (ЕСИА), однако этот функционал не расширился дальше государственного портала.



#### Подтверждение данных в VK через банковский Tinkoff ID

Задача. Основная задача, стоявшая перед VK, – создание доверенной и безопасной среды на платформе через рост доли подтвержденных пользователей. Подтвержденный статус – это указание на то, что пользовать указал в профиле свои реальные данные. Такой профиль получает серую галочку рядом с именем, и, таким образом, другие пользователи социальной сети понимают, что перед ними реальный человек, а не бот или мошенник. Для социальной сети важно расширить охват проверки, поэтому она должна быть максимально простой и удобной для пользователей, а также она должна включать все самые популярные способы.

**Выбор.** В качестве одного из способов подтверждения данных аккаунта был выбран Tinkoff ID – сервис одного из крупнейших банков по числу розничных клиентов, который полностью соответствует требованиям VK и подходу к обеспечению безопасности данных. С Tinkoff ID процедура подтверждения данных полностью прозрачна для пользователя: пользователь видит, какие данные передаются, и может отказаться передавать все или часть из них. В случае, если данные, получаемые от Tinkoff ID, отличаются от ранее указанных в профиле, пользователь всегда имеет право выбора: он может заменить данные или отказаться от подтверждения. Кроме того, пользователь может отменить подтверждение в любой момент и изменить данные профиля.

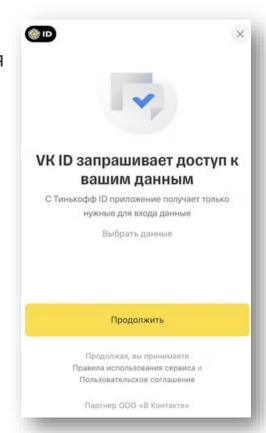


#### Подтверждение данных в VK через банковский Tinkoff ID

**Для пользователя.** Подтвержденные пользователи отображаются выше в поиске. Дополнительным бонусом для пользователей, подтвердивших свои данные, является упрощенная процедура восстановления доступа при утере пароля, так как верифицированные личные данные пользователя уже известны социальной сети. Кроме того, они получают преимущество быстрой авторизации в принадлежащем VK магазине приложений RuStore, где используется авторизация через Tinkoff ID.

**Внедрение.** Внедрение проводилось VK самостоятельно, в соответствии с документацией, предоставленной Tinkoff ID. Весь процесс занял не более месяца, причем срок определялся больше внутренними процедурами VK. После этого интеграция прошла внутренний аудит на соответствие со стандартами социальной сети.

Сложностей при внедрении не возникло. Негативных обращений в поддержку со стороны пользователей также не было. Внедрение Tinkoff ID расширило набор доступных способов подтверждения, а лояльная аудитория Tinkoff помогла увеличить долю подтвержденных пользователей VK.





# Другие игроки

### Общие черты других игроков

Общее свойство игроков других типов, не являющихся ни банками, ни государственными органами, – отсутствие базы достоверно верифицированных пользователей. Специализированные компании не обладают такой базой, а базы пользователей мобильных операторов до последнего времени не отличались достоверностью.

Компании работают с этой особенностью разными способами:

- специализированные игроки разрабатывают методы верификации, применимые ко всему населению;
- мобильные операторы активно повышают качество данных в последние месяцы, требуя у пользователей подтвердить данные\*;
- кроме того, мобильные операторы делают фокус на своей уникальной возможности определении номера телефона, с которого пользователь выходит в сеть.

<sup>\*</sup> Пример: https://rg.ru/2023/05/16/pokazhite-pasport.html.

#### Mobile ID









Mobile ID в России развивается совместно с крупнейшими операторами: МТС, Мегафон, Билайн, Теле2. Сервис работает по спецификациям международной Ассоциации GSM. Первые тестовые внедрения начались в 2021 году.

Количество интеграций: нет данных (десятки).

Заметные интеграции: Альфа-Банк, VK, ЮМопеу, БКС, Ютека, Ozon, Ivi.

Статистика: общая пользовательская аудитория более 100 млн человек.

MTC: <a href="https://mobileid.mts.ru/">https://mobileid.mts.ru/</a>

Мегафон: <a href="https://mobileid.megafon.ru/">https://mobileid.megafon.ru/</a>

Билайн: <u>https://mobileid.beeline.ru/</u>

Теле2: нет выделенной страницы

### Особенности и позиционирование Mobile ID

Уникальная особенность Mobile ID в том, что оператор знает телефонный номер пользователя и может использовать ассоциированные с этим пользователем данные.

#### Преимущества для пользователей:

- Не нужно вводить номер телефона;
- Не нужно ждать SMS-подтверждение операций, возможен вход без введения кода (технология SIM-PUSH);
- Не нужно помнить пароли;
- Автозаполнение форм.

#### Преимущества для партнеров:

- Снижение барьеров при входе и сокращение клиентского пути повышают конверсию;
- Дополнительные данные о клиентах (скоринг, данные для персонализации);
- Верификация (сравнение) введенных данных с данными, имеющимися у оператора;
- Быстрое и простое внедрение;
- Общая база операторов.

#### Mobile ID: Pros & Cons

**Аудитория.** Очень большой суммарный охват: мобильной связью пользуется все население страны.

**Уникальные возможности.** Автоматическое определение номера телефона пользователя.

Менее надежная база на данный момент. Значительное количество «серых» сим-карт и номеров, оформленных на посторонних людей. Операторы активно решают эту проблему.

**Несколько провайдеров.** Эффективность и надежность решения зависят от успешной совместной работы четырех разных операторов.

#### **IDX**



IDX – пример специализированной компании, предоставляющей услуги в сфере удаленной идентификации и верификации. Компания создана в 2017 году Фондом развития интернет-инициатив.

Количество клиентов: несколько сотен, в том числе крупнейшие маркетплейсы.

Заметные клиенты: Альфа-Банк, МТС, X5, Ozon, Ростелеком.

Статистика: более 2,5 млн проверок в месяц, менее 5 секунд на операцию.

Описание услуги подтверждения личности: <a href="https://iidx.ru/uslugi/proverka-fizicheskogo-litsa/#podtverzhdenie-lichnosti">https://iidx.ru/uslugi/proverka-fizicheskogo-litsa/#podtverzhdenie-lichnosti</a>.

# Особенности специализированных компаний ІРХ



Специализированные компании не принадлежат ни к категории банков, ни к категории государственных сервисов и не обладают уже готовой базой верифицированных пользователей. Поэтому, в частности, они не могут предоставлять услугу внешней авторизации. При верификации данных специализированные компании полагаются на открытые данные, доступные эталонные базы, данные из достоверных источников (например, от сервис-провайдеров различных услуг). С одной стороны, отсутствие собственной базы лишает их возможности работать с уже проверенными данными, с другой – они не ограничены аудиторией базы и могут применять свои алгоритмы ко всему населению.

Фокус услуг IDX – на верификации отдельных данных, необходимых для авторизации операций, и на верификации личности. Например:

- верификация данных, необходимых для прохождения таможни;
- подтверждение личности клиента или участника сделки, выявление подмены личности;
- проверка совершеннолетия;
- распознавание и верификация различных документов: от паспорта до ОСАГО.



#### **IDX: Pros & Cons**



Собственные алгоритмы и датасеты покрывают 100% населения и не ограничены фиксированной аудиторией.

Алгоритмы совершенствуются в режиме реального времени.

Дополнительная проверка может выявлять даже мошенников, купивших подтвержденные учетные записи на ЕСИА.

Отсутствие собственной готовой базы верифицированных клиентов.

Нет услуги внешней авторизации.

Верификация основана на вероятности, а не на точном формальном соответствии документов личности.

## Пограничные кейсы

Теоретически, в определение «удаленная идентификация и верификация» могут попадать самые разные кейсы.

Например, основным профилем компании **ЕФИН** является доставка финансовых документов, банковских карт, анкетирование, предлагает, в том числе, и **сбор данных для идентификации клиентов МФО курьерами:** к потенциальному клиенту выезжает курьер, проверяет его паспорт, фотографирует и высылает в МФО. В открытых источниках есть упоминание только об одной интеграции – с МигКредит в 2020 году. Однако МФО в целом не склонны раскрывать информацию о методах своей работы.

Сайт компании: <a href="https://efin.ru/">https://efin.ru/</a>.

Другой пример пограничного кейса — **идентификация через пункты денежных переводов** Contact, которая также используется несколькими МФО. Клиент приходит в пункт Contact, где кассир проверяет паспорт, вводит данные клиента и отправляет их МФО.

Информация об услуге: <a href="https://www.contact-sys.com/payments/identifikatsiya">https://www.contact-sys.com/payments/identifikatsiya</a>.



#### Онлайн-проверка данных клиентов МФО\* через IDX

**Задача.** В соответствии с требованиями ЦБ, прежде чем выдать кредит, микрофинансовая организация обязана идентифицировать клиента и провести несколько проверок из предложенного ЦБ списка. Однако проверка по минимальному набору критериев (действительность паспорта и ИНН, селфи с паспортом, телефон) легко обходится мошенниками. Многие МФО используют для более надежной идентификации проверку через Госуслуги. Однако и этот способ мошенники могут обойти: подтвержденные учетные записи в ЕСИА доступны на черном рынке.

**Выбор.** Самостоятельная же проверка клиентов по максимальному набору критериев сложна и затратна для МФО и, кроме того, сказывается на конверсии: чем тщательнее проверка, тем ниже конверсия. По статистике МФО, даже регистрация через Госуслуги может отпугнуть до половины потенциальных клиентов. Важно, чтобы проверка не была заметна клиенту, не усложняла клиентский путь.

**Решение.** IDX использует уже введенные клиентом данные (фамилия, имя, дата рождения, телефон) и на основе заранее собранных данных анализирует историю использования телефонного номера: как долго и часто он использовался, ассоциируется ли он с другими людьми, замечен ли в мошеннических действиях, какова вероятность, что номер действительно принадлежит заявителю. Дополнительно, с устройства, с которого подается заявка, также снимается цифровой след, который используется для анализа поведения пользователя. Суммарно весь анализ занимает не более пяти секунд и не виден клиенту.



<sup>\*</sup> Компания предпочла сохранить анонимность.

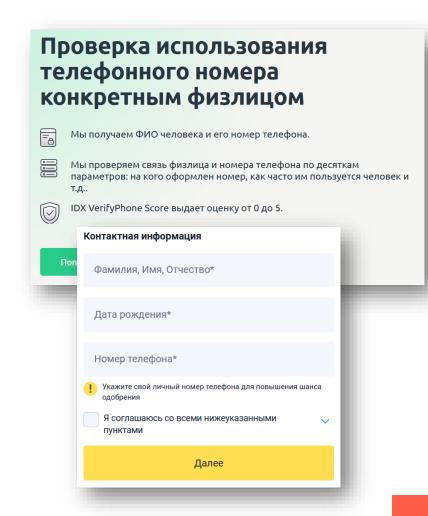


#### Онлайн-проверка данных клиентов МФО через IDX

Как показал опыт использования, система способна разметить 90— 95% входящего потока клиентов, разделить их на добросовестных заявителей и потенциальных мошенников. Вероятность определения мошенничества составляет 98%.

Внедрение. Внедрение было реализовано силами самой МФО через подключение к API поставщика и заняло не более двух дней. Внешний интерфейс сайта МФО не изменился. Важным вопросом для МФО остается принятие решений по остающимся неразмеченным 10%. Обычно у таких клиентов запрашиваются дополнительные данные.

Результатами работы системы МФО делится с поставщиком, и, таким образом, данные, собранные IDX, постоянно обновляются, а модель совершенствуется.



# Тренды

#### Потенциальные новые игроки

- 1. Существенная часть российских банков предоставляет своим клиентам набор сервисов и услуг родственных компаний минимальную экосистему и часто предоставляет клиентам возможность авторизоваться в этой экосистеме, используя единый идентификатор, например, учетную запись в интернет-банке. Потенциально все банки, имеющие такую единую систему авторизации во внутренних сервисах, могут выйти на рынок банковских ID. Однако крупнейшие розничные банки на рынке уже присутствуют, и новички с меньшей аудиторией розничных клиентов смогут закрепиться на рынке, только предлагая уникальные или нишевые решения.
- **2.** Провайдеры социальной авторизации также смогут стать игроками на рынке верификации при условии, что они сумеют верифицировать большинство своих пользователей.

### Регулирование методов авторизации

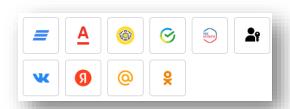
С 1 декабря 2023 года вступает в силу федеральный закон № 406-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О связи», в соответствии с которым авторизация в российских сервисах возможна только:

- по номеру телефона;
- через портал Госуслуг (ЕСИА);
- через Единую биометрическую систему (ЕБС);
- с помощью иной системы для авторизации пользователей, владельцем которой является гражданин РФ или российское юрлицо.

Это напрямую запрещает работу иностранных сервисов внешней авторизации (преимущественно касается методов социальной авторизации). А также вступает в прямой конфликт с требованиями Apple для приложений, согласно которым, если в приложение встраивается вход через любой сторонний сервис, то разработчик обязан дополнительно встроить и вход через Apple ID.

### Рост выбора способов на площадках

Конкуренция между игроками и простота интеграции приводит к росту числа способов авторизации или верификации, используемых площадками. Например, mos.ru на данный момент предлагает для авторизации едва ли не все доступные способы, включая социальную авторизацию, а для верификации – все доступные банковские сервисы и Госуслуги. Есть примеры и других площадок, которые внедряют новые способы авторизации по мере их выхода на рынок.



Для площадок внедрение нескольких способов требует минимальных затрат и повышает конверсию и удовлетворенность пользователей, но для игроков рынка это приводит к снижению доходов с одной площадки.

В то же время это компенсируется быстрым ростом рынка: запрос на верификацию пользователей продолжает расти. Кроме того, с уходом иностранных провайдеров социальной («неверифицированной») авторизации, определенная доля площадок, использовавших их услуги, также может перейти к российским провайдерам авторизации по верифицированным данным.

### Перспективы Единой Биометрической Системы

ЕБС – государственная система, база биометрических данных граждан России. ЕБС была создана в 2018 году, но за первые годы работы собрала данные только нескольких сотен тысяч пользователей. Однако к 30 сентября 2023 года все банки и другие владельцы биометрических данных обязаны передать собранные данные в ЕБС, и система становится единственным в стране оператором биометрии. ЕБС связана с ЕСИА: в системе хранятся только данные клиентов, имеющих подтвержденную учетную запись в ЕСИА.

Потенциально ЕБС должна обеспечивать удаленную идентификацию при помощи биометрии и позволить пользователям, в числе прочего, получать удаленно финансовые услуги и заключать договора. Однако на данный момент далеко не все банки дают возможность открыть счет или получить услугу с использованием биометрии. В перспективе полноценное применение ЕБС расширит спектр операций, доступных при помощи полностью удаленной идентификации.

А, так как такая услуга будет неразрывно связана с профилем на ЕСИА, это может стать дополнительным конкурентным преимуществом ЕСИА по отношению к другим игрокам на рынке верификации личности.

# Приложение. Гайд по терминологии

## Гайд по терминологии

#### «Идентификация», «Аутентификация», «Авторизация», «Верификация».

Все эти термины нередко смешиваются, взаимно заменяются, используются неверно.

На следующих слайдах мы попытаемся дать им понятные определения, но стоит иметь в виду, что рынок далек от устоявшейся терминологии: игроки рынка по-разному обозначают одни и те же операции, исходя из собственного понимания, внутренней терминологии или идеологических причин.

Пример: На сайте Хабр Фриланс "верификацией аккаунта" называют простое подтверждение аккаунта через номер мобильного телефона. Никакие документы показывать не требуется, внешние системы верификации не используются. В VK "верификацией" называют только подтверждение того, что профиль действительно принадлежит известному человеку (музыканту, бизнесмену, блогеру), и эта сложная процедура включает предоставление документов и доказательства известности. Схожая процедура для обычных пользователей VK называется "Подтверждение данных аккаунта" и задействует внешние системы верификации (описанные в этом обзоре).

# Идентификация и Аутентификация

**Идентификация** отвечает на вопрос «Кто это?».

Идентифицируется один пользователь из множества пользователей.

Ответом на вопрос является идентификатор клиента, который может быть любым: логин, электронная почта, телефонный номер, имя и фамилия, номер паспорта, ИНН, СНИЛС, другие коды, номера или ID.

**Аутентификация** – это процесс подтверждения того, что пользователь действительно тот, за кого себя выдает. Это проверка подлинности пользователя.

Подтверждением может служить пароль (соответствующий логину), цифровой сертификат, код из СМС (приходящий на указанный пользователем телефон), звонка, письма или пуш сообщения.

### Авторизация и Верификация

**Авторизация** - это следующий шаг после аутентификации. На основе выполненной проверки клиенту выдается разрешение на выполнение действий: войти на сайт, выполнить какие-либо операции, воспользоваться сервисами, получить доступ к ресурсам. Если проверка (аутентификация) выполняется сторонним провайдером, а не самой компанией, то такая авторизация называется «внешней авторизацией».

**Верификация** – это процедура проверки данных. Это проверка того, что личные данные, которые предоставил клиент, верны. Это проверка корректности документов, соответствия документов личности. Сравнение лица с фотографией в паспорте. Сравнение данных, указанных в профиле, с данными поставщика идентификации. Один к одному.

Пользователь, прошедший верификацию, называется «верифицированным пользователем».

### Пересечение терминов

И верификация, и аутентификация описывают процедуру проверки, и поэтому они часто используются как синонимы. Однако, аутентификация в большей степени описывает проверку подлинности самого пользователя, а верификация – проверку предоставленной им информации.

И аутентификация, и авторизация относятся к процедуре входа на сайт. Система сначала аутентифицирует пользователя, а потом позволяет ему войти на сайт (авторизует вход). Аутентификация не имеет смысла без следующего шага, который выполняется на основе результата проверки. Авторизация не может выполняться без проверки подлинности пользователя и его прав.

И **идентификация**, и **верификация** могут относиться к проверке личности клиента. Но, если идентификация подразумевает первичное установление личности, то верификация личности – это проверка ранее предоставленных клиентом данных о себе.

# Исследования Data Insight



<u>Карта Экосистема</u> электронной торговли 2022



ТОП-1000 российских интернет-магазинов 2022



Рейтинг российских интернетмагазинов Топ-100 2022



<u>Логистика итернет-торговли в</u> России 2023. Мнения и ожидания



Интернет-торговля в России 2022



### Партнеры Data Insight































































































































# Data Insight

Data Insight – первое в России агентство, специализирующееся на **исследованиях** и **консалтинге** в области eCommerce и digital рынков.

#### **Новости Data Insight**

Рассылка исследований
Data Insight на почту в
день публикации

Подписаться

#### Мониторинг eCommerce

Новостной еженедельный мониторинг рынка eCommerce от Data Insight

Подписаться

#### Контакты

datainsight.ru

a@datainsight.ru

+7 (495) 540 59 06









