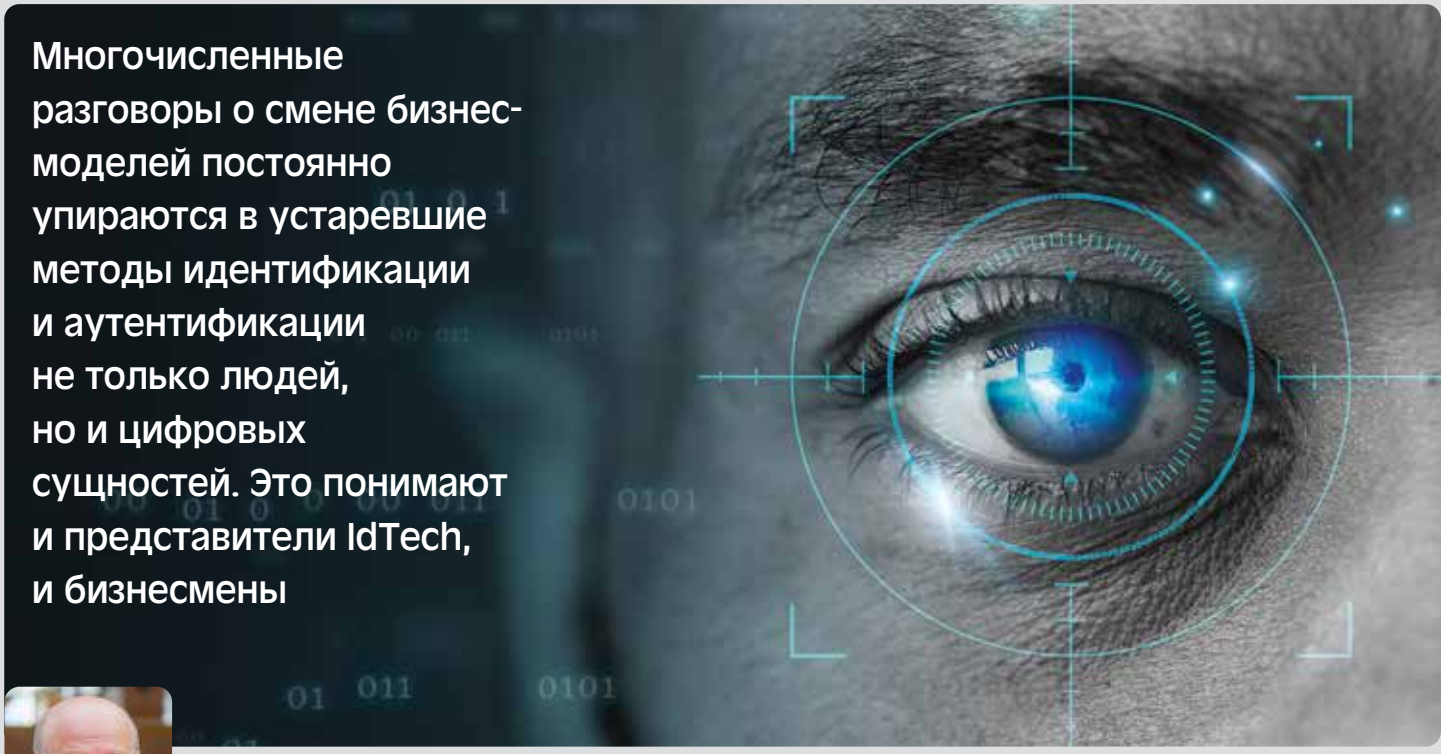
Сквозная многофакторная

Многочисленные разговоры о смене бизнес-моделей постоянно упираются в устаревшие методы идентификации и аутентификации не только людей, но и цифровых сущностей. Это понимают и представители IdTech, и бизнесмены





Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Сквозная и многофакторная идентификация (ID) с использованием ИИ и биометрии становится одним из условий развития финансовой отрасли. Традиционные способы неудобны в том числе длительными процессами верификации клиентов, рисками мошенничества и утечек данных, а также ограниченным доступом для клиентов из удаленных регионов.

Однако улучшение клиентского опыта и удобства перевешивают риски старых и новых способов ID. Сегодня крайне трудно заставить пользователей, например, ДБО постоянно вводить дополнительные факторы идентификации, перемещаясь по страницам финансового маркетплейса, предложения которого рассчитаны на инвесторов разного уровня квалификации. Сделать это трудно и на маркетплейсах для ограничения доступа к контенту и товарам для взрослых, алкоголю, табаку и т.д.

Что не так?

Но почему именно сейчас стек технологий IdTech находится на пике внимания? Ведь проблему идентификации и аутентификации людей так или иначе решали уже во времена строительства египетских пирамид. Напомним, именно оттуда в мир безопасности пришла максима: «Чтобы доказать, что ты это ты, у тебя должен быть хотя бы один фактор аутентификации — “я знаю”, “я имею”, а также “я есть”». Что здесь не так?

Не так здесь то, что все это хорошо работает, когда одному человеку нужно удостовериться, что перед ним именно тот человек, который себя за него выдает. Так сегодня происходит на перронах вокзалов, когда пассажиры предъявляют паспорт проводнику («я имею»), когда пользователи вводят логин и пароль («я знаю»), а также прикладывают палец к биометрическому терминалу («я есть»). Под эту связку факторов была «заточена» и правоохранительная система, которая пыталась карать тех, кто умышленно закрывал глаза на наличие или отсутствие факторов, например, на очной ставке при опознании подозреваемых или продаже алкоголя несовершеннолетним.

В цифровом мире все это перестает работать в единой связке: теперь не только люди должны идентифицировать не только людей, это, во-первых. Во-вторых, в виртуальном пространстве человек может находиться в любом месте физического мира, а услуга, к которой он хочет получить доступ или которую хочет приобрести, — во множестве виртуальных пространств: маркетплейсах, метавселенных, банковских или платежных приложениях. В-третьих, зачастую нарушается фундаментальный закон безопасности в физическом мире, предполагающий, что идентифицируемый человек уникален. В мире различных профилей в разных соцсетях, цифровых двойников и дипфейков понятно: он уже не один, и никакая ЕСИА, работая по старинке, здесь не поможет. Наконец, в рамках IoT человек может иметь не просто несколько своих профилей — появляются новые профили, уже не имеющие идентификаторов людей (поскольку они не люди), но привязанные, например, к банковскому счету какого-то человека.

Ну и что?

Поэтому на вопрос «Что не так с ID?» эксперты дают короткий ответ: «Бизнес-модели старого, исключительно физического мира не дают развиваться новым бизнес-моделям цифрового мира, а порой входят в противоречие с ними». Причем слово «законы» имеет прямое отношение к юриспруденции: и к 152-ФЗ «О персональных данных», и к «антиотмывочному» 115-ФЗ, и к 161-ФЗ «О национальной платежной системе».

Неудивительно, что в ноябре 2023 года в ходе Первой конференции Центра идентификации МТС председатель Национального совета финансового рынка (НСФР) **Андрей Емелин** заявил: «Меня больше всего беспокоит правоохранительная составляющая, потому что все технологические меры — это превенция, т.е. попытка не допустить покушения на клиента или удержать его от совершения действия под влиянием социального инженера. А по большому счету пресечение правонарушения обязательно должно заканчиваться привлечением к ответственности виновного. В этом вопросе НСФР вместе с коллегами готов проявить максимум активности».

В сентябре 2024 года в рамках XXI Международного банковского форума при обсуждении вала утечек персональных данных **Игорь Ашманов,** президент компании «Крибрум», дал понять, в каком направлении движется процесс наведения порядка в области ID. По его словам, старая бизнес-модель, когда собираются все персональные данные в самых неожиданных местах для возможной идентификации человека в будущем, ущербна и крайне неудобна своей бумажной бюрократией. Например, упомянутому выше проводнику в поезде при посадке вовсе не нужен паспорт пассажира, ему необходимо убедиться, что пассажир именно тот человек, на имя которого куплен билет. И всё!

Всё, да не всё

В принципе, идея экспертов понятна: нужно создавать один или несколько верхнеуровневых информационных хабов, где бы хранилась обезличенная информация о гражданах, как это сделано в ГИС ЕБС или ЕСИА. Это отраслевые базы о текущей активности граждан типа платформы «Знай своего клиента» Банка России, которые нужны исключительно для определения уровня доверия субъектов друг к другу.

Нужны хабы для обеспечения доступа по сквозному, универсальному ID в разные подсегменты рынка: виртуальный и физический, как это предлагает компания «Центр идентификации МТС». Потребуется закручивание гаек со стороны платежных систем, как это уже делает НСПК. Проблему с виртуальными сущностями можно отчасти решить при помощи аудита смарт-контрактов при тотальном переводе всех «нелюдéй» на платформу цифрового рубля.

А у основания всей этой пирамиды будут располагаться антифрод-системы самых разных масштабов и различной отраслевой принадлежности (эта работа уже активно ведется). Их назначение — не только контрольно-надзорная функция, но и обеспечение доверия ко всей цифровой инфраструктуре, в которой уже мало кто сегодня доверяет тому, кто находится на той стороне телефонной трубки или платежного терминала. Главное — пользователи получат доступ с минимальным количеством факторов аутентификации к тем сервисам, владельцы которых в рамках своей риск-политики будут готовы их допустить к ним, обеспечив сохранность клиентских данных.

Задача масштабная, и не факт, что все будет так, а не иначе. Но пока юристы пытаются понять, что думают представители бизнеса о том, как «не опоздать на этот поезд» и какие их сервисы могут быть доступны в рамках новых бизнес-моделей для клиентов.

Некоторые мысли представителей платежной индустрии были озвучены в ноябре 2024 года на ежегодном форуме «Банковского обозрения» FuturePay_24. В частности, **Владислав Святик,** заместитель генерального директора Центра Биометрических Технологий (ЦБТ), отметил: «Проект с московским метрополитеном "Плати улыбкой" показал, как можно изменить в лучшую сторону клиентский опыт за счет ускорения процессов. Но главное во всем этом то, что совместно с ГИС ЕБС и НСПК крайне успешно проходит пилотный проект биоэквайринга. Он позволяет подключаться любым участникам рынка с реальным обеспечением всем равноудаленности, равнодоступности и бесшовности клиентского пути. Любой человек в любой точке страны может расплатиться в любом ТСП с использованием биометрии. В этой связи у меня есть мечта — зайти в магазин, взять товар и просто выйти. Все остальное сделают технологии, они уже есть».

По мнению спикера, биоэквайринг, по-хорошему, — это только начало. На платежи всегда обращают внимание, поскольку все с ними сталкиваются. В связке с госуслугами и ЕБС биоэквайринг предоставляет ряд сопутствующих услуг. В портфеле ЦБТ сейчас 14 сервисов, а в 2025 году можно будет прийти в МФЦ без паспорта и без него же купить алкоголь с учетом ограничений по возрасту покупателя. Уже работает проход в бизнес-залы, готовится заселение в гостиницы без предъявления бумажного документа. Все это практическое проявление нового подхода к ID и IdTech. Б.О