сенсус

ЦИФРОВОЙ МАРКЕТПЛЕЙС

Цифровые решения – 2026 · аналитика по направлениям

Финансы, банки и страхование: агенты, биометрия и общая ответственность

Как банки, страховщики и финансовые платформы на форуме «Цифровые решения – 2026» обсуждали ИИ-агентов, массовую биометрию и ГИС «Антифрод»: цифры эффекта, барьеры и запросы к регуляторам.

Содержание

Ключевые показатели

Кратко

1. Состояние отрасли: платформы и биометрия

2. Масштаб угроз для финансового сектора

3. ИИ в банковских процессах и разработке

4. Клиентский сервис, каналы и киберстрахование

5. Барьеры отрасли

6. Запрос к регулятору: правила для ИИ-агентов и платформ

7. Антифрод и распределение ответственности

8. Капитал и финансирование инфраструктуры

9. Прогнозы и планы игроков

10. Барьеры и предложения

11. Ключевые игроки темы

Выводы

Источники

Ключевые показатели

около 1,2 трлн руб.

Сделки через финансовые платформы с начала действия закона

Алешина Кристина, Банк России

13 организаций

Операторы в реестре финансовых платформ

Алешина Кристина, Банк России

около 10 млн человек

Клиенты операторов финансовых платформ

Алешина Кристина, Банк России

порядка 100 млн

Биометрические оплаты за первое полугодие 2026 года

Святик Владислав, ЦБТ; статистика Банка России

0 успешных атак

Успешные атаки на оплату по биометрии в Сбере

Евсеев Олег, Сбер; при 27,5 млн успешных транзакций

порядка 400 тыс.

Счета, открытые дистанционно по биометрии

Поволоцкий Владислав, ЦБТ; без случаев мошенничества

в 3–10 раз дороже

Цена украденного аккаунта с биометрической верификацией

Иванов Антон, «Лаборатория Касперского»; к обычному аккаунту

около 40

Участники, подключённые к ГИС «Антифрод»

Скворцова Татьяна, Минцифры России; более 25 – финансовые

более 130

ИИ-проекты банка на этапе промышленного использования

Кутузов Станислав, Банк «Санкт-Петербург»

более 70 млн руб. в год

Эффект продукта, созданного сотрудником через вайб-кодинг

Кутузов Станислав, Банк «Санкт-Петербург»

50 000 клиентов в неделю

Темп открытия единого ИИ-ассистента для юрлиц

Баттулин Дамир, Альфа-Банк

около 50 млн руб.

Оборудование для прямого подключения МФК к ЕБС

Пустовит Александр, «МигКредит»; оценка

более 200 млрд руб.

Заявки на финансирование ЦОД в портфеле ВТБ

Голыгина Юлия, ВТБ; общая мощность более 200 МВт

100 млн руб.

Ущерб ритейлера от шифровальщика при полисе дешевле 10 млн

Скворцов Владимир, «АльфаСтрахование»; оценка

38 млн клиентов

Согласия клиентов Сбера на обмен через цифровой профиль

Днепровский Петр, Сбер

Кратко

Финансовый сектор на форуме «Цифровые решения – 2026» обсуждал уже не цифровизацию каналов, а три сдвига сразу. Первый – ИИ-агенты как новый тип клиента и сотрудника: банки считают эффект в рублях и одновременно спорят, кто отвечает за действие агента. Второй – биометрия перешла в массовые платежи, но стоимость подключения отсекает небольшие организации. Третий – борьба с мошенничеством переходит от добровольного обмена данными к обязательной ГИС «Антифрод» с распределённой ответственностью банков, операторов и платформ. В основу отчёта легли 23 сессии с участием Банка России, Минцифры России, банков, страховщиков, финансовых платформ и ИБ-компаний.

Главные цифры: через финансовые платформы проходит 120 млрд руб. сделок в квартал (Алешина Кристина, Банк России); за первое полугодие 2026 года проведено порядка 100 млн биометрических оплат (Святик Владислав, ЦБТ); в Банке «Санкт-Петербург» более 130 ИИ-проектов, а эффект втрое превышает инвестиции (Кутузов Станислав, Банк «Санкт-Петербург»); подключение к ГИС «Антифрод» станет обязательным с 1 марта 2027 года (Скворцова Татьяна, Минцифры России).

1. Состояние отрасли: платформы и биометрия

Финансовые платформы и биометрическая оплата вышли из стадии пилотов: у первых устойчивый квартальный оборот и крупные банки среди участников, у второй – десятки миллионов транзакций в месяц без зафиксированного мошенничества.

1.1 Финансовые платформы: оборот и смена роли

Кристина Алешина (Банк России) привела сводные данные по рынку финансовых платформ. С начала действия закона через них совершено сделок примерно на 1,2 трлн руб., в реестре 13 операторов, клиентами являются около 10 млн человек. За последние четыре квартала ежеквартальный объём сделок составлял 120 млрд руб. Линейка расширилась от вкладов до облигаций и цифровых финансовых активов, но всплеска операций с ЦФА регулятор пока не видит. Регионы привлекают через платформы средства граждан по народным облигациям; Игорь Алутин (Московская биржа) назвал Калининград, Красноярск и Амурскую область. При размещении облигаций регионов и компаний Банк России требует от операторов полностью раскрывать информацию об эмитенте (Алешина Кристина, Банк России).

Изменился и состав участников. По словам Алешиной, крупные банки присоединяются к платформам, чтобы использовать готовую инфраструктуру и сокращать расходы на привлечение клиентов, а микрофинансовые организации – чтобы идентифицировать клиентов по поручению и не строить собственную биометрическую инфраструктуру. Александр Крайник («Сравни») описывает это как двустороннее движение: небольшие организации получают доступ к спросу и конкурируют с банковскими экосистемами

качеством продукта, а для крупных банков маркетплейс становится последней возможностью удержать клиента, который вышел на открытый рынок. Конкуренция, по его оценке, смещается от владения клиентом к закрытию конкретного клиентского пути: человек «с утра клиент одного сервиса, в обед клиент другого, а вечером третьего».

Рост финтеха за пределами классических банков фиксируют и маркетплейсы. По данным Ozon, финтех компании вошёл в топ-25 крупнейших банков России по объёму активов и регулярно показывает чистую прибыль; банк выделен в изолированный контур с выполнением требований Банка России, а вход в него из кабинета маркетплейса требует дополнительного подтверждения.

1.2 Биометрия как массовая платёжная инфраструктура

Биометрия в финансах перестала быть пилотом. По статистике Банка России, которую привёл Владислав Святик (ЦБТ), за первое полугодие 2026 года проведено порядка 100 млн биометрических оплат, а за весь период биоэквайринга – порядка 400 млн транзакций без зафиксированного фрода. Олег Евсеев (Сбер) сообщил, что только за сентябрь банк провёл 21,5 млн таких транзакций, а у сервиса более 2,7 млн уникальных пользователей в месяц. Оплата занимает около четырёх секунд, доля ложных отказов – меньше 2%. Без дополнительного фактора по биометрии можно оплатить до 10 000 руб., выше нужен биометрический ПИН.

> 27 с половиной миллионов успешных транзакций оплаты и 0 успешных атак. – Олег Евсеев, Сбер

Из 111 млн клиентов Сбера по биометрии могут обслуживаться 32 млн (Евсеев Олег, Сбер). В коммерческих биометрических системах крупных банков хранится 100 млн векторов (Скворцова Татьяна, Минцифры России). Владислав Поволоцкий (ЦБТ) сообщил, что с помощью биометрии дистанционно открыто порядка 400 тыс. банковских счетов без случаев мошенничества, и ожидает практически полного покрытия финансово активного населения – это 90+ млн человек – в ближайшие 1–2 года. По данным ЦБТ, в биометрической базе более 70 млн образцов, из них для сервиса небанковских финансовых организаций доступны 27 млн, а подключением к биометрии охвачено порядка 80% рынка таких организаций (Святик Владислав, ЦБТ).

80% атак на биометрические терминалы Сбера, по словам Евсеева, – попытка предъявить фото с экрана смартфона. Вирусные видео об «оплате по фото друга» банк разобрал и квалифицировал как монтаж. Слабое место технологии – близнецы: Сбер закрывает его ПИН-кодами и обсуждает с оператором ЕБС общий подход.

2. Масштаб угроз для финансового сектора

Финансовый сектор остаётся главной мишенью: злоумышленники покупают инсайдеров и биометрически верифицированные аккаунты, а каждая новая защитная мера за несколько месяцев вызывает смену тактики.

2.1 Инсайдеры, утечки и спрос на верифицированные аккаунты

Антон Иванов («Лаборатория Касперского») по данным киберразведки сообщил, что 29% рассмотренных объявлений на закрытых ресурсах связаны с поиском инсайдеров в финансовом и микрофинансовом секторе с доступом к банковским данным. Зафиксировано 3 603 объявления с предложениями сотрудникам микрофинансовых организаций и 236 публикаций баз данных заёмщиков банков и МФО. Спрос на украденные банковские аккаунты, прошедшие биометрическую верификацию, вырос в 2 раза, а стоят они в 3–10 раз дороже обычных. По оценке Иванова, злоумышленники готовятся к атакам на биометрическую идентификацию, собирая данные через инсайдеров финансовых организаций. Алексей Лукацкий (Positive Technologies) добавил, что в даркнете уже продаются записи в ЕБС: люди за деньги дают мошенникам пользоваться своим лицом и голосом.

2.2 Смена тактики мошенников

Алексей Ипатов (Сбер) описал, как мошенники реагируют на ограничения. После введения лимитов на токены они за несколько месяцев перешли на NFC и заставляют жертву прикладывать карту к телефону. Периоды охлаждения вызвали новую волну вредоносного ПО, в том числе против юрлиц, где средний ущерб на порядки выше. Мошенничество, по словам Ипатова, – уже не одиночки, а крупные организации, которым можно противостоять только через государственно-частное партнёрство.

ИИ меняет и атаки на бизнес. Петр Хенкин (Сбер) указал, что персонализированный фишинг из инструмента против крупных компаний превращается в массовую автоматизированную атаку, а наличие денег и дистанционного банковского обслуживания делает целью компанию любого размера. Его формула: «Голос и письмо – это больше не доказательства». Максим Кабрера (Билайн) отметил возврат фишинга в мессенджеры, которым люди доверяют больше: схемы стали трёхуровневыми, с поддельными документами, вредоносным ПО и полным контролем над телефоном.

При этом уровень защиты крупных банков остальным недоступен. В центре киберзащиты Сбера, по словам Лукацкого, работают 1 400 человек – ресурс, которого нет почти ни у кого за пределами крупных банков. Андрей Выборнов (Банк России) сформулировал позицию регулятора: «идея о том, что он сам себя защитит», применительно к гражданину принципиально неверна, клиента банка нужно защищать как аксиому. Мошенничество, по его описанию, проходит три этапа – воздействие на человека, поиск денег и их передача, – и защита нужна на каждом, в первую очередь со стороны банка.

3. ИИ в банковских процессах и разработке

Банки считают эффект ИИ в рублях, но расходятся в оценке масштаба: одни отчитываются подтверждённой финансовой службой отдачей и кратным ускорением разработки, другие не видят сквозного прироста на уровне всей компании.

3.1 Эффект, подтверждённый финансовой службой

Станислав Кутузов (Банк «Санкт-Петербург») представил наиболее полный отчёт об эффектах. Более 130 ИИ-проектов банка выходят на этап промышленного использования, а подтверждённый финансовой службой эффект втрое превышает инвестиции. Один продукт, созданный сотрудником через вайб-кодинг в выделенной безопасной среде, принёс более 70 млн руб. в год. Банк запустил агентную платформу для передачи рутинных задач цифровым помощникам и рассчитывает привлечь первую 1 000 цифровых сотрудников в первом квартале. Проекты оцениваются по трём признакам: бизнес-эффекту, высвобождению ресурсов и сокращению времени поставки функционала.

Ключевой вывод банка: когда доступ к инструментам дали всем сотрудникам, они начали приносить кейсы, которые централизованная команда не могла придумать. «Мы верим в то, что это больше про смену культуры», – сказал Кутузов: сотрудники учатся нанимать цифровых сотрудников, ставить им задачи и контролировать результат. Оговорка та же, что и у других банков: результат агента нельзя передавать дальше без проверки, а ошибки зависят в том числе от качества контекста и инструкций.

3.2 Разработка: кратное ускорение и скепсис

В разработке банки фиксируют разные результаты. По словам Алексея Фетисова (Альфа-Банк), агенты по качественной спецификации делают за 2 недели то, что раньше делали за полгода; агент в среде разработки задаёт 400–500 вопросов по бизнес-идее и встраивает в спецификацию правила кибербезопасности. На последней итерации оркестратора банк получил ускорение до 4 раз на определённом классе задач. Обратная сторона – огромный объём кода, который нужно проверять. Рафаел Тонаканян (Сбер) сообщил, что у отдельных команд объём генерируемого кода вырос в 8–10 раз, а бизнес-метрикой выбрано число задач, внедрённых в production на одного сотрудника.

Игорь Маслов (Т-Банк) занимает более осторожную позицию. Массовое применение ИИ для написания кода пока не дало банку общего результата: «на масштабе большой компании значимого прироста в эффективности» и в сроках вывода продуктов, по его словам, нет. Т-Банк снизил удельную стоимость экспериментов за счёт дешёвой эксплуатации GPU и баланса внешних токенов с собственными развёртываниями. Среды выполнения агентов банк переводит в облако и ограничивает их локальное использование: запуск универсальных агентов на компьютерах сотрудников создаёт риск выгрузки корпоративных данных на устройства. Там, где эффект заметен, он связан с эксплуатацией: агент в платформе Sage заранее обнаруживает большую часть проблем и ускоряет их устранение (Маслов Игорь, Т-Банк).

4. Клиентский сервис, каналы и киберстрахование

В клиентских каналах банки и страховщики передают ИИ рутину и первую линию, но ответственность перед клиентом оставляют человеку; тот же принцип разделения риска лежит в основе киберстрахования.

4.1 Клиентский сервис и цифровые каналы

В корпоративном банкинге Альфа-Банк перенёс розничный подход на юрлиц; принцип, принятый в 2023 году, Дамир Баттулин (Альфа-Банк) сформулировал так: «Юрик – это физик». Банк выделил 4 роли пользователей – предприниматель, бухгалтер, руководитель и финансовый эксперт – и меняет интерфейс под выбранную роль. Единый ИИ-ассистент открыт клиентам-юрлицам, доступ расширяется примерно по 50 000 клиентов в неделю; следующий шаг – переход ассистента к выполнению операций.

Сбер строит омниканальную оркестрацию: Сбер ID используют более 100 млн клиентов, а следующий шаг клиента банк прогнозирует трансформерами, обученными на последовательностях действий (Дзюба Александр, Сбер). Андрей Турунов («Ренессанс страхование») сообщил, что компания за год утроила месячную аудиторию собственных цифровых каналов с ростом удовлетворённости и разработала собственный мультиканальный шлюз-оркестратор. Стратегия страховщика – AI First, но не AI Only: как только у клиента падает удовлетворённость или он не согласен с решением ИИ, диалог передаётся живому эксперту. «Перед клиентом ответственность всегда несёт человек, компания и люди, которые в ней работают», – пояснил Турунов. Александр Дзюба согласен: у агентов никогда не будет полного знания контекста и клиентов, поэтому ответственность останется за человеком.

> Люди доверяют людям, а не искусственному интеллекту. – Андрей Турунов, «Ренессанс страхование»

На «Финуслугах» Московской биржи клиент может включить переоткрытие вклада по наиболее выгодной ставке на момент завершения размещения, а банки используют платформу как канал розничной ликвидности, меняя ставки под текущую потребность в средствах (Алутин Игорь, Московская биржа). Реализован MCP-доступ, позволяющий агенту открыть счёт в интегрированной финансовой организации. «Сравни» после разъяснения пользователям долговой нагрузки увеличил частоту возврата в продукт «Кредитный рейтинг» в 3 раза (Гамзаев Магомед, «Сравни»).

4.2 Киберстрахование и сервисы безопасности

Владимир Скворцов («АльфаСтрахование») описал киберстрахование как элемент архитектуры защиты: оно необходимо, потому что «полностью защититься невозможно». Перед заключением договора клиенту проводят бесплатный киберчекап, обсуждают план восстановления и реагирования, а премия зависит прежде всего от оценки системы защиты. В кейсе крупного регионального ритейлера шифровальщик остановил все системы, магазины перешли на бумагу; ущерб оценивается в 100 млн руб. при полисе дешевле 10 млн и лимите выплаты 1 млрд руб. Полис покрывает восстановление и локализацию, материальный ущерб, ответственность перед третьими лицами и перерыв производства. Страховщик ожидает, что с ИИ предстраховой аудит станет дешевле и

быстрее. Иную оценку рынка дал Александр Ковалевский («ИКС Безопасность»): доступного страхования киберрисков, сопоставимого со страхованием обычных бизнес-рисков, в России пока нет.

Банки выводят собственные инструменты безопасности на рынок. В Альфа-Банке ИТ-ландшафт меняется несколько сотен раз в день, поэтому банк создал облачный «Альфасканер» и открыл его клиентам и партнёрам (Фетисов Алексей, Альфа-Банк). Рядом формируются гарантийные модели ИБ-вендоров: по данным Positive Technologies, компания возвращает деньги, если защиту удалось взломать, и работает со страховщиками; по данным ГК «Солар», компания обязуется компенсировать ущерб до 30 млн руб. без участия страховой.

5. Барьеры отрасли

Три главных ограничения отрасли – стоимость биометрии для небанковских организаций, качество доступа к государственным данным и неописанные риски ИИ-агентов.

5.1 Стоимость и сложность биометрии

Для небанковских организаций биометрия упирается в деньги. Александр Пустовит («МигКредит») оценил закупку оборудования для прямого подключения к ЕБС под объёмы компании примерно в 50 млн руб.; к этому добавляются специалисты, соблюдение ГОСТ и ежегодный аудит. Делегированные решения через банк или платформу, по его оценке, примерно на треть дешевле и на горизонте трёх лет экономически обоснованнее. Магомед Гамзаев («Сравни») сообщил, что компания создала облачный сервис, позволяющий МФО интегрироваться с биометрией за 2 недели. Владислав Святик (ЦБТ) поддерживает такие схемы: задача оператора – масштабировать рынок, а не зарабатывать на прямых подключениях. Евсеев назвал причину дороговизны: экономику проектов осложняет стоимость криптозащиты, аттестации, аккредитации и сертификации.

Второй барьер – клиентский путь. По описанию Михаила Булатова (Т-Банк), биометрическая идентификация в МФО сейчас требует множества переходов между банком, Госуслугами, MAX и приложением биометрии; цель – 1–2 касания и 1–2 интерфейса. По замерам «Сравни», около 15% клиентов теряются из-за отсутствия перехода между приложениями, а после его внедрения показатели успешных авторизаций выросли в 2 раза (Гамзаев Магомед, «Сравни»). Пустовит предупреждает о последствии: клиент без биометрии в базе может не получить финансирование и уйти к нелегальным кредиторам. Евсеев признаёт, что отрасль нашла «баланс между безопасно и удобно, но немножко забили на доступно».

> В этом залатывании дыр мы немножко увлеклись и чуть-чуть замуровали вход. – Олег Евсеев, Сбер

Лукацкий оценивает требования жёстче: они подняты настолько, что войти на рынок могут единицы, и система недоступна почти всему рынку. Евгений Семёнов (ЦБТ) возражает, что высокие требования к государственной инфраструктуре доверия оправданы рисками, а упрощать нужно клиентские сценарии – соразмерно уровню риска.

5.2 Доступ к государственным данным

Петр Днепровский (Сбер) описал проблемы цифрового профиля как инфраструктуры для онлайн-кредитования. Согласие на обмен данными дали 38 млн клиентов банка, но, по его словам, 20% ответов не поступает, а из поступивших лишь 20% приходит за минуту. Для онлайн-сценариев это слишком долго. Сокращение срока согласия и введение платы за обновление данных вынуждают клиентов вручную обновлять сведения, то есть сервис для клиента ухудшился.

У финансовых платформ свой разрыв. Оператор может получить данные цифрового профиля и кредитный отчёт с согласия клиента, но не может передать их банку-партнёру, и банк повторно запрашивает те же сведения (Крайник Александр, «Сравни»). Алутин отмечает, что статус финансовой платформы не снимает трудоёмкость интеграций: ряду банков ещё нужно развивать дистанционное обслуживание и внешние API.

5.3 Риски ИИ-агентов в финансах

Банки формулируют риски агентов конкретно. Дмитрий Никишов (Банк ДОМ.РФ) указывает, что ИИ вскрывает процессы, державшиеся на устных договорённостях, массовое повторение безобидных действий агента может перерасти в масштабную проблему, а обновление облачной модели требует пересборки защитной обвязки. В кредитном процессе агенту, по его словам, можно поручить сбор данных в защищённом контуре, но решение об изменении условий для клиента следует оставить человеку. Фетисов фиксирует, что расход токенов на одну и ту же задачу различается до 5 раз, что ломает бюджетный цикл. Хенкин призывает внимательно контролировать права и привилегии агентов.

Отдельный риск – конфликт интересов. Баттулин ставит вопрос, чьи интересы представляет агент платформы, и предупреждает, что непрозрачность может стоить дистрибуции в пользу независимых агентов; его вывод – «честным быть становится технологически выгодно». Алутин указывает на рекламную подмену в ИИ-поиске и на противоречивые сведения нейросетей о стоимости акций. Для критической финансовой инфраструктуры экономия на дешёвом внешнем доступе к ИИ, по его оценке, может обернуться миллиардами расходов на восстановление систем; к определённому критическому контуру биржа генеративный ИИ не допускает.

6. Запрос к регулятору: правила для ИИ-агентов и платформ

Главный запрос рынка к Банку России – нормативно описать сделку, которую от имени клиента совершает ИИ-агент, и расширить полномочия финансовых платформ в работе с данными и идентификацией.

6.1 Правила для финансовых ИИ-агентов

По словам Игоря Алутина, нормативного описания взаимодействия человека с финансовой организацией через агента сейчас нет. Московская биржа намерена вместе с Банком России и участниками рынка описать цепочку «клиент – ИИ-агент – финансовая организация»; Алутин рассчитывает, что для этого запустят рабочую группу на площадке Ассоциации ФинТех. Финансовым организациям, по позиции биржи, нужны подтверждение распоряжения человеком и хранение данных для проверки регулятором, а сделки агентов следует фиксировать в доступном человеку реестре. Речь при этом идёт о правилах взаимодействия, а не об отдельной правосубъектности агентов. Алутин также ожидает появления реестра доверенных финансовых агентов, роль которого могла бы выполнять биржа, а для нейросетей биржа планирует выдавать проверенные агрегированные данные рынка.

> Описать, кто где, на каком этапе несёт ответственность, как это регулируется и где сделки будут записываться, – это вот сейчас самое важное. – Игорь Алутин, Московская биржа

Практическая база для таких правил уже есть: на хакатоне Московской биржи ИИ-агенты совершили 17 000 операций, и этот эксперимент биржа использовала для определения инфраструктуры нового рынка (Алутин Игорь, Московская биржа). Банкам Алутин объясняет новую роль коротко: «агент – это ваш новый клиент».

Крайник добавляет, что без описания клиентских путей на рынке появятся непрозрачные финансовые агенты, которых сложнее контролировать, чем обычных посредников. Алутин просит, чтобы регулирование ИИ учитывало разницу между крупными финансовыми организациями и небольшими финтех-компаниями, и ожидает разделения ИИ-систем на критичные и некритичные с требованием суверенных моделей только для первых.

6.2 Функциональность финансовых платформ

Операторы платформ просят расширить свои возможности. Крайник предлагает привлекать их к проектам открытых API с этапа проектирования клиентских путей, допустить к видеоидентификации, разрешить передачу данных цифрового профиля и кредитной истории партнёру по поручению клиента. Алутин предлагает открыть для платформ API государственных сервисов по примеру открытых интерфейсов финансовых организаций.

Кристина Алешина сообщила, что часть изменений уже прорабатывается, а подключение платформ к открытым API регулятор отнёс ко второму контуру. Банк России обсуждает с ведомствами допуск на платформы юрлиц и индивидуальных предпринимателей. Видеоидентификацию Алешина поддержала как личное мнение, оговорив, что вопрос в компетенции другого департамента. Надзор, по её словам, сосредоточен на корректной передаче данных регистратору финансовых транзакций и подтверждении прав клиента на продукт; недочёты в такой передаче у платформ выявлялись.

7. Антифрод и распределение ответственности

Борьба с мошенничеством переведена на обязательную основу: с 1 марта 2027 года участник, получивший сигнал ГИС «Антифрод» и не принявший мер, отвечает за ущерб, – но операторы связи считают распределение ответственности неполным.

7.1 ГИС «Антифрод»: сроки и модель

Татьяна Скворцова (Минцифры России) изложила принятые решения. Законом № 41-ФЗ создана ГИС «Антифрод» – единая платформа обмена значимыми событиями между банками, операторами связи, цифровыми платформами и регуляторами; второй пакет мер (закон № 210-ФЗ) дополняет антифрод-регулирование. Подключение станет обязательным с 1 марта 2027 года для операторов связи, кредитных организаций, цифровых платформ и ряда органов власти. Сейчас подключено около 40 участников: крупнейшие операторы связи, более 25 финансовых организаций и цифровые платформы. До конца года Минцифры планирует более 120 участников, запущено 11 сценариев взаимодействия из 34 запланированных на год. Новый сценарий можно запустить в течение месяца, что позволяет опережать новые схемы.

Скворцова объяснила выбор модели: ответственность консолидированная, между операторами, банками и платформами, а не британская модель с перекосом на банки. Отвечает тот участник, который получил сигнал, но не принял мер; неподключение от ответственности не освобождает. Добровольные каналы обмена, по оценке министерства, ответственности не создают и проблему не решают. По данным МВД России, которые привела Скворцова, мошенничество снизилось на 32% к аналогичному периоду прошлого года.

Андрей Выборнов сообщил, что Банк России добивается подключения всех банков к 1 марта 2027 года, когда возникает ответственность за неиспользование сигналов. Прежние попытки наладить обмен данными банков и операторов системного успеха не дали, и ГИС «Антифрод» он назвал первым таким механизмом. Антифрод-системам банков нужно больше качественных данных, чтобы выявлять мошенничество без большого числа ложных срабатываний, а сами инструменты зависят от вендоров АБС и ДБО, не все из которых воспринимают проблемы граждан как свои.

7.2 Спор о том, кто отвечает

Максим Кабрера (Билайн) считает модель неполной. Закон, по его описанию, закрепляет каскад: сначала проверяется банк, затем оператор связи. Отвечает тот, кто обслуживает клиента, – оператор-получатель вызова, тогда как оператор, в сети которого находится мошенник, ответственности не несёт. Кабрера предлагает распространить ответственность на цифровые платформы и мессенджеры, куда со временем перетечёт мошенничество, и указывает на слабость пакетных мер: схема, закрытая одним участником, переходит к тем, кто меры не внедрил, раньше, чем принимается закон. Билайн планирует распространить страховку от мошенничества на всех абонентов в дополнение к компенсации по закону.

Алексей Ипатов напоминает, что для банков ответственность не нова – они давно компенсируют гражданам потери, а регулятор публикует статистику возмещений. Сбер выбрал стратегию shift left – получать сигналы о мошенничестве и заражении до финальной стадии перевода – и ожидает, что при сохранении тренда объём и число возмещений в следующем году снизятся. Открытым Выборнов назвал вопрос о том, на какие ограничения граждане готовы ради защиты: пропущенный мошеннический перевод вызывает такое же недовольство, как остановленная операция. Лукацкий видит побочный эффект: антифрод-меры выталкивают мошенников в неконтролируемые каналы, и борьба идёт с каналом, а не с причинами.

8. Капитал и финансирование инфраструктуры

Банки готовы финансировать центры обработки данных, но только под подтверждённый спрос и с оговорками о стоимости длинных денег; у регулятора просят снизить нагрузку на капитал.

8.1 Портфель заявок ВТБ

Юлия Голыгина (ВТБ) сообщила, что банк рассматривает заявки на финансирование ЦОД общей мощностью более 200 МВт и суммой более 200 млрд руб. Ориентир общего срока окупаемости проекта – 10–12 лет, в этом году банк планирует начать финансирование двух проектов. При оценке ВТБ смотрит прежде всего на подтверждённый денежный поток, регион, крупных заказчиков и опыт оператора. Отсутствие оператора в реестре ЦОД само по себе финансирование не блокирует. Собственная энергетическая нагрузка банка, связанная с развитием ИИ, к 2030 году, по оценке Голыгиной, вырастет в разы.

8.2 Ограничения и инструменты

Ограничения названы прямо: долгосрочные проекты финансируются более короткими деньгами, что создаёт риск фондирования; фиксированная ставка на длинный срок практически недоступна, и финансовая модель должна выдерживать плавающую. Рыночный риск регионального ЦОД под спрос, не подтверждённый документами, банк не берёт; комфортнее вариант, когда крупный инициатор сам обеспечивает потребление части мощностей (Голыгина Юлия, ВТБ).

Из доступных инструментов Голыгина назвала лизинг будущего объекта инфраструктуры и аккредитивы с постфинансированием по ставке в юанях для импортного оборудования. Схему она советует обсуждать с банком на раннем этапе, чтобы подобрать инструменты под возникающие расходы. Отрасли, по её мнению, помог бы единый по стране индекс средней стоимости строительства мегаватта мощности ЦОД с разбивкой по регионам. Для банковских вложений в капитал приоритетных инфраструктурных компаний ВТБ предлагает Банку России снизить регуляторную нагрузку на капитал.

9. Прогнозы и планы игроков

Участники рынка ждут, что пользовательский интерфейс перестанет быть основной точкой контакта с клиентом, а ближайшие обязательства привязаны к 2027 году – сроку подключения к ГИС «Антифрод» и расширения биометрии для МФО.

9.1 От продукта и интерфейса к сценарию и протоколу

Алутин допускает, что финансовая платформа перейдёт от интерфейса к протоколу, предоставляющему внешним агентам интеграции с финансовыми организациями. Компаниям он советует открывать данные через MCP и адаптировать сайты для агентов: кого не видит агентный поисковик, того, по его словам, нет на рынке. Турунов прогнозирует сервис, который решает потребность до обращения клиента и взаимодействует с его персональным агентом. Дзюба ожидает, что ИИ-помощники с памятью о контексте пользователя смогут конкурировать с персональными менеджерами.

> На мой взгляд, интерфейсов не будет. Мы видим себя протоколом для агентов. – Игорь Алутин, Московская биржа

Крайник прогнозирует переход финансового рынка от продуктовой стратегии к сценарной: банки сохраняют управление рисками, а платформы доставляют продукты под жизненные ситуации. Старение населения и изменение рынка труда усилят спрос на решения в медицине и благосостоянии. Алутин ожидает, что при снижении ключевой ставки часть вкладчиков перейдёт в инструменты коллективных инвестиций; биржа развивает фонды денежного рынка и сервис «Финмаяк». Алешина назвала идеальным будущим платформ трансграничную интеграцию – начиная с СНГ, затем БРИКС, – оговорив, что это взгляд «если помечтать».

9.2 Обязательства и сроки

Банк «Санкт-Петербург» ставит цель сделать агентную разработку в 2 раза быстрее и в 2 раза дешевле и в следующем году объединять цифровых сотрудников в процессы (Кутузов Станислав, Банк «Санкт-Петербург»). Альфа-Банк рассчитывает на двукратный рост производительности в направлениях AI-native, а его группа по токеномике до конца года подготовит 2 блюпринта по стоимости генеративной разработки и экономике эксплуатации

(Фетисов Алексей, Альфа-Банк). По данным Сбера, банк перестраивает внутреннее производство ПО на агентную разработку и вместе со «Школой 21» запускает внешнюю сертификацию.

По биометрии Булатов сообщил, что Т-Банк вместе с Минцифры России прорабатывает новые способы сбора и рассчитывает к марту 2027 года обеспечить доступность сервиса для МФО нескольким десяткам миллионов людей. «Сравни» разрабатывает коробочное решение подключения, на тестовом контуре уже 4 интеграции (Гамзаев Магомед, «Сравни»). Святик надеется обеспечить идентификацию только по лицу до наступления следующего года. Евсеев считает правильным, что аккредитованных операторов коммерческих биометрических систем будет мало – по траектории операторов сотовой связи. Семёнов предостерегает от крайности: он не видит будущего, в котором всё делается по лицу в отрыве от других механик и контролей.

10. Барьеры и предложения

Большинство барьеров, названных на форуме, адресованы Банку России и Минцифры России и касаются трёх тем: правил для ИИ-агентов, стоимости биометрии и обмена данными.

Барьер	Кто называет	Что предлагают (адресат)
Нет нормативного описания взаимодействия клиента с финансовой организацией через ИИ-агента	Игорь Алутин, Московская биржа	Рабочая группа на площадке АФТ, подтверждение распоряжений человеком, реестр доверенных агентов (Банк России)
Риск непрозрачных финансовых ИИ-агентов	Александр Крайник, «Сравни»	Заранее описать клиентские пути и правила (регулятор, участники рынка)
Высокая стоимость прямого подключения к ЕБС для МФО	Александр Пустовит, «МигКредит»; Магомед Гамзаев, «Сравни»	Делегированные и коробочные решения, совместное наполнение биометрической базы (ЦБТ, операторы платформ)
Длинный клиентский путь биометрической идентификации в МФО	Михаил Булатов, Т-Банк	Сократить до 1–2 касаний, перенести часть сервисов в коммерческие системы (операторы биометрии, регуляторы)
Избыточная строгость правил биометрии в бытовых сценариях	Олег Евсеев, Сбер	Упростить правила для гостиниц и продаж 14+ (Минцифры России)
Ответы цифрового профиля не поступают или приходят поздно	Петр Днепровский, Сбер	Согласовать SLA, тарифы по модели «себестоимость плюс», порядок споров (Минцифры России)

Барьер	Кто называет	Что предлагают (адресат)
Платформа не может передать банку данные цифрового профиля и кредитную историю	Александр Крайник, «Сравни»	Передача сведений по поручению клиента (регулятор, законодатели)
Добровольный обмен данными о мошенничестве не создаёт ответственности	Татьяна Скворцова, Минцифры России	Обязательное подключение к ГИС «Антифрод» с 1 марта 2027 года (банки, операторы, платформы)
Не отвечает оператор, в сети которого находится мошенник	Максим Кабрера, Билайн	Распространить ответственность на всех участников цепочки, включая платформы и мессенджеры (законодатель, Минцифры России)
Неясно, кто отвечает перед гражданином при инциденте с биометрией	Алексей Лукацкий, Positive Technologies	Определить ответственного (Минцифры России)
Банки финансируют долгие проекты ЦОД короткими деньгами	Юлия Голыгина, ВТБ	Снизить нагрузку на капитал при вложениях в приоритетные отрасли (Банк России)
Нет доступного страхования киберрисков	Александр Ковалевский, «ИКС Безопасность»	Создать доступный продукт (страховые компании)

11. Ключевые игроки темы

Повестку направления определяли регуляторы, крупнейшие банки и операторы платформ и биометрии.

- **Банк России** – Кристина Алешина привела сводную статистику финансовых платформ (1,2 трлн руб. сделок), Андрей Выборнов – позицию по ГИС «Антифрод» и защите клиента как аксиоме.
- **Московская биржа** – Игорь Алутин: «Финуслуги» как протокол для агентов, инициативы рабочей группы АФТ и реестра финансовых агентов.
- **Сбер** – Олег Евсеев (биометрическая оплата, 0 успешных атак), Петр Днепровский (цифровой профиль, 38 млн согласий), Алексей Ипатов (shift left в антифроде), Александр Дзюба (омниканальная оркестрация), Рафаел Тонаканян (агентная разработка).
- **Альфа-Банк** – Дамир Баттулин (принцип «юрик – это физик», 50 000 клиентов в неделю), Алексей Фетисов (ускорение разработки до 4 раз, «Альфасканер»).
- **Т-Банк** – Игорь Маслов (скептическая оценка ИИ-кодинга, перенос агентов в облако), Михаил Булатов (путь биометрии в 1–2 касания).

- **Банк «Санкт-Петербург»** – Станислав Кутузов: более 130 ИИ-проектов, эффект втрое выше инвестиций.
- **Банк ДОМ.РФ** – Дмитрий Никишов: правила ответственности за действия агента, решения по кредиту за человеком.
- **ВТБ** – Юлия Голыгина: заявки на финансирование ЦОД более 200 млрд руб., окупаемость 10–12 лет.
- **«Сравни»** – Александр Крайник и Магомед Гамзаев: сценарная стратегия, общий модуль ЕБС, интеграция МФО за 2 недели.
- **ЦБТ (Центр биометрических технологий)** – Владислав Поволоцкий, Владислав Святик, Евгений Семёнов: 100 млн биометрических оплат за полугодие, 400 тыс. счетов без случаев мошенничества.
- **«АльфаСтрахование»** – Владимир Скворцов: киберполис как элемент архитектуры защиты, кейс ущерба 100 млн руб.
- **«Ренессанс страхование»** – Андрей Турунов: рост аудитории цифровых каналов втрое, ответственность человека перед клиентом.
- **«МигКредит»** – Александр Пустовит: экономика подключения к ЕБС, оборудование около 50 млн руб.
- **Минцифры России** – Татьяна Скворцова: ГИС «Антифрод», консолидированная ответственность, подключение более 120 участников.
- **«Лаборатория Касперского»** – Антон Иванов: инсайдеры в финсекторе, рост спроса на биометрически верифицированные аккаунты.
- **Билайн** – Максим Кабрера: критика каскадной модели ответственности, страховка от мошенничества для абонентов.

Выводы

- Финансовые платформы вышли на устойчивый оборот – 120 млрд руб. сделок в квартал и около 1,2 трлн руб. с начала действия закона, – и к ним подключаются уже не только региональные, но и крупные банки (Алешина Кристина, Банк России).
- Платформы готовятся стать протоколом для ИИ-агентов, но правил агентных сделок нет: рынок просит Банк России описать цепочку «клиент – ИИ-агент – финансовая организация», подтверждение распоряжений человеком и реестр доверенных агентов (Алутин Игорь, Московская биржа; Крайник Александр, «Сравни»).
- Эффект ИИ банки считают в рублях, но оценки расходятся: в Банке «Санкт-Петербург» более 130 проектов и эффект втрое выше инвестиций (Кутузов Станислав, Банк «Санкт-Петербург»), тогда как Т-Банк не видит значимого сквозного прироста от массового ИИ-кодинга (Маслов Игорь, Т-Банк).
- Решения с риском для клиента оставляют человеку: агенту поручают сбор данных и рутину, а изменение условий кредита и ответственность перед клиентом остаются за сотрудником (Никишов Дмитрий, Банк ДОМ.РФ; Турунов Андрей, «Ренессанс страхование»).

- Биометрическая оплата стала массовой: порядка 100 млн оплат за первое полугодие 2026 года (Святик Владислав, ЦБТ), в Сбере 0 успешных атак при 27,5 млн транзакций (Евсеев Олег, Сбер); полного покрытия финансово активного населения ЦБТ ждёт за 1–2 года (Поволоцкий Владислав, ЦБТ).
- Главный барьер для небанковского сектора – стоимость подключения к ЕБС: оборудование для прямого подключения оценивается примерно в 50 млн руб., делегированные решения дешевле примерно на треть (Пустовит Александр, «МигКредит»).
- Борьба с мошенничеством становится обязательной и общей: с 1 марта 2027 года подключение к ГИС «Антифрод» обязательно (Скворцова Татьяна, Минцифры России), при этом операторы связи оспаривают распределение ответственности (Кабрера Максим, Билайн), а киберстрахование встраивается в архитектуру защиты (Скворцов Владимир, «АльфаСтрахование»).

Источники

- Сессия «ИИ-агенты под контролем: как управлять рисками и строить доверенную инфраструктуру», Форум «Цифровые решения – 2026»
- Сессия «Эффекты применения ИИ в системах управления ресурсами: метрики, кейсы, масштабирование», Форум «Цифровые решения – 2026»
- Сессия «От ускорителя к ИИ-сервису: как сделать корпоративную ИИ-инфраструктуру управляемой», Форум «Цифровые решения – 2026»
- Сессия «Защита малого и среднего бизнеса от атакующего ИИ», Форум «Цифровые решения – 2026»
- Сессия «Роль финансовых платформ в инфраструктуре финансового рынка», Форум «Цифровые решения – 2026»
- Сессия «Государственные данные для цифровых платформ», Форум «Цифровые решения – 2026»
- Сессия «Доступ разрешен: повышение эффективности ИИ-агентной экономики и новые стандарты ПО», Форум «Цифровые решения – 2026»
- Сессия «Неотех-платформы: сближение корпоративного и розничного цифрового опыта», Форум «Цифровые решения – 2026»
- Сессия «От цифровой идентификации к цифровому доверию. Как государству и бизнесу выстроить единый контур», Форум «Цифровые решения – 2026»
- Сессия «ЕБС в финансах: как снизить издержки на комплаенс и защитить клиентов от мошенничества», Форум «Цифровые решения – 2026»
- Сессия «Конференция билайн. Каждый контакт имеет значение», Форум «Цифровые решения – 2026»
- Сессия «Маршрут построен: „дорожная карта“ цифровизации пассажирского транспорта в России», Форум «Цифровые решения – 2026»

- Сессия «Суверенный ИИ: сколько независимости нужно заказчику», Форум «Цифровые решения – 2026»
- Сессия «ЦОД 2.0: энергия, регулирование, региональная стратегия», Форум «Цифровые решения – 2026»
- Сессия «Инновации нон стоп: как внедрять технологии на непрерывном производстве», Форум «Цифровые решения – 2026»
- Сессия «Пленарная сессия. Кибербезопасность сегодня: когда защита перестает быть надстройкой», Форум «Цифровые решения – 2026»
- Сессия «Кибербезопасность в эпоху платформенной экономики», Форум «Цифровые решения – 2026»
- Сессия «На шаг впереди: переход от реагирования к предупреждению угроз», Форум «Цифровые решения – 2026»
- Сессия «Доверие и безопасность в цифровой торговле: технологии, стандарты и защита участников рынка», Форум «Цифровые решения – 2026»
- Сессия «Периметр больше не спасает: почему фокус отрасли смещается в сторону защиты данных», Форум «Цифровые решения – 2026»
- Сессия «Доверенная генеративная разработка: единые правила для отрасли», Форум «Цифровые решения – 2026»
- Сессия «Развитие системы противодействия киберпреступлениям: меры, координация и измеримые эффекты», Форум «Цифровые решения – 2026»
- Сессия «Кибербезопасность и биометрия: в поисках идеального баланса», Форум «Цифровые решения – 2026»