

#ПЛАС

ПЛАТЕЖИ. СИСТЕМЫ. КАРТОЧКИ

PAYMENTS
& CASH
CIRCULATION
International PLUS-Forum



uniTodi Собственная
разработка – от идеи до продукта

 Life Pulse S10 F*

Смарт-терминал 3-в-1 от Life Pay



Включён в реестр Минпромторга.
Разработан и произведён в России
для банков и корпораций.

*Лайф Пульс



life-pay.ru

#ПЛАС

ПЛАТЕЖНЫЙ
БИЗНЕС
и НДО
Международный ПЛАС-Форум

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

ПЛАС №07-08 (339-340)*2026

PLUSWORLD.RU

Колонка редактора

2 Конец лета: полномасштабный ЦР, легализация криптобизнеса, господдержка ИИ, антимошенническая доктрина. Что скажут на ПЛАС-Форуме?

След в истории

6 Пеле, King of Football, — журналу «ПЛАС»: «В первую очередь я заботился о том, чтобы спорт вошел в жизнь беднейшей части бразильцев»

Cover Story

12 uniTodi. Собственная разработка – от идеи до продукта

Госрегулирование

18 Станислав Кузнецов, Сбер: «Кибербезопасность становится ключевым конкурентным преимуществом»
Интервью Станислава Кузнецова, заместителя председателя Правления Сбербанка, для спецвыпуска журнала «ПЛАС».

Маркетплейсы

22 Какого цвета будущее: синее, зеленое или красное? АДМ для ПВЗ: как превратить пункт выдачи заказов в точку роста клиентской базы банка?

Финтех

26 ART Fintech: «Строим платформу, где бизнес сам красит забор, и считаем это стратегическим партнерством»

Платежный бизнес

30 Зачем России свой платежный терминал
В декабре 2025 года терминал LIFE PULSE вошел в реестр контрольно-кассовой техники ФНС.

Безопасность

34 Платежная инфраструктура больше не принадлежит только банкам: как управлять всей цепочкой платежа
Аркадий Прокудин, коммерческий директор международной консалтинговой группы Compliance Control & Rakasta, о Вселенной безопасных платежей.

Венчурный капитал

48 Венчур и таланты – главный капитал 21 века. Почему Узбекистану нужно спешить
Беседуем с основателем и управляющим партнером R136 Ventures, инвестором Кремниевой долины Виктором Орловским.

Криптобизнес

60 Использование стейблкоинов для трансграничных B2B-платежей резко возросло



С полным содержанием данного номера журнала вы сможете знакомиться в электронной версии номера по адресу <https://plusworld.ru/journal/2026/plus-7-8-339-340-2026/>



6



30



34



48



60

Конец лета: полномасштабный ЦР, легализация криптобизнеса, господдержка ИИ, антимошенническая доктрина.

Что скажут на ПЛАС-Форуме?



Если анализировать главные события конца лета 2026 года, то одним из них является сам спецномер журнала «ПЛАС», который вы держите в руках. Это печатная версия нашего издания, к которой мы решили вернуться в эпоху искусственного интеллекта.

Как известно, журнал «ПЛАС» является ведущим профессиональным медиа, посвященным вопросам финансового обслуживания населения, банковской розницы, финтеха, платежной индустрии, криптобизнеса и государственных цифровых сервисов. Вот уже 32 года мы помогаем читателям быть в курсе главных тенденций на российском рынке, в мире, и особенно — в странах ЕАЭС, СНГ и других перспективных для бизнеса регионах, например, на рынках Евразийского континента. При этом на протяжении всей своей истории наше издание совершенствовало не только дизайн и контент, но и сам форм-фактор, несколько лет назад став полностью цифровым. В этом году мы впервые решили параллельно задействовать офлайновый подход.

Выпущенный в физическом формате, текущий номер нацелен на максимально эффективный таргетированный охват читательской аудитории с использованием всех возможностей, которые предоставляет офлайн в наш цифровой век.

Тираж будет распространяться в том числе 8–9 сентября среди участников еще одного близящегося крупного события — **Международного ПЛАС-Форума «Платежный бизнес и денежное обращение 2026»**.

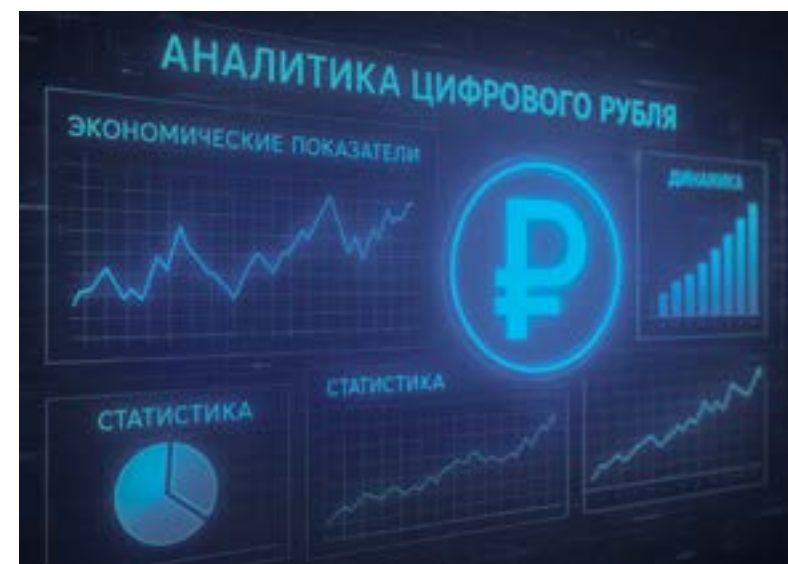
А теперь перейдем к ключевым событиям рынка, которых к концу лета традиционно много.

Сразу оговоримся, что в рамках нашей колонки мы не будем рассматривать ситуацию с Wildberries, безусловно, заслуживающую отдельного внимания, несмотря на свой сугубо геополитический характер. Отметим лишь, что происходящее повлияло не столько на расстановку сил на рынке электронной коммерции, сколько на подход его участников к оценке рисков. На этом фоне сегодня селлеры распределяют свои запасы товара между Wildberries, Ozon, независимыми складами и дополнительными каналами продаж, а не держат их, как еще недавно, внутри какой-либо одной площадки. Последнее стало слишком рискованным.

Кроме того, значительные складские мощности, которые, по нашей информации, должны войти в единый контур с уже существующими российскими складами Wildberries, созданы в Казахстане. Ожидается, что это в значительной степени ускорит обработку и доставку товарных потоков, направленных на потребителей в РФ.

Как отметил по этому поводу **Михаил Галузин**, заместитель министра иностранных дел РФ, «мы знаем, что на Ozon, Wildberries зарегистрированы уже сотни тысяч казахстанских поставщиков».

Еще один интересный факт — в последнее время наши новостные ресурсы отмечают резкое ускорение выполнения онлайн-заказов, осуществляемых, в частности, узбекскими потребителями: с 2–3 недель до двух-трех дней. В частности, также компания Wildberries открыла в Ташкенте один из крупнейших логистических центров в Центральной Азии, способный обрабатывать до 500 тыс. заказов в сутки. На этом фоне упомянутые склады следует рассматривать как лишь одну из составляющих масштабной складской системы Wildberries



в Евразии. В то же время, как отмечают эксперты, действующий в регионе складской фонд уже работает на пределе возможностей.

Этот вопрос наряду с другими будет рассматриваться в том числе на **Международном ПЛАС-Форуме Digital Uzbekistan в Ташкенте 26–27 мая 2027 года**.

Цифровой рубль — счета в комбанках?

Полномасштабный запуск проекта цифрового рубля с 1 сентября является, вероятно, самым ожидаемым рынком событием — хотя далеко не все ожидают его с легким сердцем. В первую очередь интересуют возможные сценарии развития, такие как возможность создания соответствующих смарт-контрактов для юридических лиц, эксперимент оплаты ЦР в офлайне, а также заявление НСПК о планах присоединения к проекту.

По словам **Виталия Копысова**, амбассадора проекта цифрового рубля, ЦБ РФ уже объявил, что Банк России планирует по пути исследования международного опыта CBDC и в качестве эксперимента разрешить провести открытие цифровых счетов ЦР непосредственно на балансе финансовых посредников.

Антимошенническая доктрина — обсуждаем и развиваем?

В конце июля на публичное обсуждение был представлен весьма актуальный документ — проект Указа Президента Российской Федерации «Об утверждении Доктрины развития системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий».

Доктрина определяет комплексную стратегию развития системы борьбы с правонарушениями, совершаемыми с использованием информационно-коммуникационных технологий (ИКТ), на среднесрочный и долгосрочный период (до 2035 года). Реализация разделена на три этапа: первый (2027–2028 гг.), второй (2029–2030 гг.) и третий (2031–2035 гг.).

По мнению независимого эксперта **Николая Пятизбланцева**, доктрина интересна в первую очередь тем, что представляет собой не набор разрозненных мер, а логичную и комплексную стратегию системной трансформации. Ее реализация имеет высокий потенциал для повышения эффективности борьбы с ИКТ-преступлениями. Однако успех будет зависеть от качества исполнения, преодоления межведомственных барьеров, достаточного финансирования и способности системы адаптироваться к эволюции угроз.

Крипта в законе? Или еще не совсем?

21 июля Госдума РФ приняла сразу во втором и третьем чтениях законопроект о регулировании криптовалют в России, по сути, впервые легализовав отечественную криптоиндустрию. Основные положения закона должны заработать уже с 1 сентября.

Документ признает цифровые валюты имуществом, вводит общие требования к их обороту и предусматривает судебную защиту прав на криптовалюту независимо от ее предварительного декларирования. Согласно ему, операции будут проходить через лицензированных ЦБ посредников, а их объем для частных инвесторов будет ограничен. Россияне получат возможность легально инвестировать в криптовалюты на российских биржах и пользоваться услугами брокеров, доверительных управляющих и управляющих компаний, а также крипто-обменников при совершении сделок и операций с ними.

При этом оплачивать товары и услуги криптовалютой будет по-прежнему запрещено.

Участники рынка отнеслись к данному крайне ожидаемому ими событию неоднозначно. Так, **Максим Боков**, главный аналитик AML/KYT оператора «Шард», считает, что принятый закон формирует компромиссную модель легализации рынка цифровых активов. С одной стороны, регулятор отказывается от полного запрета криптовалют, а с другой — выстраивает инфраструктуру их обращения, близкую к традиционным финансовым институтам. По мнению эксперта, для государства и институциональных участников рынка такой подход является рациональным, особенно в контексте развития трансграничных расчетов и повышения управляемости финансовых потоков. Вместе с тем для розничных пользователей и DeFi-сектора это означает усиление регуляторной нагрузки и сокращение возможностей для свободного использования криптовалют, что может

спровоцировать переход части ликвидности в теневой сектор экономики.

В свою очередь **Олег Ушаков, исполнительный директор АРЦП**, уверен, что благодаря новому закону создается новая регулируемая инфраструктура для обращения цифровых активов (в широком смысле): «Участники ВЭД смогут использовать криптовалюту для трансграничных расчетов без ограничений (то есть не только в рамках экспериментального правового режима, как это предусмотрено в настоящее время). Резиденты смогут проводить операции с криптовалютой за рубежом, но без использования российской банковской инфраструктуры и находящегося в России имущества». Кроме того, подчеркивает эксперт, хотя документ не оперирует термином «стейблкоин», но вводит понятие «иностранных цифровых инструментов», которое покрывает собой любые криптоинструменты, выпущенные за рубежом, за исключением цифровых валют.

А вот **Ян Кривоносов**, директор Crypto Emergency, придерживается практически противоположного мнения, считая, что принимать такие законы в условиях жесточайших санкций нецелесообразно: «Это прямой путь к образованию «черного рынка» криптовалют. А люди однозначно будут пользоваться криптовалютами, потому что для многих нет другого варианта, к сожалению. Моряки, которые получают зарплату в USDT; айтишники, путешественники, которые пополняют свои карты через стейблкоины или берут с собой в поездку. Где они будут это покупать? Все это уйдет в зарубежный контур, никак не в российский. И те налоги, которые законодатели рассчитывали собирать, собрать не получится». «Будет ли отток капитала?» — задается вопросом эксперт. По его мнению, «будет, и с помощью криптовалют, и с помощью других инструментов. Ибо в РФ вся крипта будет санкционная. И риск блокировок прямо на кошельках у таких компаний и бирж или у тех компаний, которые купили и были связаны с этими кошельками и с этой криптовалютой, без преувеличения огромен».

Как отмечает финансовый эксперт и предприниматель **Александр Винник**, законопроект оставляет нерешенными много вопросов, которые, видимо, будут прорабатывать в будущем. В нем не описано, что именно считать иностранным кошельком, как считать налоговую базу, какие активы попадут в белый список. «По формальным критериям даже популярные стейблкоины, такие как USDT, не подходят для публичных торгов, и их статус отдельно определяют уже осенью. Такая рамка лучше правового вакуума, но работы предстоит еще много», — считает эксперт.



Возвращаясь к мнению **Виталия Копысова**, принятый закон стоит рассматривать как попытку в первом приближении наконец-то упорядочить некоторые уже существующие схемы расчетов в криптовалютах и попытаться все это перевести в правовые рамки. А поскольку

закон носит рамочный характер и ссылается на пока не существующие подзаконные акты, однозначно судить о его эффективности еще рано.

Так или иначе, до 1 июля 2027 года у участников рынка будет время привести свою деятельность в соответствие с законом, далее будем следить за правоприменительной практикой и общим развитием ситуации и посмотрим, как будет выглядеть криптоиндустрия в легализованном виде.

Закон о поддержке ИИ — не все однозначно?

Помимо полномасштабного старта цифрового рубля, с 1 сентября 2026 года вступает в силу Федеральный закон № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации».

Согласно закону, основной массив норм вступает в силу с 1 сентября 2026 года. Отдельные положения — о требованиях к моделям, маркировке, использовании интеллектуальной деятельности — с 1 марта 2027 года. Для уже работающих систем предусмотрен переходный период до 1 сентября 2032 года при условии хранения данных в России. Почти шесть лет на адаптацию —

достаточный срок, но достаточно ли его для создания конкурентоспособных моделей?

Как отмечает **Тимур Аитов**, председатель комиссии по безопасности финансового рынка ТПП РФ, закон содержит ряд противоречий с другими законодательными документами. Так, если «Антифрод 3.0» примут в текущей жесткой версии, банки окажутся между двух огней: ИИ-закон требует от них внедрения интеллектуальных систем, а антифрод-закон запрещает им доверять этим системам в ключевой операции — решении о блокировке. Это не просто разнонаправленное регулирование, это настоящий регуляторный нож, бьющий по работающим ИИ-системам.

Напомним, что отдельно в прошлом году озвучена инициатива Роскомнадзора: заменить индивидуальные согласия на обработку персональных данных отраслевыми стандартами. Это может ограничить сбор данных, необходимых для обучения ИИ. Пока это только предложение, но если и его оформят законодательно, разработчики потеряют доступ к ключевым массивам. Баланс между защитой данных и развитием ИИ в России пока отчетливо не просматривается.

Как прокомментировал советник генерального директора АФТ **Алексей Войлуков**, как и закон, легализующий криптобизнес, 243-ФЗ носит достаточно «верхнеуровневый», рамочный характер, устанавливая определенные понятия, категории, рамки, но при этом не вводя никаких конкретных жестких требований. Отчасти такой подход оправдан — определенные конкурентные преимущества у России по сравнению с другими странами мира в сфере ИИ имеются, однако существуют и признанные мировые лидеры, которых необходимо стремиться догонять и, по возможности, даже обгонять. На этом фоне чрезмерное регулирование в области ИИ могло бы оказать значительное негативное влияние на развитие данной технологии.

С другой стороны, очень важно ввести данное направление в четкое законодательное поле с возможностью контроля всех имеющихся рисков. А самое главное — чтобы в России создавались собственные ИИ-модели,

а не бездумно использовались некие западные разработки, что не только неэффективно, но и крайне рискованно.

На взгляд редакции журнала «ПЛАС», возможны два сценария. Первый, оптимистический: подзаконные акты пропишут понятные и необременительные правила, доступ к данным станет реальным, а малый бизнес получит субсидии на аренду мощностей — тогда закон станет настоящим драйвером. Второй, пессимистический: все утонет в бюрократии, фильтр «традиционных ценностей» станет инструментом выборочного давления, а господдержка осядет в госкорпорациях. В каком из этих миров мы проснемся 1 сентября 2026-го — зависит от того, кто именно будет писать подзаконные акты.

Сентябрьский ПЛАС-Форум — ждем реальную реакцию рынка на госинициативы?

Все эти тренды и прогнозы будут совместно обсуждаться многочисленными участниками масштабного события — **Международного ПЛАС-Форума «Платежный бизнес и денежное обращение 2026»**.

Что в действительности ожидает рынок от новых законов и нацпроектов, станет понятно только после того, как своим мнением о новых регуляторных инициативах поделятся 3000+ представителей банковского сектора, платежных систем, операторов связи, регуляторов и поставщиков решений. Среди них — руководители Сбербанка, ПСБ, ВТБ, Альфа-Банка, Ozon Банка, ВЭБ.РФ и других ведущих структур, а также представители ЦБ РФ, НСПК, Минцифры.

Ожидается, что всего через неделю после 1 сентября многое станет понятнее, а векторы развития тех или иных инициатив — более четкими и прозрачными. Поэтому сентябрьский ПЛАС-Форум этого года обещает стать одним из интереснейших в истории мероприятия! ПЛАС

Ждем вас в Москве 8–9 сентября в «Рэдиссон Славянская»!

Глава Резервного банка Индии призывает индийские банки взять под контроль использование ИИ

Банковский сектор Индии должен проявлять инициативу в части внедрения ИИ и самостоятельно определять, как эта технология влияет на преобразование отрасли, не позволяя ей диктовать неизбежные изменения.

Такое предупреждение сделал глава Резервного банка Индии (Reserve Bank of India, RBI) Санджай Малхотра (Sanjay Malhotra). Выступая на конференции в Индии, он призвал банки рассматривать ИИ как трансформационную технологию, а не просто еще один цифровой инструмент. В результате банкам придется переосмыслить ряд фундаментальных процессов и задач, от управления рисками до распределения капитала и обслуживания клиентов.

«Единственный вопрос, стоящий перед нами сейчас, — это будете ли вы сами формировать путь развития ИИ или позволите ему по умолчанию формировать вас», — заявил С. Малхотра. Он назвал государственную цифровую инфраструктуру Индии надежной основой для будущего развития ИИ, на базе которой банки и другие поставщики финансовых услуг могут разрабатывать новые решения на основе искусственного интеллекта. С. Малхотра также подчеркнул, что одной из областей, где ИИ может оказать существенное влияние на тенденции занятости, является разработка программного обеспечения.

Пеле, King of Football, – журналу «ПЛАС»: «В первую очередь я заботился о том, чтобы спорт вошел в жизнь беднейшей части бразильцев»

Четыре с половиной года назад, 29 декабря 2022 года, от нас ушел Эдсон Арантис ду Насименту (Edson Arantes do Nascimento), известный всему миру как «Пеле (Pele) – 1000 голов». Легендарный бразильский футболист, игравший за клубы «Сантос» и «Нью-Йорк Космос», провел 92 матча и забил 77 голов в составе сборной Бразилии. Трехкратный чемпион мира умер в возрасте 82 лет. Мало кто знает, но свыше четверти века назад, накануне финального матча чемпионата EURO 2000, он дал эксклюзивное интервью нашему издателю Александру Ивановичу Гризову.

Интервью с King of Football – истинное счастье для любого журналиста. Пеле и Александр Гризов



Футбольный матч состоялся 2 июля 2000 года в Роттердаме на стадионе «Фейеноорд» (также известный как «Де Куйп») между сборными Франции и Италии. Матч завершился со счетом 2:1 в пользу французской сборной. В результате сборная Франции стала двукратным чемпионом Европы.

В силу различных обстоятельств это интервью увидело свет только сейчас, в завершение чемпионата мира по футболу 2026. Как вы сможете убедиться, Пеле открывается в нем с совсем другой стороны, представляя, кроме всего прочего, еще и неизвестной большинству из нас крупной и многосторонней политической фигурой. King of Football действительно очень много сделал для народа Бразилии, особенно для ее молодежи. А его дружба с Нельсоном Манделой легла в основу выбора ЮАР в качестве страны проведения чемпионата мира по футболу в 2010 году.



«Мои друзья, которые помогли организовать это интервью с Пеле» – Александр Гризов.

Эти же отношения в итоге стали одной из точек опоры, благодаря которым выбор был сделан в пользу того, чтобы вторые в истории Олимпийские игры в Латинской Америке прошли в 2016 году в Бразилии.

А. Гризов: Прежде всего прошу прощения за то, что беспокою вас накануне финального матча чемпионата EURO 2000!

Пеле: Ничего страшного, господин Гризов, это вы извините меня – сами видите, все на стадионе сегодня стремятся поговорить со мной и что-то обсудить, поэтому иногда буду отвлекаться от нашей с вами беседы!

А. Гризов: Да, только оказавшись в такой ситуации, можно понять, как трудно нести титул King of Football даже в 2000 году.

Пеле: Вы, конечно же, понимаете, насколько это важно. Очевидно, что люди рады узнавать некоего своего кумира и, в ответ, хотят быть им узнаны. Просто в моем случае – это именно футбол. Люди делают все, что в их силах, чтобы посетить такого рода события, как финальные матчи. Их нужно уважать за эту любовь к футболу. Но сегодня это вдвойне важно, поскольку все происходит не столько на футбольном поле, сколько в нашей повседневной жизни.

Я благодарен Богу за свою замечательную жизнь!

Как многие помнят, после официального завершения футбольной карьеры Пеле успешно проявил себя в качестве главы Министерства спорта Бразилии (который сам Пеле в интервью назвал Министерством Бразилии по делам спорта и молодежи. – Ред.), а также послом футбола во всем мире, в том числе Амбассадором платежной системы MasterCard. Футбольный гений многократно посещал СССР и, впоследствии, Россию.

Как близкие люди, так и поклонники по всему миру отмечали его полную свободу от каких-либо материальных привязанностей, что редкость для знаменитостей нашего времени. Так, например, проведенный Пеле аукцион, в ходе которого он выставил на торги свои многочисленные спортивные трофеи, принес почти 4,5 млн евро, причем львиная доля этой суммы была направлена бенефициаром на благотворительность.

Именно поэтому лучшей эпитафией, если это статичное слово вообще может быть применимо к вечно живой футбольной легенде, представляется не длинный перечень рекордов и заслуг, но простые слова самого Пеле: «Я счастливый человек. Я рад, что оставил о себе память, рад, что меня знают. Конечно, я благодарен Богу за то, что он мне дал такую замечательную жизнь».

А. Гризов: Вы могли бы поделиться вашей точкой зрения на профессиональный футбол как на бизнес? Каково состояние этого популярнейшего вида спорта в самом конце 20-го столетия, его перспективы? Ваше мнение – а остается ли футбол спортом номер один?

Пеле: Я постараюсь ответить на ваш вопрос, хотя это, безусловно, весьма непростая задача. Во-первых, если посмотреть на футбол как на бизнес, мы придем с вами к весьма неожиданным выводам. Несколько десятков лет



Один из интереснейших моментов финального матча EURO 2000 между Францией и Италией, который завершился голом.

назад, когда я играл на поле, телевидение еще не было столь массовым и всепроникающим, особенно если сравнивать с нынешними возможностями информационных технологий. Не было кабельного телевидения, не было платного TV, не было всеобъемлющей коммерциализации... Именно поэтому ситуация вокруг футбола была несколько иной.

С другой стороны, если смотреть на спорт как на возможность отдохнуть, развлечься, – футбол не только был, но и сейчас, безо всякого сомнения, является величайшим видом спорта. Тем более что сегодня у телевизионных



Настоящую бурю эмоций на только что хранящих спокойствие трибунах вызвал второй гол в ворота сборной Италии, взорвавший стадион.

компаний и международных информационных структур практически полностью закрыты любые технологические проблемы. Именно поэтому футбол и стал исключительно важной областью профессионального спорта и мирового бизнеса.

Например, у нас в Бразилии на матчах порой происходят настоящие столкновения между болельщиками, притом что на футбольном поле бразильцам нет равных. Однако за пределами футбольного поля бразильцам, на мой взгляд, не хватает профессионализма, организованности. Со своей стороны, я убежден, что бразильская экономика получит новый импульс развития, если в наш спорт придет новый человек, настоящий профессионал в области спорта, это очень важно для бизнеса.

А. Гризов: Если мы коснулись Бразилии, логично возникает вопрос: каким был ваш личный вклад в спортивный бизнес страны, и насколько велика роль современного футбола в национальной экономике и сегодняшней жизни Бразилии?

Пеле: Вы абсолютно правы. До апреля 1998 года я был министром спорта Бразилии. На этом посту я попытался сделать все зависящее от меня, чтобы превратить спорт в национальное достояние всего народа Бразилии. И в первую очередь я заботился о том, чтобы спорт вошел в жизнь беднейшей части бразильцев. Я уверен, что настоящий спорт организует и дисциплинирует молодежь. Спорт несет с собой истинные ценности. Футбол уводит детей-подростков от употребления наркотиков, уличной преступности и секс-индустрии. (Как добавил Пеле, каждый мальчишка, который увлекся футболом в Бразилии, – это минус один наркодилер на ее улицах, а приятельница этого новоиспеченного футболиста – минус одна жертва проституции. – Ред.)

«Практически любой финал любого крупного чемпионата – это эмоциональная драма, а для проигравших – супертрагедия»

В финале чемпионата Европы 2000 года сборная Франции одержала победу над Италией в тяжелой борьбе. На 55-й минуте счет открыл итальянский полузащитник Марко Дельвеккио. И сборная Италии вела в счете до самого конца основного времени. На последней компенсированной минуте второго тайма французский защитник Сильвен Вильтор забил ответный мяч и перевел игру в дополнительное время. В овертайме, который игрался до первого забитого мяча, победный «золотой гол» на 103-й минуте забил Давид Трезеге. Таким образом, Франция стала двукратным чемпионом Европы, а этот матч вошел в историю как один из самых драматичных в истории футбола.

Комментирует **А. Гризов:** «Практически любой финал любого крупного чемпионата – это эмоциональная драма, а для проигравших – супертрагедия. Мне повезло, что я сидел в итальянском секторе. Итальянцы забивали первый гол в этом матче в первом тайме. Как они отплясывали, как веселились и радовались, будучи абсолютно уверенными, что победят и разгромят соперников! Да-да, это была заявка на победу. Игра стала еще более интересной и агрессивной с их стороны. Тем более, все понимали, что итальянцы – это супергорячая кровь. И вдруг во втором тайме в их ворота влетает первый «шарик» от французов. Я видел, как итальянцы и итальянки, которые только что отплясывали, сидя вокруг меня, теперь рыдали – не плакали, а именно рыдали в голос... Но когда в их ворота влетел второй мяч, настала тишина. Гробовая. Да, гробовая. Почему? Потому что итог оказался очевидным. Сознаю, когда я иду на интересный фильм, то не только смотрю на экран, но и наблюдаю за реакцией зала. А реакция в этот раз на стадионе была просто штормовая, как весы, сначала взлеты, потом полный крах у итальянцев, и веселье началось уже во французском секторе. Это было незабываемо! Настоящую бурю эмоций вызывали не только события на футбольном поле EURO 2000, но и та трагедия, которая взорвала итальянский сектор после второго гола, а потом перекинулась волной восторга на французских болельщиков, охватила все трибуны стадиона».



Руководители ста лучших банков Eurocard были приглашены платежной системой на финал EURO 2000. И все они сочли необходимым воспользоваться шансом лично поприветствовать легендарного Пеле, выстроившись в длинную очередь.

Проанализировав всю ситуацию целиком, мы получаем очень интересную картину. Если правительство действительно «в национальном масштабе» реализует программу по вовлечению молодежи и детей в спорт – мы решим исключительно важные задачи. В этом случае молодежь занимается интересным делом. А мы организуем молодых людей, ведь спорт и дисциплина неразделимы. Как минимум мы решаем задачу дисциплинализации общества. Снижаем расходы на содержание полицейского аппарата и борьбу с криминалом. При этом помимо социальных решаются и экономические задачи. И это на самом деле очень важно! Я неоднократно обсуждал эту проблему с президентом Бразилии господином Фернандо Энрике: «Господин президент, вы должны уделять больше внимания спорту и его базе. Вам следует больше внимания уделять обществу. Необходимо создавать условия для появления нового поколения бразильской молодежи!».

Именно в этом я вижу свой основной вклад в развитие спорта в Бразилии. И именно эту задачу я пытаюсь решить в первую очередь в моей стране.

А. Гризов: Огромное спасибо за интересную и глубокую позицию в вопросе развития спорта в Бразилии. А насколько, по вашему мнению, взаимосвязаны профессионализм менеджмента футбольных команд с уровнем их игры? Ваша оценка европейского футбола в сравнении с латиноамериканским. Как вы видите основные тенденции развития?

Пеле: Во-первых, организация всего чемпионата EURO 2000 и каждого его матча в отдельности отличается очень высоким общим уровнем и квалификацией. В целом организация любых спортивных мероприятий в Европе гораздо более профессиональна по сравнению с тем, что делается в Латинской Америке или Африке, даже в ЮАР.

Кроме того, у нас недостаточно денег, чтобы платить необходимую зарплату нашим футболистам. Их судьба примерно одинакова, каждый интересный спортсмен, как только начинает показывать результаты на поле, тут же оказывается в Европе. Мне просто стыдно, господа! Причем этот процесс касается не только Бразилии, но и Аргентины и Уругвая. Практически каждый большой игрок из Латинской Америки принадлежит тому или иному европейскому клубу. Просто потому, что мы не можем позволить себе платить такие суммы собственным футболистам. В-третьих, проведение крупных спортивных мероприятий в Европе имеет многолетние традиции. Чемпионат EURO 2000 – яркое тому подтверждение. По моему мнению, по крайней мере уровень организации проведения чемпионата EURO 2000 не просто хороший или отличный, а без преувеличения фантастический. Да, это моя независимая личная оценка. С другой стороны, кто как не я видел или принимал участие в достаточном количестве футбольных мероприятий, чтобы быть объективным?

А. Гризов: Благодарю вас за искренность! Ваше мнение, кто победит в финальном матче Франция – Италия? И каким будет счет? Извините за дурацкий вопрос.

Пеле (смеется): Нет-нет, все очень правильно! Просто, если вы задумаетесь над игрой команд Голландии и Италии (они играли в полуфинале EURO 2000, победителя определили только в серии пенальти: сборная Нидерландов реализовала только один пенальти против трех итальянских. – Ред.), то поймете, что предсказывать что-либо в спорте невозможно.

Пеле выступает перед представителями ста лучших банков Eurocard.





Бары Амстердама во время проведения EURO 2000 выглядели особенно привлекательно.

А. Гризов: Полностью согласен!

Пеле: Поэтому, если посмотреть с исторической точки зрения на эту игру, можно вполне определенно заявить: никто не способен был поверить, что Италия выиграет этот матч. А если вспомнить предстоящую игру, можно лишь заявить, что Франция, скорее всего, будет нападать, а Италия, скорее всего, будет защищаться. Но кто знает, что произойдет в ходе матча?

А. Гризов: Кто?! Вы!

Пеле (смеется): Это будет жестокая игра. И у Франции не будет больше другой такой возможности выиграть. Но предсказывать результаты финального матча EURO 2000 – это то же самое, что предсказывать результаты выбора той или иной страны или Кубка мира 2006. Кстати, у Африки никогда не было возможности провести Кубок мира в одной из своих стран. А проведение в Африке такого масштабного события могло бы дать очень многое. Именно для спорта, да и для всего африканского общества в целом. Здесь я имею в виду чистый спорт, а не бизнес в спорте. Именно поэтому в свое время я встречался с президентом ЮАР господином Нельсоном Манделой. Я заявил ему: «Послушайте, мы поддержим вас сейчас в вопросе выбора страны проведения Кубка мира в 2006 году, а вы поддержите кандидатуру Бразилии при голосовании по кандидатуре страны – организатора Кубка в 2010-м!»

Думаю, я достаточно подробно рассказал об основных направлениях внутренних и внешнеполитических событий, в которых я принимаю непосредственное участие. Однако, если мы будем говорить с точки зрения безопасности, организации и инфраструктуры, в этом случае есть смысл обратить внимание на Англию и Германию. Эти страны-кандидаты подготовлены как нельзя лучше.

А. Гризов: Не напишете ли несколько слов российским болельщикам, которые знают вас очень хорошо и прекрасно помнят вашу игру?

Пеле: С удовольствием! Я напишу им: «Моим друзьям я желаю всего наилучшего! Пеле»

А. Гризов: Благодарю вас!

Пеле: В прошлом году я был в Москве. Думаю, вы слышали, что в Москве появилось кофе Café Peli?

А. Гризов: Конечно!

Пеле: Я планирую приехать в российскую столицу в ноябре 2000 года!

Возможно, мой партнер, компания, которая непосредственно занимается продвижением Café Peli, захочет, чтобы я посетил Москву, и мы там увидимся. Mastercard должна пригласить вас встретиться со мной!

ПЛАС



Правоохранительные органы ЕС и Голландии приложили все силы для поддержания порядка в период EURO 2000. Тем не менее, хулиганам и вандалам удавалось громить бутики столицы и банкоматы.



Мяч с автографом самого Пеле – мечта любого футбольного болельщика!

Российскую делегацию от Eurocard на EURO 2000 представляли, в том числе, Андрей Королёв, тогдашний глава Московского офиса платежной системы, Андрей Погодин, ИТ-директор Сбербанка, Андрей Соболев, руководитель карточного направления Сбербанка, и Андрей Тарусов, исполнительный директор Eurocard. Представьте себе искреннее изумление Пеле, когда четвертый подряд пожавший ему руку россиянин назвался Андреем, как и три его предшественника. «А в России вообще есть другие имена?» – нашелся King of Football, считавшийся еще и королем остроумия.

«To my friends All the best» – автограф Пеле на бейдже Александра Гризова

Пеле – каким мы все его запомнили навсегда..



Еще раз Пеле посетит Москву в самом конце 2017 года в составе делегации звезд мирового футбола, приглашенных для участия в церемонии финальной жеребьевки ЧМ 2018. В тот раз спортсмены, в числе которых, помимо Пеле – Никита Симонян, Диего Марадона, Фабио Каннаваро, Карлес Пуйоль, Роналдо и Роналдиньо, смогли откровенно побеседовать с Владимиром Путиным.



Meeting Pelé... Priceless!



uniTodi. Собственная разработка — от идеи до продукта



Илья Галиуллин

Для покупателя оплата занимает несколько секунд. Для банка или ритейлера за этими секундами стоит сложная система: оборудование, программное обеспечение, безопасность, требования регуляторов и клиентский сервис. uniTodi работает со всей этой системой целиком — от архитектуры устройства и интеграции в инфраструктуру заказчика до дизайна интерфейса, звуков и анимации на экране.

uniTodi — бренд группы компаний PBF Group, которая работает на рынке платежного оборудования более 20 лет. За это время в России и странах СНГ было поставлено более миллиона терминалов. Накопленная экспертиза помогла хорошо понять рынок изнутри: как меняются требования банков и ритейла, какие решения выдерживают интенсивную эксплуатацию и чего не хватает заказчикам, когда стандартного оборудования уже недостаточно.

От поставок — к собственному продукту

Поворотным моментом для компании стал период пандемии. Рынок быстро менялся, международные цепочки поставок становились менее предсказуемыми, а запрос на технологическую независимость и локальные разработки усиливался. Тогда uniTodi приняла решение выйти за рамки классической дистрибуции и последовательно наращивать собственные компетенции — инженерные, программные и дизайнерские.

«За годы работы у нас сложилось сотрудничество с крупными международными вендорами ИТ-оборудования, — рассказывает Илья Галиуллин, генеральный директор uniTodi. — Но в период пандемии стало ясно, что рынку нужен собственный продукт, который можно развивать здесь, учитывать российские требования и адаптировать под задачи конкретного заказчика. Так



Терминал P8 BIO-F

появилась торговая марка uniTodi и начался новый этап компании».

Сегодня работа над устройством начинается задолго до сборочной линии. Инженеры участвуют в выборе ключевых комплектующих и оценивают их надежность, меняют архитектуру устройства под техническое задание, работают с драйверами и прошивками.

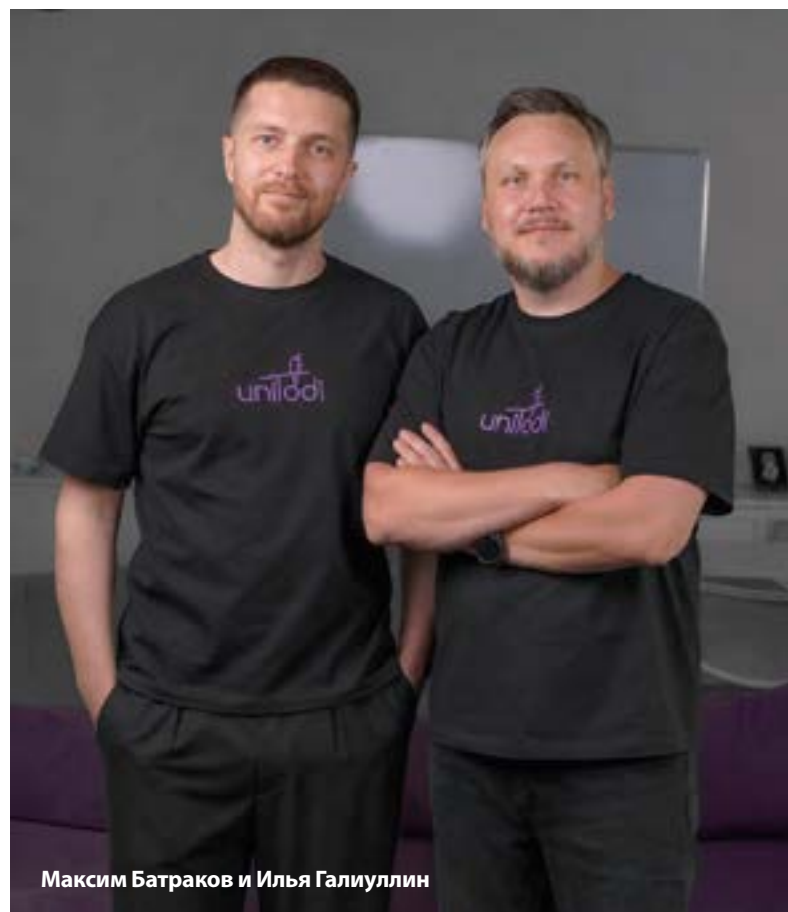
Программное обеспечение адаптируется к ИТ-ландшафту заказчика, а промышленные дизайнеры соотносят внешний вид будущего терминала с расположением компонентов, требованиями производства и реальными условиями эксплуатации. Собственная команда uniTodi в Китае сопровождает взаимодействие с производителями, а партнерские площадки собирают устройство по подготовленной документации и заданным параметрам.

Такой подход дает компании возможность создавать собственную линейку и одновременно разрабатывать кастомные решения совместно с банками, финтех-компаниями и ритейлом.

Речь может идти о новом форм-факторе, особой конфигурации оборудования, нестандартном сценарии оплаты или программном продукте, встроенном в инфраструктуру заказчика. Базовая платформа сокращает сроки запуска, но итоговое решение не ограничивается готовой «коробкой».



Терминал P8 BIO-F



Максим Батраков и Илья Галиуллин

тировать решения, готовые к следующим изменениям в эквайринге. Для этого нужна глубокая экспертиза — от инженерной архитектуры и программного обеспечения до промышленного дизайна и пользовательского сценария».

Флагманские модели **P8 BIO** и **P8 BIO-F** работают на Android и поддерживают разные способы оплаты: банковской картой, по QR-коду, с использованием биометрии и технологии «Волна». Устройство можно разместить в привычной кассовой зоне, при этом его возможности выходят далеко за рамки приема платежа. Корпус, интерфейс, звуковые уведомления и дополнительные сервисы адаптируются под бренд и бизнес-процессы заказчика.

Линейка uniTodi охватывает разные сценарии использования. В нее входят мобильные и стационарные терминалы, устройства с биометрией, модели с двумя экранами, кассы «три в одном», решения для касс самообслуживания и POS-системы для ритейла. Например, **K10** совмещает мобильность, большой дисплей и прием оплаты по биометрии; **MF919** и **X1** используют два экрана для раздельного отображения информации сотруднику и покупателю; **MF960** может работать как мобильное или стационарное устройство на Android или Linux. Модель **K10** уже получила более 150 тыс. установок в российских банках. Разнообразие форм-факторов позволяет подбирать решение под конкретную точку — от небольшого кафе до крупной торговой сети.

Терминал как часть бренда

Покупатель взаимодействует с платежным устройством всего несколько секунд, но именно в этот момент завершается покупка и формируется последнее впечатление о сервисе. uniTodi рассматривает терминал как полноценную часть клиентского опыта: он должен быть понятным,



Терминал P8 BIO

Локализация без технологического компромисса

Одно из ключевых направлений uniTodi — развитие российского платежного оборудования. В мае 2026 года в Минпромторге был зарегистрирован P8 BIO — первый терминал компании, производство которого организуется в России.

Следующим шагом стало развитие модели P8 BIO-F, объединяющей возможности платежного терминала и кассы «три в одном».

Для компании локализация означает не формальную замену страны сборки, а постепенный перенос компетенций: конструкторской документации, работы с компонентами, программным обеспечением, тестирования и дальнейшего развития продукта. При этом российское происхождение решения не должно ограничивать его технологичность. Напротив, новые модели создаются с учетом актуальных способов оплаты и требований рынка.

«Мы хотим развивать локальное производство на современной технологической базе, — говорит **Максим Батраков**, управляющий партнер uniTodi. — Важно не повторять уже существующие устройства, а проек-

быстрым и визуально связанным с брендом, которому принадлежит.

«Для нас важно создать платежный продукт, который отражает характер заказчика и при этом остается удобным для человека, — объясняет **Елена Низовская**, арт-директор uniTodi. — Терминал может быть сдержанным или ярким, минималистичным или необычным. Его цвет, материал, форма и интерфейс должны работать вместе. Тогда устройство не выглядит случайным предметом у кассы, а становится естественным продолжением бренда».

Брендинг начинается с корпуса: компания подбирает материалы и покрытия, работает с цветом, логотипом, подсветкой и деталями конструкции. Но внешний облик — только один уровень. Команда разрабатывает UI/UX платежного приложения, анимацию, звуковые сценарии и графику. Над проектами вместе работают специалисты по промышленному, графическому и интерфейсному дизайну, 3D, motion-, AI- и саунд-дизайну. Благодаря этому физическое устройство и цифровая среда воспринимаются как единый продукт.

Интерфейс также может учитывать контекст. На автозаправочной станции уместен один визуальный сценарий, в кофейне — другой, в премиальном магазине — третий. Экран успешной оплаты, анимация и предложение после покупки меняются в зависимости от места установки и задач бизнеса. Возможна персонализация контента с учетом характеристик аудитории, а также интеграция чаевых, программ лояльности, рекламных сообщений и дополнительных сервисов непосредственно в платежный сценарий.

Еще одно направление — геймификация. После оплаты пользователь может увидеть интерактивный сценарий, сыграть в короткую игру, получить бонус или персональное предложение. Цифровой маскот помогает сделать коммуникацию эмоциональнее, а привычное действие — запоминающимся. Для бизнеса это дополнительная точка



Елена Низовская

контакта с покупателем в момент, когда его внимание уже сосредоточено на экране.

Елена Низовская подчеркивает, что задача дизайнера здесь не в украшении технологии: «Любой эффект должен иметь смысл. Анимация помогает человеку понять статус операции, звук дает быструю обратную связь, персональное предложение продолжает сценарий покупки. Когда каждый элемент решает свою задачу, интерфейс становится живым, но не перегруженным».

Единый контур: оборудование, ПО и сопровождение

Запрос клиентов на работу «в одном окне» стал еще одной причиной, по которой uniTodi расширила собственную разработку. Банкам и ритейлерам важно получить не только устройство, но и программную среду, интеграцию, тестирование, мониторинг и дальнейшее сопровождение. Поэтому сегодня аппаратная и программная части развиваются параллельно.

Программные продукты uniTodi внесены в реестр российского ПО. Решения поддерживают российские



Терминал K10

Терминал P8 BIO



Терминал MF960

системы управления базами данных и аппаратные модули безопасности HSM, необходимые для защищенного взаимодействия терминалов с процессинговыми центрами.

Компания прошла сертификацию в распространенных платежных процессингах и адаптирует продукты под инфраструктуру разных заказчиков. Это позволяет внедрять единое приложение на устройствах нескольких вендоров и снижать зависимость бизнеса от конкретной модели оборудования.

Отдельное внимание уделяется качеству релизов и скорости реакции на инциденты. Автоматизированное тестирование помогает быстрее проверять обновления, а система мониторинга и дашборды дают команде сопровождения информацию о состоянии устройств и возникающих ошибках. По оценке компании, такой подход вдвое ускоряет выпуск стабильных релизов и примерно на 40% сокращает время реакции на обращения клиентов.

В мае 2026 года unitodi запустила собственное программное решение для кассы «три в одном», соответствующее требованиям 54-ФЗ. В одном устройстве объединяются прием оплаты, фискализация и учет товаров. Для малого бизнеса это возможность сократить количество оборудования на кассе и упростить запуск торговой точки, а для крупных сетей — стандартизировать инфраструктуру и управлять ею централизованно. Параллельно компания развивает решения для касс самообслуживания и POS-систем, усиливая присутствие не только в классическом эквайринге, но и в ритейле.

Технологические изменения в платежной индустрии происходят быстро, поэтому продукт должен быть готов к новым сценариям еще до того, как они станут массовыми. unitodi одной из первых на российском рынке реализовала прием оплаты по биометрии, цифровым рублем и технологии «Волна». При разработке команда отслеживает изменения законодательства и требования платежной отрасли, чтобы заказчик получал не экспериментальный прототип, а решение, готовое к промышленной эксплуатации.

«Наша задача — не просто следовать изменениям рынка, а заранее готовить продукты к новым требованиям, — подчеркивает **Илья Галиуллин**. — Мы внимательно отслеживаем регуляторные изменения и запросы бизнеса, чтобы технологии можно было внедрять не в формате эксперимента, а как надежное решение для ежедневной работы».

Команда как главный актив

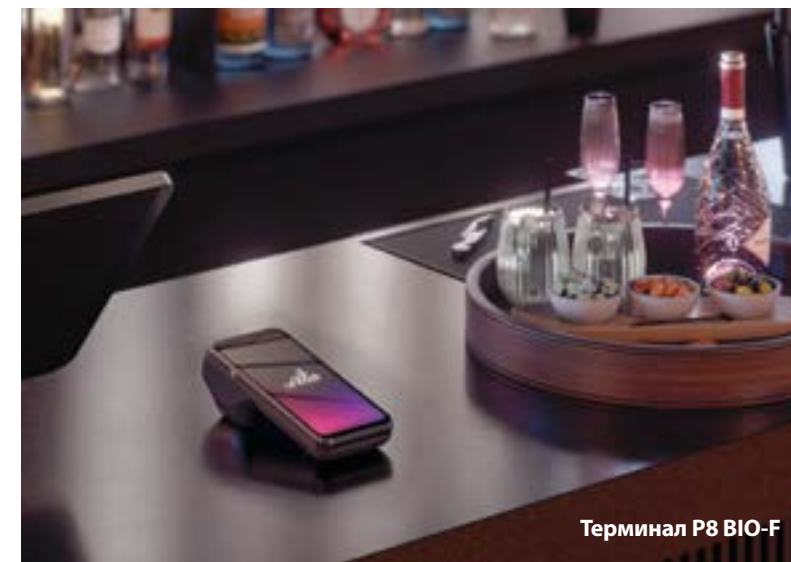
За оборудованием, интерфейсами и программным обеспечением стоит команда с разными компетенциями: инженеры, разработчики, тестировщики, специалисты по сопровождению, аналитики и дизайнеры. Именно

соединение этих ролей позволяет пройти весь путь — от идеи и технического задания до серийного устройства и его работы в инфраструктуре клиента.

«Секрет успеха компании — не в одной технологии и не в одной удачной модели, — отмечает **Максим Батраков**. — Он в людях, которые умеют видеть задачу целиком, глубоко разбираться в своей области и вместе находить нестандартные решения. Благодаря нашей команде мы можем начинать проект с чистого листа и доводить его до работающего продукта».

Сегодня unitodi продолжает расширять линейку российских терминалов, кассовых решений и программного обеспечения. При этом главная ставка сделана не на количество устройств в каталоге, а на способность собрать из инженерных, цифровых и дизайнерских компетенций решение под конкретный бизнес. Рынок эквайринга движется к персонализации: банки и ритейлеры хотят, чтобы платежная инфраструктура была узнаваемой, управлялась как единая система и помогала выстраивать отношения с клиентом.

В этой логике терминал становится больше, чем последний шаг оплаты. Он превращается в часть сервиса, в носитель бренда и в технологическую платформу, кото-



Терминал P8 BIO-F

КОНТАКТЫ:
unitodi.ru
info@unitodi.ru

рую можно развивать вместе с бизнесом. Именно таким unitodi видит будущее платежного опыта — локальным по происхождению, современным по технологиям и индивидуальным по своему характеру.

ПЛАС



Станислав Кузнецов, Сбер: «Кибербезопасность становится ключевым конкурентным преимуществом»

ПЛАС: Как развитие технологий дипфейков меняет работу финансовой сферы, а возможно, влияет и на другие сферы жизни? Каковы прогнозы развития угрозы?

С. Кузнецов: Это серьезная угроза, она на слуху у государства и бизнеса. Сбер сам активно привлекает к ней внимание, в частности, наша сессия на ПМЭФ-2026 была посвящена именно дипфейк-атакам и способам борьбы с ними на законодательном и технологическом уровнях. Мы в режиме реального времени демонстрировали, как легко и быстро можно создавать высококачественные поддельные видео и голос любого человека, в том числе публичной личности. Также мы показали, как с этими подделками можно бороться с помощью разработанного Сбером сервиса «Алетейя».

Но дипфейки — это лишь вершина айсберга, который называется «ИИ в киберпреступности». Они все чаще используются злоумышленниками как часть комплексной атаки — вместе с вредоносным программным обеспечением, фишингом, утечками данных и автоматизированными коммуникациями.

К сожалению, мы уже находимся в той точке преступной эволюции, когда сравнительно небольшая группа злоумышленников с помощью современных технологий может одновременно атаковать сотни тысяч и даже миллионы людей. И чем дальше, тем более адресными будут эти массовые атаки. Например, команды злоумышленников в расчете на большой куш уже собирают всю доступную информацию о потенциальной жертве: ее круг общения, привычки, психологические особенности, личную компрометирующую информацию. Потом начинают готовить персональную легенду, создавать лжедокументы и необходимые аудио- и видеодипфейки. А затем, выбирая нужное время и место, наносить удар, чтобы жертве такая психологическая атака казалась максимально правдоподобной.

Только в 2025 году мы зафиксировали десятикратный рост мошенничества с использованием дипфейков. Наиболее популярная сейчас схема — «фейк босс», когда людям через мессенджеры приходят сообщения с дипфейками их руководителей, также мы фиксировали множество дипфейков с образами крупных предпринимателей, чиновников — это тысячи рассы-



Интервью Станислава Кузнецова, заместителя председателя Правления Сбербанка, для спецвыпуска журнала «ПЛАС».

лок ежедневно. По данным Сбера, преступные группы уже подготовили поддельные материалы с образами руководителей десятков тысяч российских организаций. Потенциальная аудитория таких атак превышает миллион сотрудников.

Что касается дипфейков вне финансовой сферы: их применение действительно не ограничивается хищением денег. Дипфейки могут использоваться для дискредитации руководителей, распространения ложных сообщений, провоцирования паники у населения и нарушения управления организациями. Поэтому это уже не только финансовая, но и общественная и государственная угроза. По факту

ИИ в преступности — это вызов правоохранительной системе. Сможет ли ИИ на стороне защиты эффективно противодействовать этому вызову? Вот ключевой вопрос. Нашим государственным структурам, бизнесу, да и всему обществу надо быть готовыми к этому вызову.

ПЛАС: А каким же образом простые люди могут быть готовы к применению против них дипфейков?

С. Кузнецов: Прежде всего — нельзя выполнять финансовые или административные поручения только на основании видео, голосового сообщения или звонка. Надо перепроверять просьбу через другой заранее известный канал связи. Важно обращать внимание на необычность самой ситуации: срочность, давление, секретность, требование перевода денег или разглашения какой-либо важной информации. При малейшем сомнении надо прекращать коммуникацию. Распознавать дипфейк «на глаз» становится все сложнее, поэтому защищаться надо не угадыванием подделки, а перепроверками.

В целом я рекомендую людям развивать критическое мышление: не доверять слепо всему, что они видят и слышат, особенно если это какое-то одиозное заявление публичной личности. Надо смотреть на источник информации — это официальное уважаемое СМИ или какой-то непонятный канал в соцсетях или интернете? Если после просмотра видео — даже с публичным лицом — у вас возникает чувство тревоги, паники, это тоже признак возможной манипуляции. В общем, надо искать первоисточники, черпать информацию из официальных каналов, а не из тех, где кричащие заголовки и послы, которые подталкивают вас к деструктивным мыслям и поступкам. Сбер создал для всех россиян библиотеку знаний по кибербезопасности — «Кибрарий». Там мы рассказываем обо всех актуальных уловках мошенников и способах противодействия им, в том числе даем рекомендации по противодействию дипфейкам.

ПЛАС: Как противодействовать дипфейкам и другим современным угрозам?

С. Кузнецов: Противостоять преступному применению ИИ можно только с помощью сопоставимых по скорости и масштабу технологий защиты. В Сбере такие технологии активно используются и в антифроде — для защиты денег клиентов, и в других подразделениях — для защиты самого Сбера.

Другой момент: все мы действуем в рамках законодательства, у мошенников же нет ограничений. К сожалению, регуляторика отстает от темпов развития мошеннических технологий. Закон должен признать использование дипфейков в злонамеренных целяхотячающим фактором. Подобные инициативы появились у законодателей еще в 2023 году, потом не раз они возникали в публичном поле. Но новых правовых норм так и не введено. Одними инициативами эту угрозу мы не победим. Нужны срочные конкретные меры.

Отдельное направление противодействия современным угрозам — обеспечение кибербезопасности самого ИИ

Необходимо не только принять соответствующий закон, надо обеспечить его эффективное и прозрачное применение. Нужны конкретные результаты, нужен правовой и практический механизм моментальной блокировки аккаунтов и ресурсов, намеренно распространяющих дипфейки.

Повсеместное распространение технологий выявления дипфейков также крайне важно. Выявление синтетического контента должно становиться стандартной функцией мессенджеров, видеосервисов, корпоративных систем связи, банковских каналов идентификации и других сред, где подмена личности способна причинить ущерб.

Что касается Сбера — мы создали сервис с рабочим названием «Алетейя». Для «обучения» сервиса мы использовали миллионы видео и сотни методов генерации дипфейков. «Алетейя» работает с лицами в кадре с разным освещением, фоном и распознает дипфейки с высокой точностью. В Сбере мы интегрируем этот сервис в систему корпоративных видеоконференций и мессенджер, адаптируем под потребности банка. Мы также готовы предоставлять доступ к сервису компаниям-партнерам для тестирования в реальных условиях и для интеграции в бизнес-процессы. Я считаю, что дипфейки должны выявляться уже в момент их появления в мессенджерах, видеосервисах и других цифровых каналах до начала масштабирования. Поэтому дальнейшее эффективное противодействие требует совместных действий государства и бизнеса.

Осознание угрозы растет, однако скорость практического внедрения механизмов противодействия пока не соответствует скорости развития технологии защиты. Производители и цифровые платформы традиционно конкурируют удобством и функциональностью. Теперь безопасность должна стать таким же обязательным параметром продуктов. Даже если мыслить в рыночной парадигме, такой шаг стал бы серьезнейшим конкурентным преимуществом для производителей и продавцов устройств.

Отдельное направление противодействия современным угрозам — обеспечение кибербезопасности самого ИИ. Массовое внедрение генеративных моделей, мультиагентных систем, а также усложнение архитектур ИИ-решений существенно изменили ландшафт киберугроз для всех современных организаций. Поэтому Сбер опубликовал в открытом доступе на портале «Кибрарий» в разделе «Экспертам» обновленную модель угроз ИИ, учитывающую эти изменения. Документ описывает 37 угроз и 51 способ их реализации. Реализация конкретных описанных в модели угроз может привести,



Станислав Кузнецов
на ПМЭФ-2026

например, к утечке или искажению данных, нарушению доступности и логики работы ИИ-решений, компрометации моделей и инфраструктуры, а также выполнению ИИ-агентами нелегитимных действий. Предоставление Сбером открытого доступа к модели угроз ИИ позволит всем российским государственным структурам и частным компаниям учитывать наш опыт для повышения киберустойчивости своих ИИ-решений.

ПЛАС: Вы думаете, что запрос на безопасность настолько велик в обществе, что может быть конкурентным преимуществом?

С. Кузнецов: Недавно вышло исследование Аналитического центра НАФИ: при выборе банка для семейного обслуживания примерно половина опрошенных назвала безопасность и доверие главным фактором. Почти для каждого второго респондента важны мгновенные уведомления о подозрительных операциях близких и возможность их остановить. Это показывает, что безопасность уже является огромным конкурентным преимуществом. Если раньше компании конкурировали ценой, скоростью, удобством, то теперь все большее значение имеет способность защитить клиента в момент опасности.

ПЛАС: Какое звено в борьбе с мошенничеством является самым уязвимым и требует первоочередного внимания?

С. Кузнецов: Одним из наиболее уязвимых звеньев остается инфраструктура вывода и легализации похищенных средств через дроп-курьеров и дроповые счета с последующей конвертацией в криптоактивы.

Через дроп-курьеров в 2025 году, по экспертным оценкам, было похищено 120 млрд рублей, а всего через криптовалюту в прошлом году выведено порядка 295 млрд рублей. Пока преступник может быстро переве-

сти похищенные деньги через цепочку счетов и вывести их за пределы регулируемого контура, даже сильная система выявления будет работать с запаздыванием. Поэтому необходимо регулировать не криптовалюту как технологию, а профессиональную инфраструктуру обмена, хранения и вывода средств: через регистрацию участников, идентификацию клиентов, мониторинг операций и ответственность за обслуживание преступного оборота.

В России приняли Закон «О цифровой валюте и цифровых правах». Мы надеемся, что на основе закона будет сформирована эффективная система управления рисками на рынке криптовалюты, учитывающая интересы легальных участников и способная защищать интересы россиян.

ПЛАС: Считается, что в первой половине 2026 года в борьбе с мошенничеством в России произошел положительный сдвиг. Насколько этот вывод соответствует действительности? Какие факты на это указывают?

С. Кузнецов: Эту тенденцию подтверждают официальная статистика и наши собственные наблюдения. По данным МВД РФ, с начала 2026 года количество преступлений в сфере компьютерной информации снизилось на 38,7%, дистанционных краж — на 17,8%, ИТ-мошенничеств — на 26,4%. По данным ЦБ РФ, объем несанкционированных операций у физлиц в первом квартале текущего года также сократился по сравнению с аналогичным периодом прошлого года. За первую половину 2026 года мошенники безуспешно пытались похитить у клиентов Сбера порядка 180 млрд руб., что меньше, чем за тот же период прошлого года. В совокупности эти данные позволяют говорить о признаках устойчивого улучшения, но расслабляться рано: преступники меняют каналы, легенды, вывод похищенных денег происходит стремительно.

ПЛАС: На ПМЭФ-2026 вы справедливо заявили, что действующая система регулирования в сфере кибербезопасности поощряет сокрытие инцидентов вместо открытого обмена информацией о них, что делает Россию фактически «слепой» в борьбе с киберугрозами. Как можно изменить сложившуюся ситуацию?

С. Кузнецов: Сегодня регулирование построено по принципу «наказывать за открытость и поощрять сокрытие». Взломали компанию — надо наказать штрафом. Поэтому у всех первая реакция одинаковая: «У нас все в порядке, ничего страшного не произошло». Регулирование следует развернуть на 180 градусов. Нам надо поощрять обсуждение инцидентов на рынке, говорить о них открыто и признавать их. Нужно переключать сознание и корпоративную культуру каждой компании, чтобы никто не боялся последствий раскрытия. Этому способствовало

бы изменение отношения к инцидентам контрольно-надзорных органов: роль союзника, партнера, помощника, а не строгого судьи помогла бы бизнесу перестроить мышление. Надо понимать, что государство и бизнес — не противники, они по одну сторону баррикад. При этом открытость не должна освобождать компанию от ответственности за грубые нарушения, но своевременное добровольное раскрытие инцидента и передача индикаторов атаки должны учитываться как смягчающие обстоятельства. Сегодня же молчание бизнеса играет на руку киберпреступникам.

Первопроходцем в плане открытости выступила страховая компания «ВСК» — именно на ее сессии на ПМЭФ я поднял эту тему. ВСК действовала по тому принципу, который я описал. Опыт компании показал, что открытое признание инцидента и профессиональная коммуникация не разрушают доверие. Напротив, ответственное поведение компании может укрепить ее репутацию и помочь другим участникам рынка усилить защиту.

Это должно стать системным подходом. Например, можно создать рабочую группу технических специалистов при национальном координационном штабе, о необходимости создания которого мы уже неоднократно говорили.

Нужен не еще один совещательный орган, а постоянно действующий оперативный механизм, который имеет полномочия, технологическую платформу и регламент принятия решений при отработке инцидентов. Наличие такой группы позволит также делать качественный анализ инцидентов и делиться информацией с другими компаниями, чтобы они соответствующим образом совершенствовали свою защиту. Техническим фундаментом для обмена такой информацией может стать, например, разработанная Сбером платформа управления киберугрозами X Threat Intelligence — к ней уже подключено более 760 организаций, которые бесплатно получают качественную аналитику со всего мира об актуальных киберугрозах.

ПЛАС: На ПМЭФ-2026 прозвучал совет контрольно-надзорным органам провести аудит киберустойчивости компаний — насколько эта мера может оказаться результативной?

С. Кузнецов: Я считаю, что с учетом новых рисков в цифровой среде на фоне развития ИИ необходимо расширять функции российских контрольно-надзорных органов. В частности, нужен системный аудит цифрового иммунитета компаний — их способности противостоять киберинциденту, адаптироваться и восстанавливаться. Цифровой иммунитет — новая мера зрелости киберустойчивости бизнеса и новая задача государственного аудита. Роль контрольно-надзорных органов — курировать это направление, показывая, как совершенствовать работу по усилению защиты.

ПЛАС: Можете подробнее раскрыть суть понятия «цифровой иммунитет»?

С. Кузнецов: Цифровой иммунитет — это способность организации предупреждать типовые атаки, быстро обнаруживать неизвестные угрозы, сохранять критические функции во время инцидента, восстанавливаться и исключать повторные атаки. Он должен охватывать весь контур деятельности организации: каналы обмена данными, права доступа, подрядчиков и клиентов и т. д. Проверять следует не только наличие средств защиты, но и реальную способность организации продолжать работу при компрометации отдельных систем, подрядчиков, учетных записей. Роль контрольно-надзорных органов — формировать требования, методики оценки, отраслевые ориентиры и стимулы для повышения зрелости.

ПЛАС: Ваши прогнозы на ближайшую и среднесрочную перспективу — есть ли объективные основания ожидать реального перелома в борьбе с телефонным мошенничеством, дипфейками и т. п. — и за счет чего?

С. Кузнецов: Основания для осторожного оптимизма есть: впервые за долгое время официальная статистика и данные банков показывают улучшение. Но окончательный перелом произойдет только тогда, когда скорость защиты сравняется со скоростью активности преступников. Для этого сигналы об атаке должны передаваться между банками, операторами связи, цифровыми платформами и правоохранительными органами в реальном времени; преступная инфраструктура — блокироваться на этапе подготовки атаки; а похищенные средства — замораживаться до их вывода в наличные или криптоактивы. Нам нужна система, которая не просто расследует уже совершенное преступление, а делает его экономически бессмысленным.

ПЛАС

С. Кузнецов:
«Нам надо поощрять
обсуждение инци-
дентов на рынке»



Какого цвета будущее: синее, зеленое или красное?



Алиса Аппалуп

Сегодня уже все универсальные банки активно развивают онлайн-каналы взаимодействия с клиентами. Но это сегодня, а что необходимо делать для завтрашнего успеха?! Попытка повторить успех Т-Банка похожа на поиск ответа на вопрос, который уже никто не задает... А ответ, между тем, знает каждый из нас — это платформенная экономика (доля маркетплейсов уже 52% от всей непродовольственной розничной торговли). Банки неизбежно станут частью платформы (экосистемы) или уйдут с розничного рынка. Ключевая компетенция платформы — онлайн-продажа товаров (82% населения заходят на eCommerce-ресурсы хотя бы раз в месяц, 59% населения заходили на eCom-площадки в среднем в день). Первым это понял «зеленый» банк и создал МегаМаркет (почему МегаМаркет проигрывает конкуренцию большой тройке Wildberries — Ozon — Яндекс Маркет? Наверняка ответ на этот вопрос упорно ищет коллектив высокооплачиваемых аналитиков, мы же рискуем предположить, что среди комплекса причин выделяется факт отсутствия у МегаМаркет сети ПВЗ). Осознав угрозы, банки предприняли попытку принудить платформы предоставить им равный доступ к их клиентской базе — все по классике: отрицание, гнев.

Перепрыгнуть все ступеньки и сразу оказаться в будущем сейчас пробуют «синие», купив часть Wildberries. При верном подходе, на наш взгляд, у них есть все шансы выиграть конкуренцию и в самой ближайшей перспективе занять доминирующие позиции на розничном рынке страны.



Модуль системы окраски

АДМ для ПВЗ: как превратить пункт выдачи заказов в точку роста клиентской базы банка? Свои ответы на этот вопрос предлагает Алиса Аппалуп, директор по маркетингу компании PrintTrade.

Мир стремительно меняется, и универсальный банк должен не просто идти в ногу со временем, а проактивно строить свою стратегию развития. Паразитирование на производных финансовых инструментах делает банк заложником конъюнктуры. Только работа с реальными экономическими агентами даст и стабильные фонды, и комиссионный доход.

База любой реальной экономики — домохозяйства. Как оптимально выстроить свою работу в рознице? Тотальный уход населения в интернет (86% населения — совокупная аудитория интернета в месяц, Mediascope) радикально изменил подход к стандартам банковского обслуживания. Первым это понял Т-Банк, отказавшись от офлайн-офисов и перенеся обслуживание в смартфон, что позволило ему выйти в топ-20 с ноября.



Универсальный корпус для приема поштено или пачкой

Так в чем же заключается верный подход? Первый, и самый важный шаг — мотивировать клиентов платформы открыть счет в банке. Рынок меняется, и то, что работало вчера, не будет работать завтра. Вчера платформа не имела проблем с оплатой товаров, теперь стабильность доступа покупателей к интернету не гарантирована, а объем покупок в рознице за наличные драматически растет. Вчера платформа не предлагала покупку товаров в кредит, сегодня это явный конкурентный недостаток, ведущий к оттоку части покупателей к конкурентам. Банк, который предложит на платформе кредитование товаров, а также обслуживание этих кредитов в ПВЗ, сразу получает активную клиентскую базу в 100 млн домохозяйств.

В 2025 году маркетплейсы показали впечатляющие результаты (Data Insight):

- Оборот — 13,4 трлн рублей
- Средний чек — 1600 рублей
- Заказов — 8,3 млрд

Это более 22 млн заказов ежедневно, с ежедневным оборотом — более 36 млн рублей! Если кредит на покупку товаров возьмут 5–10% покупателей — это комиссионный доход в сотни миллиардов ежегодно.

Баннер известного банка на той или иной платформе, посвященной возможности **купить товар в кредит и затем погашать его прямо в ПВЗ без доступа в интернет в любой форме: безналичным переводом или внесением наличных**, сразу сделает клиентами данного банка всех покупателей на платформе. Потому что покупатели получают решение всех своих проблем: покупка товара здесь и сейчас, прямо в их доме касса банка, которая принимает наличные, работая даже при отсутствии связи. Далее уже дело техники по продвижению всего спектра банковских и небанковских услуг лояльной клиентской базе. При этом ПВЗ не становится магазином по продаже товаров, но местом, где можно быстро пополнить свой счет, опять же даже без связи: не надо выдавать сдачу, не нужна касса — только депонирование.

ПЛАС

ПИН-пад

Прорывное решение Inktrade

Мы разработали, запатентовали и наладили серийное производство комплексного решения для рывка банка в платформенное будущее:

- биометрический ПИН-пад собственного производства, «с улыбкой» — для приема безналичных платежей (эквайринг) и управления АДМ;
- АДМ для встраивания в мебель ПВЗ (30x50x40 см, вес 40 кг, собственная система окраски банкнот при нападении);
- максимально эргономичный дизайн АДМ для возможной установки лицом к покупателю: работник ПВЗ не будет касаться наличных, прием банкнот пачкой;
- минимальные операционные расходы: никаких мешков — кассета большой емкости с укладчиком для быстрого и удобного пересчета наличных в кассе пересчета банка, околонулевая стоимость владения (нет лишних комплектующих), быстрое и дешевое перемещение комплекса между ПВЗ при необходимости;
- собственное кастомизируемое ПО (включено в реестр Минцифры), сервер мониторинга сети;
- развитая инфраструктура обслуживания — полное покрытие всей территории России услугами: доставки, запуска, сервисного обслуживания 24/7, инкассации наличных.

Почему важен прием наличных для пополнения счета в банке?

На данный момент оплата во всех ПВЗ происходит по безналичному расчету, что резко снижает лояльность клиентов. Динамика денежной массы М0 в России показывает, что в феврале 2026 года объем М0 составил 18,095 трлн рублей по сравнению с 17,854 трлн рублей





Касса банка в ПВЗ

банковской инфраструктуре. Если в такой точке клиент сможет не только получать заказ, но и пополнить счет наличными, оплатить покупку наличными, QR-кодом, картой, то ПВЗ превратится в банковский канал продаж и обслуживания.

При этом ПВЗ не является классическим магазином с привычным форматом розничной торговли: оплата разными способами, выдача сдачи, онлайн-касса самообслуживания, штат сотрудников. Клиенты ПВЗ преследуют четкий результат в виде получения товара быстро, оперативно, удобно, закрывая глаза на внешние условия. Именно способы получения товара играют решающую роль для клиента ПВЗ, возможность оплатить покупку при отсутствии интернета, взять товар в кредит прямо на месте, оплатить по QR-коду или картой.

Какие ценности преследуют клиенты маркетплейсов?

Для клиента привлекательность решения строится вокруг скорости, простоты и многофункциональности, оказание услуг под ключ или в одном окне пользуется в настоящее время огромной популярностью. Сегодня ценится скорость, люди не любят стоять в очередях и не терпят задержек, предпочитая решения, которые экономят время. Открытие счета в банке дает доступ к оплате товара, а возможность внести наличные прямо в ПВЗ снимает барьеры для клиентов, которые получают основной доход в наличной форме или предпочитают контролировать расходы через предварительное пополнение счета.

В одной точке клиент может решить сразу несколько задач:

- пополнить счет наличными;
- оплатить заказ безналичным способом;
- погасить кредит или сплит;
- создать остаток средств для следующих покупок.

Такой сценарий делает работу с банком естественной частью клиентского пути маркетплейса. Банк перестает быть отдельным сервисом, куда нужно специально идти, и становится встроенным элементом повседневной покупки.

Почему именно АДМ?

В ПВЗ, как правило, ограничено пространство и нет места для полноформатного банкомата или cash-ресайклера, поскольку главной задачей является обеспечение 100%-ного приема входящих средств и их немедленное использование в безналичном контуре. Ресайклер в этом случае избыточен из-за ненадобности в наличном обороте непосредственно на точке. Поскольку деньги не нужно выдавать обратно покупателям и остатки спокойно могут лежать на счете до следующей покупки, то усложнять устройство функцией рециркуляции экономически не-

целесообразно: она увеличивает стоимость владения, требования к сервису и занимаемый объем, без нужного эффекта.

АДМ Inktrade весит всего 40 килограмм и легко интегрируется в любую мебель, в устройстве нет лишних узлов в виде принтеров или контроллеров.

В состав входят только купюроприемник, модуль окрашивания и терминал. Такая машина ориентирована на безопасное хранение наличных за счет инновационной технологии окрашивания и авторизации персонала по ПИН-коду, определение подлинности входящих купюр, мгновенное обновление баланса на кошельке и легкую интеграцию с банковскими процессами за счет собственного программного обеспечения. АДМ Inktrade производится полностью в России, ПО интегрируется с любыми системами по стандартному протоколу ISO 8583 и сертифицировано в Минцифре, защитная краска собственной разработки.

Также для модели ПВЗ критичным является быстрый прием денег и такое же быстрое отображение на балансе. Поэтому нашим важным преимуществом является поставка в комплекте с надежным и бесперебойным ПО. Малые габариты, простая работа, внесение пачкой по принципу «положил, и готово», низкая стоимость — все это делает нашу АДМ лучшим вариантом для ПВЗ.

Какой же бизнес-эффект для банка?

Проект по оснащению ПВЗ новой банковской инфраструктурой по приему наличных работает на ключевой KPI — динамика открытия счетов в банке клиентами маркетплейсов. Вокруг этого KPI формируется сразу спектр экономических эффектов. Во-первых, растет клиентская база розницы, поскольку открытие счета становится наиболее удобным инструментом для пополнения и последующей оплаты товаров. Во-вторых, увеличиваются остатки на счетах, поскольку клиент вносит сумму с запасом, а неиспользованный остаток остается в банке как бесплатный ресурс. В-третьих, появляется устойчивый канал комиссионного и процентного дохода через предоставление кредита на товар.

Такая модель масштабируется не точечно, а сетевым образом. Если решение внедряется во все ПВЗ страны, то банк получает не набор разрозненных устройств, а российскую распределенную сеть приема наличных и подключения новых клиентов. Это не просто сервис — а новый формат физического присутствия банка без затрат на открытие новых отделений, установку банкоматов.

Что с инкассацией?

Поскольку рынок инкассации сильно монополизирован, тарифы растут, а покрытие услугой по регионам деградирует, важно иметь выстроенную сервисную модель

по поддержке АДМ на всех точках. Наша компания предлагает полное сервисное обслуживание АДМ под ключ: поэтапное развертывание, веб-портал для управления сетью, логистика, доставка, быстрое подключение, обучение персонала и сервисное сопровождение с федеральным покрытием.

С чего начать?

Для федерального запуска разумно использовать поэтапную схему. На первом этапе партнер берет на себя максимум функций: поставка устройств, доставка, подключение, сервис, логистика и управление сетью. Это позволит банку быстро проверить гипотезу на нескольких регионах без капиталоёмкого развертывания собственной инфраструктуры.

На втором этапе, после подтверждения экономики проекта, часть парка может перейти в собственность банка. Такой подход сочетает гибкость и контроль: вначале минимизация инвестиционных рисков, а затем возможность постепенного удешевления модели владения там, где трафик стабилен и предсказуем.

На третьем этапе АДМ может стать основой кросс-продаж. После открытия счета и первой операции пополнения клиенту можно предлагать сплит, дебетовые и накопительные продукты, а также сервисы регулярных платежей. Тогда ПВЗ становится не только точкой транзакции, но и полноценным каналом роста LTV клиента.

Инновационный прорыв?

Таким образом происходит создание новой клиентской модели. Ключевая инновация здесь заключается в том, что банковская инфраструктура встраивается в самый частотный офлайн-сценарий электронной коммерции — получение товара. Финансовая операция выполняется там же, где совершается покупка:

- один визит решает сразу несколько задач клиента;
- банк получает только входящий денежный поток, без цикла с выдачей наличных.

Новая инфраструктура дает возможность легкой офлайн-дистрибуции банковских продуктов через сеть маркетплейсов. По сути, ПВЗ превращается в микроканал банковского присутствия с низкой стоимостью входа, быстрым развертыванием и понятной экономикой на росте счетов, остатков и кредитного дохода.

Автоматическая депозитная машина для ПВЗ — это решение на стыке финтеха, ритейла и банковской дистрибуции. Оно решает сразу несколько задач банка: ускоряет привлечение новых клиентов, увеличивает число счетов и остатки на них, создает удобный канал оплаты товаров и погашения кредитов, а также позволяет встроить банковские сервисы в повседневный маршрут миллионов клиентов маркетплейсов.

КОНТАКТЫ:
inktrade.ru
Alisa.a@inktrade.ru
89685779227

ПЛАС

ART Fintech: «Строим платформу, где бизнес сам красит забор, и считаем это стратегическим партнерством»

Специально для читателей журнала «ПЛАС»!
Михаил Марин, PLUS Consulting, в ходе беседы с **Борисом Фищуком**, основателем ART Fintech, приходят к идее заключить судьбоносную сделку. В этот раз мы решили отойти от традиционного делового стиля нашего издания в пользу живого диалога. Это позволяет рельефнее передать всю картину происходящего, включая самые мелкие, но крайне важные для понимания детали, а также полнее отразить саму динамику обсуждения проекта и его уникальность.

М. Марин: Рынок уже устал от громких заявлений. Все говорят о «суперприложениях». Вы же утверждаете, что строите платформу уровня WeChat. Это не слишком смело для стартапа?

Б. Фищук: Смело — это когда обещают «цифровую трансформацию» и надеются, что никто не спросит, что именно трансформировали. Мы делаем систему, которая работает. Не в презентациях — в реальной жизни. К тому же мы — никак не стартап. 26 лет работы в сфере банков и финтеха кое-что значат. Скорее, это наш spin-off проект.

М. Марин: Не сомневаюсь в ваших компетенциях. Но WeChat — это Китай, миллиард пользователей, уникальная культура, государственная поддержка. Вы правда считаете, что можно повторить этот эффект не просто в другой среде, а именно на российской площадке?

Б. Фищук: Повторить? Пожалуй, нет. Создать схожую модель — да. WeChat — это целая цифровая страна. Мы строим нечто подобное — открытую среду, адаптированную под банки, государство и коммерцию.

М. Марин: То есть вы хотите стать инфраструктурой?

Б. Фищук: Именно. Не приложением — инфраструктурой.

М. Марин: Инфраструктура — звучит красиво. Но бизнесу важны не концепции, а клиенты, продажи, деньги. Что конкретно получает бизнес?

Б. Фищук: Платформа — это рынок. Не витрина, не каталог, не «еще одно приложение». Это место, где бизнес живет.



Борис Фищук

М. Марин: «Живет» — это как?

Б. Фищук: В полном экономическом смысле. Бизнес получает инструменты роста: лидогенерацию, витрины, мини-аппы, KOL, платежи, CRM, каталог сервисов. Все в одном месте.

М. Марин: Как в WeChat?

Б. Фищук: Как в WeChat — digital first в полном смысле этого понятия.

М. Марин: Теперь давайте разберем бизнес-механики. Что именно вы закладываете в них?

Б. Фищук: Семь ключевых блоков. Каждый — реальный инструмент роста бизнеса.

М. Марин: Расскажите о каждом подробно!



Михаил Марин

Блок № 1. Лидогенерация, как в WeChat

Б. Фищук: Платформа сама приводит клиентов: рекомендации, социальные механики, встроенные каналы, мини-аппы, адаптивные витрины.

М. Марин: То есть бизнес не ищет клиента — клиент сам находит бизнес?

Б. Фищук (улыбается): По крайней мере клиенту так кажется.

Блок № 2. KOL — лидеры мнений внутри платформы

М. Марин: Вы хотите встроить блогеров?

Б. Фищук: Не только блогеров — любых key opinion leaders. Лидеров мнений, которые ведут группы, рассказывают о товарах, делают обзоры, собирают аудиторию.

М. Марин: То есть это не внешняя реклама, а внутренняя экономика влияния?

Б. Фищук: Именно. KOL приводят клиентов, получают процент, помогают бизнесу расти. А уж кто скрывается под маской KOL — реальный известный человек или толпа маркетологов (или, может быть, AI?) — это не так важно.

Блок № 3. Адаптивные витрины

М. Марин: Это про персонализацию?

Б. Фищук: Про персонализацию, доведенную до ума. Витрина сама меняется под пользователя: интересы, покупки, география, сезонность, поведение.

М. Марин: Как если бы магазин сам переставлял полки под каждого клиента?

Б. Фищук: Да. И делал бы это мгновенно и без затрат.

Блок № 4. Official Sites — цифровые сайты внутри платформы

М. Марин: Это про мини-магазины?

Б. Фищук: Это больше, чем мини-магазины. Official sites — полноценный сервис: каталог, корзина, платежи, доставка, CRM, чат, подписки, программы лояльности.

М. Марин: То есть бизнес получает свой цифровой офис внутри платформы?

Б. Фищук: Да. И делает его за пару часов. Или дней, но точно — не месяцев.

Блок № 5. Мини-аппы — фабрика сервисов

М. Марин: Но мини-аппы — это же разработка. Не каждый бизнес готов.

Б. Фищук: У нас — готов. Лоу код, визуальные сценарии, автоматическая кодогенерация, и вот он — мини-апп.

М. Марин: То есть бизнес сам создает сервисы?

Б. Фищук: Да. И это ключевой момент. Или же это делают за него специализированные компании, но тоже практически без привычной разработки.

Блок № 6. Каталог мини-аппов — рынок сервисов внутри общего рынка

М. Марин: Вы хотите, чтобы бизнесы публиковали свои сервисы, а другие бизнесы их использовали?

Б. Фищук: Вы зрите в корень!

М. Марин: То есть один бизнес создает сервис, другой его использует?

Б. Фищук: ...А платформа растет!

М. Марин (смеется): Это же в чистом виде идея Тома Сойера.

Б. Фищук: Вот именно! Бизнесы сами красят наш забор, сами создают сервисы, сами развивают платформу — и еще платят за доступ к каталогу.

М. Марин: И считают это честной сделкой.

Б. Фищук: Потому что это им выгодно.





Блок № 7. Платежная инфраструктура

М. Марин: Платежи — это же просто?

Б. Фищук: Да, когда они выполнены в концепции embedded finance. Мгновенные платежи, P2P, подписки, биллинг, оплата внутри мини аппов. Механики кредитования, рассрочек, прочие сервисы. И конечно, гарантии расчетов типа эскроу-счетов.

М. Марин: То есть бизнесу не нужно думать о платежах?

Б. Фищук: Все уже придумано до него и для него. С другой стороны, банки и финтехи — это тоже бизнесы, и никто не мешает им...

М. Марин: ...тоже немного подкрасить ваш забор? (Смеется.)

Б. Фищук: Почему бы и нет?

М. Марин: Хорошо, бизнес механики понятны. Но как это работает внутри?

Б. Фищук: Там нет магии. Там технологии, которые мы выстраивали все 26 лет.

М. Марин: Перечислите их!

Лоу-код

Б. Фищук: Бизнес может создавать сервисы без классической разработки. Упрощенный конструктор для витрин, конструктор процессов (упрощенный BPM), различные конструкторы для торговых механик.

М. Марин: Не будет ли это слишком тяжеловесно?

Б. Фищук: Нет, это конструктор, который работает, и вот почему.

Автоматическая кодогенерация

М. Марин: Гмм... Остромодный вайб-коддинг?

Б. Фищук: Нет, так пока не работает. Это наше ноу-хау, широко применяющееся в наших текущих решениях, таких как АБС «АРТ-Финтех». Если кратко, то на базе простых визуальных настроек платформа сама генерирует микросервисы, API, модели данных, интеграции.

Открытый стек

Б. Фищук: Kubernetes, PostgreSQL, Java, Node.js — только «опенсорс».

М. Марин: То есть вы не зависите от проприетарных технологий типа Oracle?

Б. Фищук: Именно. И этот подход уже давно проверен нашими китайскими братьями. Только аксакалы помнят, что такое Oracle.

Микросервисы

М. Марин: Масштабирование по горизонтали?

Б. Фищук: И без остановки. Оркестрация процессов.

М. Марин: Мозг всей платформы?

Б. Фищук: Скорее ее нервная система. Тоже визуальная.

М. Марин: Возвращаясь к вопросу — в чем ваше отличие от WeChat? Давайте честно: WeChat — гигант. Вы — стартап.

Б. Фищук: Снова повторяю — мы не копируем WeChat. Мы берем его принципы и делаем технологически современную версию.

М. Марин: Тогда в чем главное отличие?

Б. Фищук: У нас платформа изначально построена как фабрика микросервисов и лоу-кода.

М. Марин: То есть вы строите именно то, что WeChat не мог построить из-за своего наследия?

Б. Фищук: Именно.

М. Марин: Теперь последний вопрос. И он, возможно, самый важный. Борис, я слушаю вас уже час, и у меня возникает ощущение, что PLUS Consulting мог бы быть полезен вашему проекту. Мы знаем банки, знаем рынок, знаем интеграции. Хотите обсудить участие?

Б. Фищук (улыбается): Михаил, я всегда говорил: браки заключаются на небесах, а судьбоносные сделки — прямо на страницах журнала «ПЛАС». Так что мой ответ — безусловно, да!

КОНТАКТЫ:
art-fintech.ru
+7 (495) 120-60-20
sales@art-fintech.ru

ПЛАС



Выручка маркетплейсов может стать базой для региональных налогов

Президент России Владимир Путин поручил Минфину проработать изменения в Налоговый кодекс, предусматривающие распределение налога на прибыль цифровых платформ не только по месту регистрации, но и между всеми регионами.

Инициаторами обсуждения, которое длится полтора года, выступают губернаторы. В текущей ситуации, когда платформы зарегистрированы преимущественно в Москве или Московской области, остальные регионы рискуют потерять значительные доходы.

На ПМЭФ губернатор Мурманской области Андрей Чибис призывал платить налог на прибыль в тех регионах, где формируется эта прибыль в рамках цифровой торговли. Первый замминистра экономического развития Максим Колесников подтвердил, что вопрос обсуждается с Минфином. Один из источников РБК отметил, что «теоретически все за, но практически нет понимания, как выработать единый подход».

Согласно статье 288 НК, налог на прибыль распределяется между регионами по удельному весу численности работников и остаточной стоимости имущества. Однако у маркетплейсов выручка в регионах генерируется не через обособленные подразделения, поэтому этот подход неприменим, поясняет партнер МЭФ Legal Сергей Челышков. Он считает справедливым определять долю выручки от продаж в регионе для распределения налога.

Глава Союза бухгалтеров и налоговых консультантов Евгения Мемрук полагает, что наиболее вероятно введение смешанного индексного подхода.

Wildberries поднял комиссию за перемещение товаров между складами до 3%

Wildberries повысил стоимость услуги по перераспределению остатков товаров между складами для продавцов до 3%. Новые тарифы уже действуют для селлеров, подключающих опцию впервые.

В личных кабинетах продавцов появилось уведомление об изменении условий. Теперь при подключении опции на

90 дней комиссия вырастет на 1%, на 60 дней — на 2%, на 30 дней — на 3%. Ранее размер надбавки составлял 0,5%. Для тех, кто уже пользуется услугой, стоимость останется прежней.

Представитель Wildberries объяснил повышение расширением логистических площадей и увеличением лимитов на прием товаров. При переездах стоимость логистики и хранения рассчитывается по тарифу склада, с которого товар отгружен изначально.

Председатель президиума Ассоциации представителей электронной торговли Алексей Москаленко отметил, что рост цен на топливо неизбежно отразится на стоимости логистических услуг маркетплейсов. Основатель «Клуба партнеров на маркетплейсах» Илья Бухарин добавил, что бизнес сталкивается со сложностями при закупке топлива. Ранее Wildberries впервые за полгода увеличил базовые комиссии для большинства категорий товаров на 5–20 п.п.

Бесконтактные банкоматы сделали классический скимминг невозможным в России

В России мошенникам стало технически невозможно устанавливать на банкоматы привычные считывающие устройства для кражи данных банковских карт. Об этом сообщили в пресс-службе МВД. В ведомстве пояснили, что после массового перехода на карты с чипом скимминг и шимминг перестали представлять прежнюю угрозу.

Дополнительным фактором стало распространение бесконтактных банкоматов, в которых отсутствует физический картоприемник. Из-за этого злоумышленники больше не могут использовать накладки, скрытые камеры и фальшивые клавиатуры для копирования данных карты.

По данным МВД, традиционные методы хищения реквизитов банковских карт фактически ушли в прошлое. Ранее преступники устанавливали на банкоматы специальные устройства, которые считывали информацию с магнитной полосы и позволяли дублировать данные карты. Сейчас такие схемы потеряли актуальность.

При этом в ведомстве предупреждают, что мошенники переходят на новые способы кражи денег. Накануне МВД сообщило о схеме с использованием NFC. В этом случае злоумышленники убеждают жертв установить файл под видом официального банковского приложения. Затем человека просят пройти якобы авторизацию: приложить карту к смартфону и ввести ПИН-код.

После получения этих данных преступники могут использовать их для доступа к счету и снятия средств в разных регионах страны.

Банки хотят ввести единую пониженную ставку в СБП для борьбы с подменой кодов

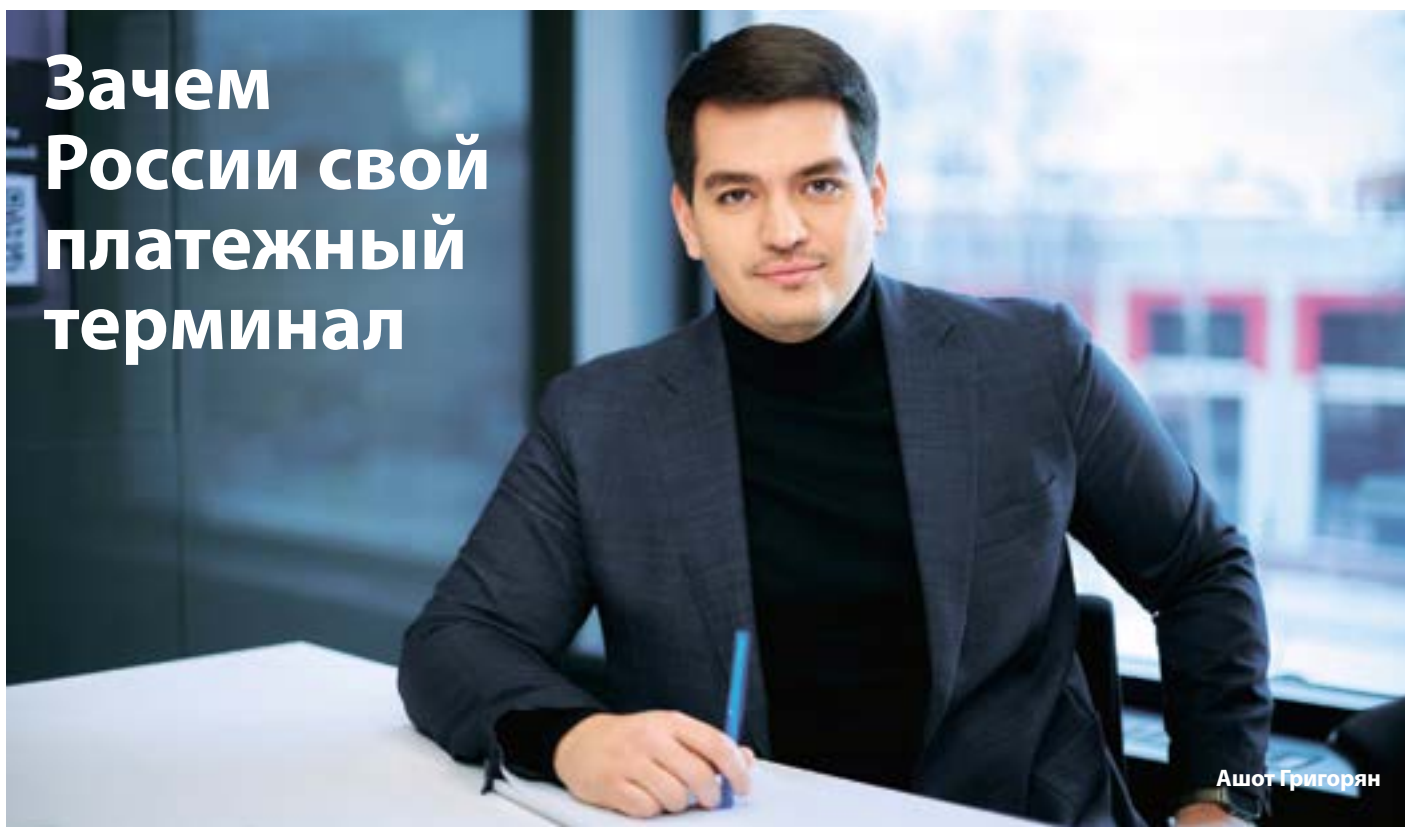
В крупнейших российских банках выявлен значительный дисбаланс в эквайринге при проведении операций через Систему быстрых платежей. Основная часть корпоративных клиентов относится к группам с максимальной комиссией (0,7%), однако более половины денежного объема транзакций генерируют организации, работающие по сниженной ставке (0,4%).

Согласно статистике Совкомбанка, на компании с комиссией 0,7% приходится 48% клиентов, но их доля в денежном потоке — лишь 33%.

В то же время предприятия, уплачивающие 0,4%, обеспечивают 66% финансового оборота. Крупные торговые сети формируют основной объем платежей при низких ставках, а многочисленные представители малого бизнеса — меньшие обороты при высокой стоимости обслуживания.

Участники рынка рассматривают переход на единую пониженную ставку (0,4%) для всех категорий бизнеса. Это позволит не только увеличить общий объем платежей, но и устранить проблему подмены кодов видов деятельности — предприниматели потеряют экономическую мотивацию использовать некорректные идентификаторы. За 2025 год сумма покупок через СБП достигла 8,9 трлн рублей, совокупный доход банков — 40–45 млрд рублей.

Зачем России свой платежный терминал



Ашот Григорян

В декабре 2025 года терминал LIFE PULSE вошел в реестр контрольно-кассовой техники ФНС. Впервые статус кассы получил локализованный смарт-терминал: разработанный и серийно производимый в России, а не собранный под российским брендом на чужом железе. Компания самостоятельно разработала и произвела терминал с самого начального этапа, от подготовки конструкторской документации до организации производства на российском предприятии. При этом банки и магазины по-прежнему пользуются в основном импортным оборудованием, а российские устройства, несмотря на сертификаты, занимают на рынке скромную долю. Ашот Григорян, генеральный директор LIFE PAY, анализирует, что стояло за этим решением и что мешает отечественной платежной электронике расти быстрее.

Почему мы вообще пошли в железо

LIFE PAY много лет сознательно не занималась ни производством оборудования, ни его дистрибуцией — компания строила софт и интегрировалась с чужим железом. Со временем стала видна системная проблема: вендоры оборудования не владеют последней милей. Обратная связь от предпринимателя, который реально пользуется терминалом на кассе, доходит до них поздно, и не напрямую, а через банк. А банк находится на стыке интересов: ему важно дать клиенту оборудование и не разочаровать, но не всегда — решить его конкретную операционную проблему.

LIFE PAY работает с клиентом иначе — полным циклом, от первой заявки до подключения, перерегистрации и сопровождения на первой и второй линиях. Именно поэтому нехватку доработок в чужом железе мы ощущали острее, чем кто-либо на рынке. При этом выходить в сегмент, где уже многие годы демпингуют китайские вендоры с несопоставимо низкой себестоимостью, было бы стратегической ошибкой. Мы рассматривали и покупку команд у сильных производителей — но не сошлись с ними по культуре и видению рынка.

Решение делать собственное устройство и строить свою сборочную линию — вместо того чтобы собирать терминалы из чужих компонентов под своим брендом — компания приняла в 2024 году, при подготовке стратегии до 2030 года: тренд на локализацию платежной инфраструктуры был уже очевиден.

Что именно произошло

Через смарт-терминал проходит оплата картой в магазине или кафе — это одновременно кассовый аппарат и платежное устройство, работающее по стандартам Банка России и Национальной системы платежных карт (НСПК). Раньше почти все такие устройства в России были импортными — чаще китайскими, реже европейскими.

В 2024 году, когда компания предметно оценивала рынок, туда уже входили новые требования: доля закупки отечественного оборудования госбанками должна была составить не менее 50% и продолжать расти, а вместе с ней и требуемая балльность, то есть уровень локализации. При такой балльности в России должна производиться не только сборка, но и пайка системной платы, также обязательно наличие низкоуровневого российского софта, который управляет всеми компонентами устройства. В этом направлении на тот момент всерьез не работал никто на рынке — и для нас это стало не поводом для сомнений, а окном возможностей. Мы собрали команду сильных инженеров с большим опытом в разработке и производстве электронных изделий, которые понимали, что такое сборочная линия, и хотели строить новое.

С тех пор компания разработала архитектуру устройства, локализовала значительную часть компонентов, прошла сертификацию Банка России и Национальной системы платежных карт и запустила собственную контрактную сборочную линию. В 2025 году LIFE PAY заключила стратегические контракты с поставщиками, настроила линию, поставила ее на учет и сертифицировала первый смарт-терминал — с фискальной частью по 54-ФЗ и платежной частью для приема банковских карт. Российское происхождение терминала в октябре 2025 года подтверж-



LIFE PULSE S10-F

дено актом экспертизы Торгово-промышленной палаты по правительственной балльной системе. Терминалы LIFE PULSE собирают на заводе в России, а не привозят готовыми.

В декабре 2025 года к этому добавился статус ККТ в реестре ФНС — по сути, финальная строчка в перечне необходимых бумаг. Терминал также включен в реестр Минпромторга (ГИСП) под номером 10737446. Первые заказчики уже есть, в их числе крупные банки.

Линейка LIFE PULSE на этом не остановится. В 2026 году к ней добавятся еще два продукта: интегрируемое кассовое решение — терминал, который подключается к кассе напрямую, без отдельного чекового принтера, и отечественная касса самообслуживания. В долгосрочной перспективе LIFE PAY намерена выстроить производство полного цикла, включая микросхемы и экраны на территории России; сейчас в проработке — выбор площадки под эти мощности.

Что мешает развитию отрасли

Несмотря на наличие отечественной разработки, более 70% рынка POS-терминалов, по данным исследования РБК за 2025 год, остается за зарубежными производителями. Российские устройства тут ни при чем — ни по качеству, ни по цене. Рынок просто недавно обновил парк.

В 2022 году из России ушел французский Ingenico, на который приходилась примерно половина установленных терминалов в стране. Опустевшее место быстро заняли китайские устройства: банки и сети замещали выходящее оборудование тем, что было доступно по цене и срокам поставки. Свежекупленный парк исправно работает, а естественное обновление идет темпом 13–14% в год, согласно оценке журнала «ПЛАС». Каждое отдельное решение выглядело разумным, но в сумме это создало



многолетнюю паузу в спросе, в которую попадает российский производитель, выходящий на рынок сейчас, когда все нужные сертификаты наконец получены. Есть и вторая часть проблемы: соответствие реестрам не всегда решает исход закупки. Формально правила в пользу отечественной электроники есть: балльная система подтверждения российского происхождения промышленной продукции (постановление № 719), единый реестр российской промышленной продукции, куда входит радиоэлектроника, и единый национальный режим в закупках (постановление № 1875), действующий с января 2025 года. Для радиоэлектроники, включая смарт-терминалы, национальный режим предусматривает правило «второй лишней»: заявку с иностранным товаром отклоняют, если на конкурс пришел российский аналог. Долгое время эту защиту обходили смешанными лотами — терминалы закупались вместе с товарами, не подпадающими под ограничения, и там решали цена и наличие на складе, а не реестр.

Рост объема подстегивает экономику: быстрее окупаемость — активнее новые инвестиции. Конкуренты в производстве платежной электроники пока не спешат. На момент разработки для нас было неожиданностью найти рынок почти свободным.

К тому же в текущих условиях в рынок готовы вкладываться только при окупаемости меньше года, а локализация железа такой скорости не дает. Если объем заказов на российскую платежную электронику падает ниже определенного порога, для любого производителя логичным шагом становится просто закрыть направление.

Пропадает при этом не линейка устройств. Пропадает инженерная и производственная компетенция — люди, которые умеют проектировать и собирать такое оборудование в России. Восстановление потом займет не один год:

life pay
контакты:
life-pay.ru
t.me/lifepay_kassa
vk.ru/lifepay



строить заново сборочные линии и растить инженерные команды быстрее, чем за несколько производственных циклов, не получается.

Верно и обратное: устойчивый рост объема улучшает экономику производства и наращивает поток инвестиций в направление — а это ровно то, ради чего стоит инвестировать в локализацию сейчас.

Что могло бы изменить ситуацию

Действующая регуляторная модель в целом верна и не нуждается в пересмотре. Первый шаг государство уже сделало — запрет смешанных лотов с января 2026 года. Дальше нужны две вещи.

Во-первых, рамочные контракты на три-пять лет для критической финансовой инфраструктуры, сразу с несколькими отечественными производителями, чтобы сохранить конкуренцию между ними. Это даст компаниям горизонт планирования, под который можно уверенно вкладываться в производство, а заказчикам — гарантированные сроки поставки, прозрачное ценообразование и единый сервис.

Во-вторых, поддержка спроса со стороны малого и среднего бизнеса — самого массового покупателя терминалов в стране, который вообще не завязан на закупочные процедуры крупных банков. Льготный лизинг и субсидирование ставки для предпринимателей, покупающих оборудование из единого реестра российской промышленной продукции, создадут рыночный спрос без дополнительного административного регулирования.

Регуляторная база в основном создана. Ближайшая задача — синхронизировать горизонты планирования закупщиков и производителей. При этом LIFE PAY уже не единственный российский производитель в этой категории. Индустрии нужно, чтобы спроса хватало сразу нескольким конкурирующим производителям, — тогда она по-настоящему состоится.

ПЛАС



PLUS
CONSULTING
plus-consulting.org



БИЗНЕС-КОНСАЛТИНГ



Стратегия



Операции



Технологии



**Экспертные
консалтинговые услуги**

Комплексные решения для бизнеса

Платежная инфраструктура больше не принадлежит только банкам: как управлять всей цепочкой платежа

Аркадий Прокудин, коммерческий директор международной консалтинговой группы Compliance Control & Rakasta, о Вселенной безопасных платежей.



Платеж давно перестал быть отдельной технической операцией внутри банковской системы. Сегодня за несколькими секундами между нажатием кнопки «Оплатить» и подтверждением транзакции стоит распределенная инфраструктура: банковские системы, процессинг, антифрод, мобильные приложения, API, платежные сервисы, маркетплейсы, ритейл, технологические провайдеры и внешние подрядчики.

Для клиента вся эта цепочка должна оставаться незаметной. Для бизнеса она становится одной из наиболее критичных частей цифровой архитектуры. Сбой, ошибка интеграции или уязвимость одного участника способны повлиять на доступность платежей, сохранность данных, выполнение регуляторных требований и доверие ко всей экосистеме.

Именно поэтому безопасность платежей уже нельзя рассматривать как задачу одного подразделения или одной организации. Банки, финтех-компании, ритейл и технологические поставщики работают внутри единой среды — Вселенной безопасных платежей.

Если деятельность организации связана с финансовыми транзакциями, она уже является частью Вселенной безопасных платежей. Вопрос лишь в том, насколько осознанно компания воспринимает свою роль и управляет возникающими рисками. Задача ИБ-комплаенса заключается не только в выполнении отдельных требований, но и в построении безопасных процессов, повышении устойчивости бизнеса и формировании доверия клиентов.

Вселенная безопасных платежей объединяет банки, финтех, платежные сервисы, ритейл, маркетплейсы, технологических провайдеров, подрядчиков и клиентов. Всех участников связывают данные о платежах и платежщиках, требования безопасности, комплаенс и взаимное доверие на основании подтвержденных требований индустрии.

Платеж превратился в систему взаимных зависимостей

Классическая платежная цепочка включала клиента, торговую точку, банк-эквайрер, платежную систему и банк-эмитент. Сегодня эта модель стала значительно сложнее.

В проведении и сопровождении одной транзакции могут участвовать мобильное приложение, облачная инфраструктура, микросервисы, системы идентификации, программы лояльности, внутренние счета, сервисы рассрочки, антифрод-платформы, API-партнеры и подрядчики, отвечающие за разработку или эксплуатацию отдельных компонентов.

Каждый новый сервис делает клиентский опыт быстрее и удобнее, но одновременно увеличивает количество точек входа, обрабатываемых данных и технологических зависимостей, а значит и потенциальных точек утечки данных и отказа.

Для CIO и CISO это означает переход от защиты отдельных систем к управлению полной картой платежной инфраструктуры. Организации необходимо понимать:

ВСЕЛЕННАЯ БЕЗОПАСНЫХ ПЛАТЕЖЕЙ

Как устроена распределенная платежная инфраструктура



Там, где есть платеж, есть данные, ответственность и доверие

- где возникают, обрабатываются и хранятся платежные и персональные данные;
- какие системы участвуют в проведении транзакции;
- какие внешние сервисы подключены через API;
- кто имеет привилегированный доступ к критичным компонентам;
- какие подрядчики участвуют в разработке и эксплуатации;
- какие процессы критичны для непрерывности платежей.

Уязвимость может находиться не в центральной банковской системе, а на стыке сервисов, в некорректно настроенном доступе, мобильном приложении, устаревшем программном компоненте или инфраструктуре подрядчика.

При этом последствия затронут не только владельца слабого звена. В распределенной платежной среде локальный инцидент быстро становится проблемой всей цепочки.

При анализе платежной среды важно учитывать, что разовая проверка или аудит подтверждают состояние системы в моменте проверки. Компании-участники Вселенной безопасного платежа, которым особенно важно доверие клиентов к своей системе, переходят к контролю соответствия стандартам в постоянном режиме — continued compliance.

Ответственность нельзя разделить так же легко, как технологии

Технические функции внутри платежной инфраструктуры могут быть распределены между десятками участников. Ответственность за безопасность при этом не исчезает.

Банк отвечает перед регулятором и платежными системами. Финтех-компании — перед банками-партнерами, клиентами и инвесторами. Ритейл или маркетплейс — перед эквайрером, клиентами, владельцами данных и покупателями своих онлайн- или офлайн-площадок. Технологический провайдер должен подтверждать надежность своих решений и процессов разработки.

В результате требования распространяются по всей цепочке. Банк проверяет контрагентов, платежная система предъявляет требования участникам инфраструктуры, крупный заказчик запрашивает подтверждение защищенности у поставщика, а регулятор оценивает не только наличие документов, но и фактическое выполнение мер безопасности.

Аудит становится не формальной процедурой, а инструментом управления взаимным доверием.

PCI DSS подтверждает способность организации безопасно работать с данными платежных карт. ISO/IEC

ОТ РАЗОВОГО АУДИТА К CONTINUED COMPLIANCE

Как меняется подход к управлению соответствием



Комплаенс становится частью архитектуры и операционной устойчивости бизнеса

27001 показывает наличие выстроенной системы управления информационной безопасностью. SWIFT CSP применяется к инфраструктуре финансовых сообщений. ГОСТ Р 57580 и требования Банка России задают требования к защите информации и операционной надежности финансовых организаций.

Анализ уязвимостей, пентесты, проверки мобильных и веб-приложений позволяют оценить не только документы, но и фактическую защищенность технологической среды.

Однако отдельные проверки сами по себе не формируют устойчивую систему. Организация может успешно пройти аудит, а через несколько месяцев изменить архитектуру, подключить нового подрядчика, запустить API или выпустить обновление приложения. Формально действующий сертификат в такой ситуации уже не всегда отражает реальное состояние инфраструктуры.

Что показывают результаты пентестов

Одна из наиболее распространенных проблем платежной инфраструктуры заключается не в отсутствии средств защиты, а в недостаточной управляемости процессов внедрения и изменения компонентов.

По данным исследовательского центра Compliance Control & Rakasta, за январь–май 2026 года в рамках пентестов компаний финансового сектора, банков, ритейла и маркетплейсов была выявлена 1341 уязвимость. Почти треть из них относилась к высокому и критическому уровням риска.

В банковском сегменте среди характерных проблем встречались компоненты с известными уязвимостями, открытое хранение учетных данных, несанкционированные места хранения данных платежных карт и ошибки конфигурации.

В финтехе значимыми зонами риска оставались авторизация и контроль доступа, небезопасные настройки, использование стандартных учетных данных и простых паролей.

В ритейле и на маркетплейсах особого внимания требуют разглашение конфиденциальных данных, аутентификация, управление сессиями, бонусные системы и программы лояльности.

За январь-май 2026 года в ходе пентестов банков, финтех-компаний, ритейла и маркетплейсов была выявлена 1341 уязвимость. Почти треть относилась к высокому и критическому уровням. Риск определяется не только количеством уязвимостей, но и их влиянием на платежную инфраструктуру и непрерывность бизнеса. Даже базовая ошибка в управлении доступом или конфигурации может стать начальной точкой атаки на сложную распределенную инфраструктуру. Поэтому защита должна строиться не только вокруг наиболее технологичных угроз, но и вокруг системного контроля стандартных процессов.

Почему точечные ИБ-решения не закрывают проблему

Большинство зрелых организаций уже инвестируют в SOC, антифрод, средства управления доступом, анализ уязвимостей, резервирование и обучение сотрудников. Но наличие большого количества защитных решений еще не означает, что платежная среда управляется как единая система.

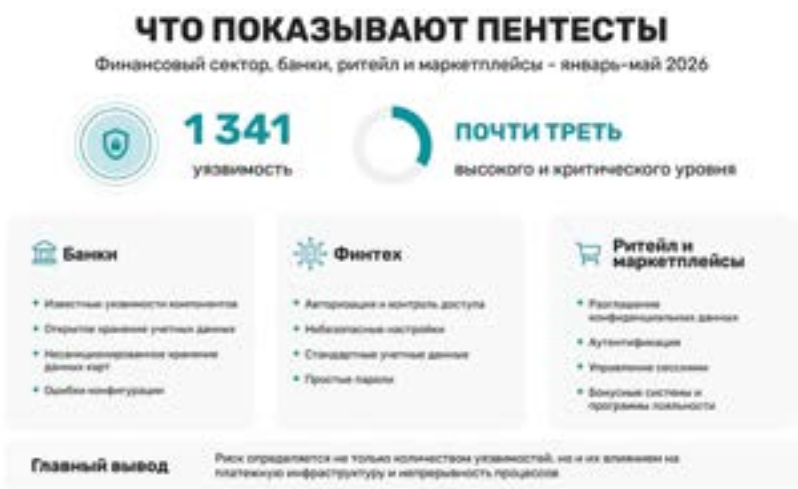
Одна из ключевых проблем — позднее подключение команды информационной безопасности к процессу разработки и внедрения ИТ-компонентов системы.

ИБ-команда часто включается перед запуском продукта, аудитом или уже после инцидента. К этому моменту архитектурные решения приняты, интеграции реализованы, подрядчики выбраны, а изменение процессов требует дополнительных ресурсов и может замедлить выход продукта на рынок (Time-to-Market).

Для платежной инфраструктуры такой подход особенно опасен. Любая ошибка способна повлиять не только на конфиденциальность информации, но и на доступность сервиса, проведение транзакций и выполнение обязательств перед партнерами.

Безопасность должна учитываться еще на этапе проектирования продукта: при выборе архитектуры, разработке API, определении модели хранения данных, подключении поставщиков и формировании ролей доступа.

Принцип Zero Trust, контроль привилегированных учетных записей, мониторинг аномалий, безопасная разработка, управление уязвимостями и контроль цепочки поставщиков компонентов должны быть не набором независимых проектов, а элементами единой архитектуры запуска услуги или платежного сервиса.



От разовой проверки к постоянному соответствию

Командам комплаенса и ИБ уже давно приходится не просто. Снаружи растет количество регуляторных, отраслевых и договорных требований. Внутри компаний становится больше систем, продуктов, подразделений и поставщиков, которые должны выполнять эти требования. При этом основная задача бизнеса — формировать прибыль, а не выполнять требования регуляторов. Нагрузка на отделы комплаенса растет как со стороны внешних требований, так и внутри компаний. Нужно не только соблюдать законы и правила, но и обеспечивать их выполнение на всех уровнях бизнеса. Одна из наших задач — обеспечение соответствия международным и локальным стандартам, а также автоматизация функций комплаенса.

Вручную управлять таким объемом данных становится все сложнее. Требования распределяются между ИБ, ИТ, юридической службой, внутренним контролем, операционными подразделениями, разработкой и бизнесом. При этом каждое направление может использовать собственные системы учета.

В результате компания нередко видит общую картину только в момент аудита, когда начинается срочный сбор подтверждений и устранение накопившихся несоответствий.

Более зрелая модель — continued compliance, или постоянное соответствие требованиям. Ее задача заключается в том, чтобы поддерживать необходимый уровень контроля непрерывно, а не восстанавливать его перед очередной проверкой.

Continued compliance превращает соответствие требованиям из периодической подготовки к проверке в постоянный управляемый процесс: требования, контроль, мониторинг, выявление отклонений и корректировка.

В рамках такой модели организация должна постоянно понимать:

- какие требования к ней применимы;
- кто в подразделении отвечает за их выполнение;
- какие подтверждения уже собраны;
- где обнаружены отклонения;
- какие изменения в инфраструктуре повлияли на соответствие;
- какие меры необходимо реализовать до внешнего аудита.

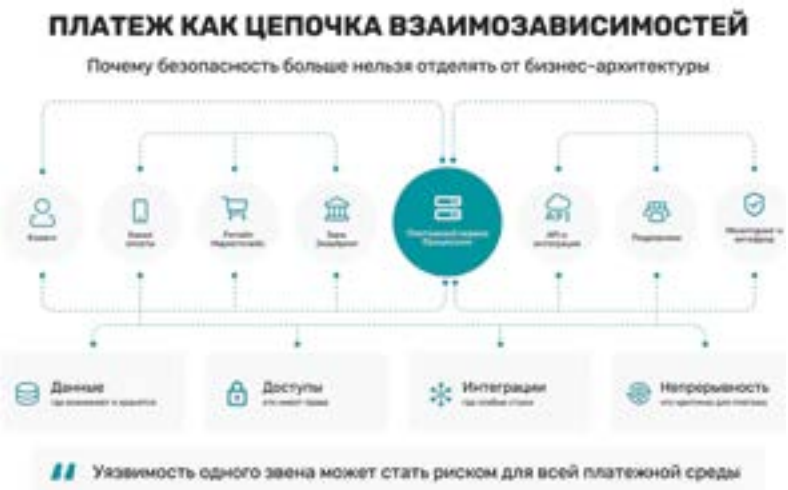
Такой подход меняет роль комплаенса. Он перестает быть функцией, которая только фиксирует нарушения, и становится частью управления архитектурой и операционной устойчивостью.

Для автоматизации этого процесса Compliance Control развивает Compliance App—решение, которое позволяет отслеживать уровень соответствия требованиям, распределять ответственность между подразделениями, фиксировать отклонения и своевременно реагировать на изменения.

Локальные требования меняют архитектуру платежных систем

Дополнительную сложность создает работа в нескольких юрисдикциях. Международные стандарты могут сочетаться с локальными требованиями к персональным данным, критической информационной инфраструктуре, сертификации решений, хранению информации и реагированию на инциденты.

В России организации учитывают требования 152-ФЗ, нормы по защите КИИ, ГОСТ Р 57580 и требования Банка России. В Европейском союзе на финансовые и технологические компании влияют регламенты GDPR, DORA и MiCA. В странах Ближнего Востока развиваются собственные



требования PDPL (реинкарнация европейского GDPR). Отдельные национальные подходы формируются в Казахстане, Узбекистане и других странах.

Для международного бизнеса задача заключается не только в том, чтобы собрать перечень применимых требований. Необходимо встроить их в архитектуру таким образом, чтобы система оставалась управляемой и масштабируемой в каждом регионе присутствия отдельно и вся целиком.

Учитывая текущие сложности для компаний в поиске выходов на внешние рынки, CISO должен понимать, где хранятся данные, какие средства защиты допустимы в конкретной стране, какие специалисты и подрядчики могут участвовать в сопровождении критичных процессов и какие доказательства соответствия потребуются предоставить регулятору или партнеру.

Единого универсального решения для всех юрисдикций может не существовать. Но должна существовать единая логика управления требованиями, рисками и контролями.

AI/ML: инструмент защиты и новый источник риска

Искусственный интеллект уже применяется в антифрод, скоринге, анализе транзакций, идентификации клиентов и выявлении подозрительных операций. Для банков и финтех-компаний это возможность повысить скорость реакции, качество аналитики и эффективность команд.

Но использование моделей одновременно создает дополнительные риски: утечки данных при взаимодействии с внешними платформами, манипуляции данными в обучающих выборках, атаки на модели, зависимость от непрозрачных алгоритмов и неконтролируемое использование публичных сервисов сотрудниками, которые могут стать источником утечки корпоративной информации.

Внедрение AI/ML также должно сопровождаться архитектурными и комплаенс-контролями. Организации необходимо определить:

- какие данные можно передавать в модель;
- какие сценарии требуют изолированной инфраструктуры;
- кто получает доступ к данным, алгоритмам и результатам;
- как проверяются решения модели;
- кто отвечает за ошибочный результат;
- как система защищается от манипуляций и утечек.

Вопрос для CIO заключается уже не в том, использовать ли искусственный интеллект, а в том, как встроить его в управляемую и безопасную платежную среду.

«Пройти мимо нельзя безопасно использовать» — запятую поставьте самостоятельно.

Меняется роль CIO и CISO

CIO и CISO больше не могут работать в параллельных контурах.

CIO определяет технологическую архитектуру, интеграции, скорость изменений и выбор поставщиков. CISO отвечает за защиту информации, управление рисками и выполнение требований. В платежной инфраструктуре эти зоны пересекаются практически на каждом шагу.

Безопасность должна учитываться при проектировании продуктов, бюджетировании, выборе облачной или локальной модели, подключении API, разработке приложений, управлении данными, работе с подрядчиками и планировании непрерывности.

Это не означает, что CIO должен заменить CISO или наоборот. Однако ответственность за устойчивость платежной среды становится общей управленческой задачей.

Безопасность платежей становится стандартом взаимодействия

Финансовые сервисы все глубже встраиваются в ритейл, маркетплейсы, цифровые платформы и клиентские экосистемы. Одновременно банки и финтех-компании используют все больше внешних технологий и партнерских решений.

В такой среде уже невозможно определить единственную границу платежной инфраструктуры. Она проходит через приложения, API, подрядчиков, облачные платформы, внутренние системы и процессы взаимодействия между организациями.

Поэтому главный вопрос для бизнеса звучит уже иначе, чем раньше: «Нужно ли компании заниматься безопасностью платежей?». Потому что если платеж присутствует в бизнесе, компания уже находится во Вселенной безопасных платежей.

Вопрос в другом: «Видит ли организация всю цепочку зависимостей, управляет ли требованиями непрерывно и способна ли подтвердить надежность инфраструктуры перед банками, партнерами, регуляторами и клиентами?».

Разовая проверка может зафиксировать состояние системы в конкретный момент. Но устойчивость обеспечивает способность компании постоянно контролировать изменения, закрывать уязвимости, управлять доступами и встраивать безопасность в бизнес-архитектуру. **ПЛАС**

КОНТАКТЫ

compliance-control.ru
info@compliance-control.ru
+7 499 136 2766

КАЛЕЙДОСКОП

Принят закон о полном раскрытии тарифов на денежные переводы

Госдума приняла в третьем, окончательном чтении законопроект, который обязывает банки и платежные сервисы подробно раскрывать условия денежных переводов, онлайн-платежей и обслуживания карт. Также поправки предписывают информировать клиентов об условиях кредитования согласно единым банковским стандартам.

Поправки закрепляют обязанность кредитных организаций публиковать в офисах и на сайтах в доступном виде полные условия денежных переводов, включая переводы через Систему быстрых платежей по номеру телефона или по QR-коду. Это же коснется условий использования электронных средств платежа, таких как банковские карты и банковские мобильные приложения.

Порядок раскрытия информации о переводах будет определяться отраслевыми стандартами. Поправки распространяют этот принцип и на размещение условий по потребительским кредитам.

Для того чтобы заемщики могли сопоставлять предложения и осознанно выбирать условия займа, порядок и форма размещения данных по потребкредитам также будут устанавливаться через банковские стандарты. Это касается информации по ставкам, полной стоимости, санкциям за просрочку и других сведений, которые важно видеть до заключения договора.

«Банки и платежные системы будут открыто информировать клиентов обо всех тарифах, комиссиях и правилах денежных переводов.

Это позволит исключить скрытые платежи и ситуации, когда человек узнает о плате за перевод или обслуживание карты уже после совершения операции. При этом мы закрепляем общие правила раскрытия условий переводов и кредитования через отраслевые стандарты. Это значит, что требования будут единообразными для каждого сегмента финансового рынка, а условия оказания услуг — максимально понятными для всех людей», — поясняет председатель комитета Госдумы по финансовому рынку Анатолий Аксаков.

Закон вступит в силу с 1 сентября 2027 года.

Госдума приняла закон о базовом определении искусственного интеллекта и регулировании больших моделей

Госдума приняла во втором и третьем чтениях документ, который вводит базовое определение ИИ и формирует принципы регулирования больших фундаментальных моделей.

Международный ПЛАС-Форум Digital Tajikistan

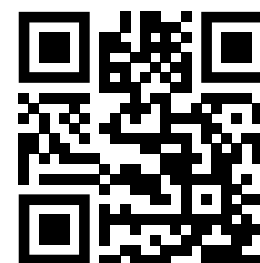
PLUS⁺
FORUM

**Digital
Tajikistan**
International PLUS-Forum

TAJIKISTAN, DUSHANBE
NOVEMBER 26|2026



**26 ноября 2026 года
Душанбе станет точкой
сбора тех, кто
формирует цифровое
будущее Центральной
Азии. Финтех, ИИ,
цифровой сомони,
исламский банкинг —
обсуждаем вместе
с Нацбанком
и топ-менеджментом
ведущих банков.
Присоединяйтесь!**



1500+
участников

50+
спонсоров

70+
спикеров

Национальная библиотека Таджикистана, Душанбе

Антифрод 2.0. Что меняется и в какую сторону

Независимый эксперт Николай Пятизбянцев анализирует изменения и правовые нормы, вводимые Федеральным законом от 26.06.2026 № 210-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации» (второй пакет «Антифрод» Минцифры).



Рассмотрим некоторые требования, вводимые данным законом, получившим неофициальное название Антифрод 2.0 и недавно прошедшим третье чтение в Госдуме, а также то, как они отразятся на банковской сфере.

Анализ изменений в 161-ФЗ

Итак, начнем с изменений, вносимых новым пакетом поправок в Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

Уточняются действия оператора платформы цифрового рубля (Банка России). Если ранее он должен был выявлять операции с цифровыми рублями, соответствующие всем признакам осуществления перевода денежных средств без добровольного согласия клиента (далее — ОБДС), то теперь — только если информация содержится в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, формирование и ведение которой осуществляются в соответствии с частью 5 статьи 27 настоящего Федерального закона (далее — база ФинЦЕРТ). Напомним, что в действующем Приказе Банка России от 05.11.2025 № ОД-2506 это пункты 2.1 и 2.2.

Хотелось бы обратить внимание на то, что участники платформы цифрового рубля (банки) обязаны реализовывать мероприятия по противодействию осуществлению ОБДС, в то время как оператор (ЦБ РФ) лишь вправе реализовывать их по собственному усмотрению (но не обязан это делать). То есть если оператор не отклонил ОБДС,

он ответственности не несет, так как это не является для него обязательным требованием, даже если информация о получателе средств совпадает с информацией из базы ФинЦЕРТ.

Статья 8, обязывающая банк осуществлять проверку наличия признаков ОБДС, дополнена **требованиями использовать сведения, полученные посредством государственной информационной системы противодействия правонарушениям**, совершаемым с использованием информационных и коммуникационных технологий, и предусмотренные пунктами 1 и 2 части 10 статьи 1 Федерального закона от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее — ГИС «Антифрод»). Также необходимо использовать информацию о выявленных с использованием средств защиты информации, указанных в частях 12 и 13 статьи 27 настоящего Федерального закона, случаях воздействия вредоносных компьютерных программ либо иной компьютерной информации, которые предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, на программное обеспечение, используемое клиентом — физическим лицом в целях осуществления переводов денежных средств (далее — информация о воздействии ВПО).

Стоит отметить, что требование об использовании сведений ГИС «Антифрод» уже содержится в пункте 1.2 приказа ЦБ РФ от 05.11.2025 № ОД-2506, а о ВПО — в пункте 1.10 этого же приказа. Что интересно, пункт 1.2, согласно приказу, применяется с 01.03.2026, то есть уже действует, а требования второго пакета «Антифрод» Минцифры относительно использования сведений ГИС «Антифрод» вступают в силу с 01.03.2027. Требования по ВПО в приказе ЦБ РФ должны применяться с 01.01.2026, а в законе «Антифрод» Минцифры — с 01.03.2027.

Меняются требования к банкам в случае выявления признака ВПО. Если ранее банк должен был отклонить или приостановить ОБДС, запросить у плательщика подтверждение и при его получении разрешить повторить или продолжить операцию, то теперь банк обязан отклонить ОБДС, если она совершается с применением окончательного оборудования, в отношении которого полу-

чена информация о ВПО, уведомить клиента о причине отказа и о возможности совершить перевод с использованием другого окончательного оборудования либо при личном присутствии клиента или его представителя в банке.

По операциям с признаками ОБДС банк может применить период охлаждения. Если ранее банк после получения от плательщика подтверждения по ОБДС был обязан незамедлительно принять к исполнению подтвержденное распоряжение клиента или совершить повторную операцию (кроме периода охлаждения на плательщика, который находится в базе ФинЦЕРТ), то теперь в таких случаях банк вправе для остальных признаков ОБДС ввести период охлаждения в течение шести часов.

Вводятся дополнения по ответственности банков по возмещению клиентам — физическим лицам денежных средств по ОБДС (части 3.13-1 — 3.13-7):

- после получения сведений из ГИС «Антифрод» и нарушения требований частей 3.1–3.5, 3.8–3.11 статьи 8;
- при невыявлении ВПО.

Возмещение осуществляется в срок не позднее 30 дней, следующих за днем получения обращения клиента — физического лица об ОБДС, при наличии у него постановления о возбуждении уголовного дела по факту хищения денежных средств. Если ОБДС физического лица осуществлены в результате поступления на окончательное оборудование клиента телефонных вызовов и (или) коротких текстовых сообщений, клиент не позднее 10 рабочих дней, следующих за днем ОБДС или получения уведомления об ОБДС, направил в банк заявление о возмещении, при этом банк надлежаще исполнил свои обязанности по выявлению ОБДС, а сведения в ГИС «Антифрод» отсутствуют, — банк направляет обращение клиента оператору связи и уведомляет об этом клиента. Ответственность оператора связи будет рассмотрена ниже.

Если со стороны банка допущены нарушения по выявлению ОБДС, то банк не вправе отказать в возмещении на основании несоблюдения клиентом — физическим лицом сроков направления обращения (не позднее 10 рабочих дней).

Статья 9 дополнена частью 2.2, согласно которой **клиенту — физическому лицу может быть предоставлено операторами по переводу денежных средств в совокупности не более двадцати платежных карт**, с использованием которых осуществляются переводы денежных средств. Решением Совета директоров Банка России могут устанавливаться случаи, при которых может быть предоставлено более двадцати платежных карт.

Непонятно, зачем Федеральным законом вводится ограничение на количество платежных карт и этим же законом разрешается ЦБ РФ данное ограничение изменять? Гораздо логичнее выглядело бы просто наделить Банк России таким правом. При этом указанное ограничение, скорее всего, будет малоэффективным в борьбе с дропами. Во-первых, так как банки активно с ними борются,

выявленные карты дропов будут активно блокироваться, в результате количество активных карт у конкретного дропа будет сокращаться, но у него останется возможность открывать новые карты, чтобы общее количество было менее двадцати.

Во-вторых, если это злостный дроп (открыл и продал более двадцати карт), то логично, что он должен попасть в базу ФинЦЕРТ (если карты дроповские, должны быть жалобы на ОБДС), а согласно части 2.1 статьи 9 банки обязаны отказать клиенту в заключении договора об использовании электронного средства платежа (в том числе в выдаче новых платежных карт), если он находится в базе ФинЦЕРТ. То есть если клиент попал в базу ФинЦЕРТ, он не получит новую карту ни в одном банке. Неужели для такого попадания необходимо более двадцати дроповских карт?

Помимо указанной неэффективности данной нормы, возникают дополнительные трудозатраты и сложности для ее реализации. Создается единая система учета платежных карт. Банк каждый раз при получении от клиента заявления на выпуск новой карты обязан запрашивать у оператора единой системы учета платежных карт (НСПК), можно ли карту выпустить. Если лимит исчерпан, банк обязан отказать в предоставлении карты. Банки обязаны направлять в НСПК информацию о номерах и видах платежных карт своих клиентов, о номерах платежных карт, использование которых прекращено, об идентификационных номерах налогоплательщиков.

Ранее требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите (статья 27), устанавливало Правительство Российской Федерации по согласованию с Банком России. **Теперь указанные требования будут согласовывать также федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (ФСБ России), и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России).**

Вводятся требования к средствам защиты информации (СЗИ) для программного обеспечения, используемого клиентом — физическим лицом, позволяющим выявлять ВПО. Данные СЗИ должны пройти оценку соответствия. Пока, правда, непонятно, какую именно и как.

Банки обязаны предоставить клиенту — физическому лицу — возможность использования СЗИ от воздействия ВПО на окончательном оборудовании клиента, если клиент дает на это согласие. С этой целью необходимо включать в договор с клиентом — физическим лицом положения о праве клиента дать согласие на обеспечение оператором по переводу денежных средств защиты своего ПО, используемого в целях осуществления перево-

дов денежных средств, включая мобильное приложение и официальный сайт в информационно-телекоммуникационной сети «Интернет», от воздействия вредоносного программного обеспечения путем подключения клиентом средств защиты информации от воздействия вредоносного ПО на пользовательское оконечное оборудование клиента либо отказаться от предоставления такого согласия.

Введены требования для банков о направлении в ГИС «Антифрод» информации об абонентских номерах, используемых при обслуживании клиентов. Данные сведения составляют банковскую тайну, и таким образом они будут направляться на законном основании.

В законе установлены процедуры и сроки реабилитации (исключения) лиц, попавших в базу ФинЦЕРТ:

- Информация об абонентских номерах подвижной радиотелефонной связи исключается из базы по истечении 180 дней со дня ее включения.
- Иная информация исключается:
- по истечении одного года со дня включения этой информации в базу, если она включена впервые;
- и по истечении трех лет со дня повторного включения этой информации в базу.

Если информация получена от органов внутренних дел, она исключается из базы до истечения общих сроков, если от органов внутренних дел получена информация о прекращении уголовного преследования в отношении такого клиента.

Анализ изменений в 41-ФЗ

Теперь рассмотрим изменения, вносимые в Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

Статья 1 дополнена правом физического лица на править с помощью сервиса «Госуслуги» в ГИС «Антифрод» информацию о том, что в отношении него совершены противоправные действия с использованием информационных и коммуникационных технологий.

- Операторы связи обязаны:
- 1) выявлять абонентские номера, которые используются в целях совершения телефонных вызовов и (или) направления коротких текстовых сообщений, имеющих признаки совершения противоправных действий, и направлять информацию о таких выявленных абонентских номерах в ГИС «Антифрод» (номера «мошенников»);
 - 2) выявлять абонентские номера, на которые совершаются телефонные вызовы и (или) направляются короткие текстовые сообщения, имеющие признаки совершения противоправных действий, и направлять информацию

о таких выявленных абонентских номерах в ГИС «Антифрод» (номера «жертв»);

3) приостанавливать оказание услуг связи и (или) услуг по пропуску трафика в отношении абонентского номера «мошенника», а также в отношении всех иных абонентских номеров, которые использует «мошенник», на срок, определяемый Правительством Российской Федерации (пока не установлен).

Определена ответственность операторов связи по возмещению денежных средств физическим лицам в случае ОБДС при одновременном соблюдении следующих условий:

- 1) физическое лицо в договоре с банком указало абонентский номер, выделенный ему этим оператором связи;
- 2) ОБДС осуществлен в результате получения физическим лицом телефонного вызова и (или) короткого текстового сообщения с абонентского номера «мошенника»;
- 3) ОБДС осуществлен в результате несоблюдения оператором связи одного или нескольких требований:
 - а) о направлении в ГИС «Антифрод» информации о номере «жертвы»;
 - б) о приостановлении оказания услуг связи и (или) услуг по пропуску трафика в отношении абонентского номера «мошенника», информация о котором получена посредством ГИС «Антифрод»;
 - в) о приостановлении оказания услуг по пропуску трафика в свою сеть связи в момент установления телефонного вызова, если такой телефонный вызов совершен с абонентского номера «мошенника» и в момент установления такого телефонного вызова данный абонентский номер соответствует критериям признаков противоправных действий;
 - г) о приостановлении оказания услуг связи по абонентскому номеру «мошенника» в момент установления телефонного вызова, если при таком телефонном вызове на абонентский номер «жертвы», совершаемом внутри одной сети связи, в момент установления такого телефонного вызова указанный абонентский номер соответствует критериям признаков противоправных действий;
- 4) банк надлежащим образом исполнил требования по выявлению ОБДС;
- 5) в базе данных ФинЦЕРТ на момент совершения ОБДС отсутствовала информация о случаях и попытках осуществления переводов денежных средств без добровольного согласия физического лица;
- 6) физическое лицо не позднее 10 рабочих дней, следующих за днем осуществления ОБДС или получения от банка уведомления об ОБДС, направило в банк обращение;
- 7) наличие на момент осуществления возмещения суммы ОБДС у физического лица постановления о возбуждении уголовного дела по факту хищения денежных средств в результате ОБДС.

ПЛАС

Теневой рынок киберпреступности переходит на комплексные решения и сервисы по подписке

Эксперты BI.ZONE Threat Intelligence и BI.ZONE Digital Risk Protection проанализировали более 35 тыс. объявлений злоумышленников на теневых форумах, маркетплейсах и в Telegram-каналах за период с лета 2025 по лето 2026 года. Результаты исследования были представлены на конференции OFFZONE 2026.

Теневой рынок все активнее переходит от разрозненных инструментов к комплексным решениям, закрывающим сразу несколько задач атакующих. Продавцы предлагают готовые продукты и сервисы для проведения атак. Например, рынок корпоративных доступов за год вырос на 20% по числу объявлений, а средняя цена увеличилась до 15% в зависимости от сегмента. Вместо простых логинов и паролей теперь предлагают подробные профили организаций с указанием уровня прав, актуальности и других характеристик.

Число киберпреступлений за полгода снизилось почти на 120 тысяч

Благодаря принятым правительством мерам по борьбе с мошенничеством число киберпреступлений за последние полгода по отношению к аналогичному периоду прошлого года сократилось на 30% — с 371,4 тыс. до 252,9 тыс. Об этом свидетельствуют актуальные данные МВД, рассказали в Минцифры. По итогам прошлого года, когда был принят «Антифрод 1.0», количество случаев онлайн-мошенничества уже снизилось на 90 тыс. Минцифры и другие ведомства продолжают работу по защите граждан.

- Какие меры уже действуют:**
- Создана и запущена ГИС «Антифрод». К системе подключились все крупнейшие банки, операторы связи и цифровые платформы. Они в автоматическом режиме обмениваются данными о подозрительных операциях и номерах.

- Микрофинансовые организации обязаны при выдаче кредита подтверждать личность клиента по биометрии. Это гарантирует, что мошенник не возьмет кредит на другого человека.
- Появилось право отказаться от массовых вызовов и рассылок. Опцией запрета обзвонов абоненты воспользовались более 340 тыс. раз.
- Смс-код от Госуслуг больше не приходит во время телефонного разговора. Такая пауза помогает предотвратить действия под давлением мошенников.
- На Госуслугах можно увидеть все свои абонентские номера и заблокировать ненужные или подозрительные. Сервисом воспользовались уже более 200 млн раз.
- Появилась возможность установить самозапреты на кредиты и договоры связи. Это исключает использование данных гражданина мошенниками. Самозапрет на кредиты установили уже более 30 млн раз, на договоры связи — почти 2 млн.

ЦБ предупредил о рисках синхронизации ошибок ИИ у десятков банков

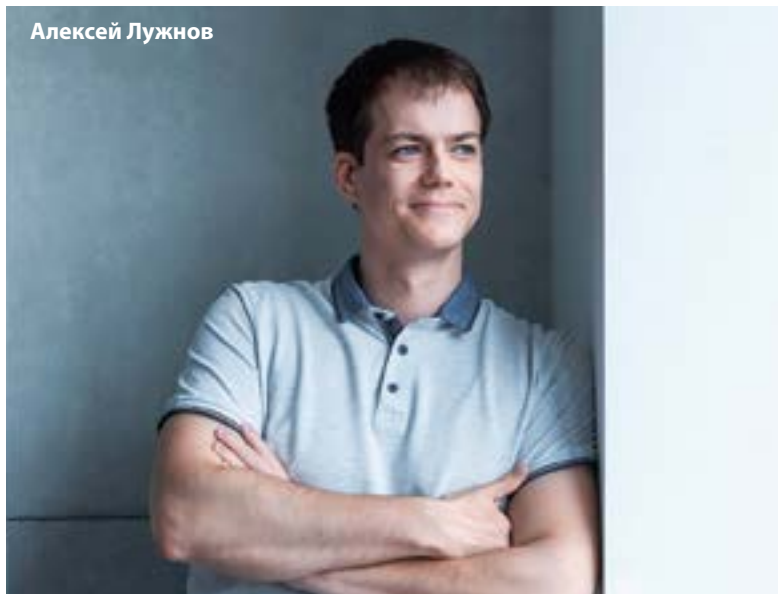
Массовое использование одинаковых глобальных платформ искусственного интеллекта российскими банками создает риск для финансовой стабильности, заявили в Банке России. В юридическом департаменте регулятора подчеркнули, что достоверность исходных данных таких ИИ-моделей проверить невозможно. На форуме Data Day 2026 заместитель директора юридического департамента ЦБ Екатерина Дёмкина отметила, что использование множеством банков одних и тех же платформ формирует значимый риск. «Искусственный интеллект может быть обучен на некачественных данных», — пояснила она. Проблема в том, что данные глобальных моделей не поддаются верификации. Эксперты указывают на непрозрачность платформ. Председатель комиссии по финансовой безопасности ТПП Тимур Аитов отметил: «Мы не видим внутреннего устройства глобальной модели, ее логика для нас остается неизвестной».

Когда десятки банков используют одну платформу, возникает эффект синхронизации ошибок. Сбой у поставщика или незаметное изменение параметров могут привести к сокращению лимитов. По оценке Аитова, потери кредитного портфеля в отдельных сегментах достигают 3–5% за квартал. Глава Ассоциации участников рынка электронных денег Виктор Достов добавил, что синхронизация создает эффект резонанса: одна модель будет инвестировать в одни и те же бумаги, поднимая спрос и создавая иллюзию прибыльности. Отечественные решения, по мнению экспертов, обеспечивают полный вертикальный контроль, обучаются на российской отчетности и позволяют разворачивать модель внутри контура банка. Регулирование, вероятно, коснется «паспорта ИИ-модели» и требований к прозрачности. **Продажу prepaid SIM-карт могут запретить в рамках «Антифрода 3.0»** Минцифры разрабатывает законопроект в рамках «Антифрода 3.0», который предполагает запрет на продажу SIM-карт со стартовым балансом. В проекте поправок к Закону «О связи» говорится, что операторы не смогут зачислять деньги на лицевой счет до заключения договора с пользователем. Сейчас мошенники часто дистанционно оформляют SIM-карты с prepaid-пакетом, используют их для доступа к аккаунтам (например, на «Госуслугах»), совершают противоправные действия и быстро избавляются от номера. Это затрудняет их поиск и привлечение к ответственности. Если поправки примут, пользователи смогут активировать номер только после заключения договора и самостоятельного пополнения баланса. Это создаст цифровой след — через банковский платеж, — который поможет установить личность владельца. В Минцифры подтвердили обсуждение обязанности продавать SIM-карты с нулевым балансом.

Социальная инженерия и дипфейки. Нападение и защита с помощью ИИ

В кулуарах форума «Кибербезопасность в финансах» мы беседовали с Алексеем Лужновым, руководителем BI.ZONE AntiFraud, о ключевых трендах в сфере кибербезопасности и борьбы с мошенничеством.

Алексей Лужнов



ПЛАС: Итак, вы возглавляете адаптивную кросс-канальную систему по борьбе с мошенниками BI.ZONE AntiFraud. Ваша специализация, да и само место беседы — Уральский форум «Кибербезопасность в финансах» — все располагает к разговору о текущей ситуации с фродом, трендами и регулированием. Начнем с вашей оценки соотношения стоимости защиты от мошенников и потенциальных рисков в случае реализации обмана.

А. Лужнов: Сегодня мы можем говорить, основываясь на своей статистике, о том, что такое соотношение выглядит как 80:20. Иными словами, если компания выделяет на антифрод бюджет размером порядка 20% от той суммы, которая может потенциально стать ущербом от действий злоумышленников, то это вполне подходящая пропорция для того, чтобы продолжать подобную политику противодействия.

Однако, как только мы выходим на соотношение 50:50, то есть стоимость защиты становится сопоставима с потенциальным ущербом — в силу неизбежно вступаю законы бизнеса. Сегодня такая пропорция встречается редко: современные антифрод-системы эффективно справляются с мошенничеством и остаются экономически оправданными для бизнеса.

Теперь об уровне защищенности. В идеале хотелось бы предотвращать 100% фрода, но на практике это почти невозможно из-за большого объема операций и сложных многоступенчатых схем, которые используют злоумышленники. Антифрод — это поддерживающий сервис или целая система для обеспечения устойчивости бизнеса от атак злоумышленников. Именно поэтому защитные процедуры ни в коем случае не должны способствовать оттоку клиентов, заметно усложняя клиентский путь, замедляя обслуживание и т. п. Необходимо давать соответствующую оценку при внедрении любой антифрод-системы, насколько просто ее использовать самим сотрудникам банка, насколько легко донести ее преимущества для конечных пользователей банковского сектора, и т. п.

На Уральском форуме в рамках панельной дискуссии была озвучена важная мысль: «пользователь пойдет туда, где, как он знает, о нем позаботятся дополнительно». Иными словами, туда, где, когда его попытаются обмануть телефонные мошенники, появится предупреждающая информация о подозрительном абоненте и т. п. Такие сервисы уже есть у банков и телекома.

Что касается финтех: в России уровень цифровизации общества в целом достаточно высокий, поэтому, когда клиенты банка работают с цифровыми сервисами, они им, как правило, доверяют. И у банковской отрасли одна из самых зрелых систем антифрода в стране.

При этом опыт погружения в тематику телефонного мошенничества у наших пользователей пока недостаточный. Банки и регуляторы этим как раз активно сейчас занимаются, стремясь привлечь внимание клиентов к цифровой и финансовой грамотности. В том числе, пользователю нужно обращать внимание на типичные признаки разговора с мошенником, его манеру общения. Такое поведение часто указывает на то, что звонит злоумышленник, а не реальный сотрудник банка или госоргана.

Поэтому обучение, просвещение и повышение осведомленности — это та самая забота о пользователях, которую банки со своей стороны готовы проявлять (и проявляют) уже сейчас.

ПЛАС: Крупные компании по-прежнему общаются с клиентами в цифровых каналах: от SMS до электронных писем. И рядовому пользователю сложно отличить фишинговую рассылку в таком случае, как здесь будет развиваться взаимодействие?

А. Лужнов: Согласен с вами, быстро перестроиться от традиционных каналов взаимодействия с клиентами в полностью цифровое пространство физически невозможно. Это постепенный, в чем-то даже эволюционный процесс.

Но для того чтобы взаимодействовать с клиентами, все равно необходимо искать удаленные каналы связи, чтобы не заставлять — например, возрастную категорию — посещать лишний раз офисы.

Общаясь по горячей линии или в интернет-чате, в мобильном приложении я могу увидеть информацию о том, что запущено обслуживание по моему запросу, убедиться, что я действительно его инициировал, плюс увидеть, с кем я разговариваю и получить дополнительную информацию, которая позволит верифицировать собеседника.

В финансовой отрасли многие банки уже начинают внедрять обратную верификацию, когда в случае общения пользователя с сотрудником банка можно подтвердить личность сотрудника, например, через мобильное приложение.

ПЛАС: Не кажется ли вам, что, когда вопросы ответственности на рынке будут поставлены законодательством более жестко, отношение к антифроду изменится?

А. Лужнов: В целом регулирующие органы в России уже предъявляют повышенные требования к защите, особенно в финансовом секторе. На первом плане сегодня крупные банки, которые обслуживают большую часть населения, они как инициаторы внедряют многие подходы, которые позволят упростить ряд проблемных моментов.

В системном противодействии в стране также критически важна роль операторов связи. Банки видят финансовую часть сценария, операторы сотовой связи — коммуникационную, маркетплейсы — поведение в своих сервисах, регуляторы — правовую и правоохранительную часть. Ключевая задача — видеть атаку еще на этапе коммуникации: в момент звонка, сообщения, перехода по ссылке, появления признаков социальной инженерии или аномального поведения человека, который потенциально вступил в контакт со злоумышленниками. И здесь роль телекома становится ключевой, ведь они первыми видят эти подозрительные контакты.

ПЛАС: Поговорим об Уральском форуме 2026 — что изменилось с точки зрения трендов и акцентов этого мероприятия?

А. Лужнов: Я наблюдаю три основных направления. Первое — это активная работа по противодействию социальной инженерии, которая от нас никуда не ушла. Нужно повышать осведомленность и навыки как россиян, так и отечественного бизнеса в распознавании мошенничества.

Важно уметь включать критическое мышление, когда слышишь «давайте быстрее», когда начинаются угрозы, шантаж, либо появляется риск якобы потерять выгоду, если моментально не отреагируете. Обязательно нужно прерывать разговор, если звучит информация о том, что, если сейчас вы пообщаетесь с кем-то из родственников, получите уголовную статью. Не стоит доверять любому

незнакомому собеседнику по телефону, особенно если он связывается с вами в первый раз.

Еще один тренд форума 2026 года — работа с дипфейками. Есть случаи, когда сотрудникам какой-либо организации, например, бухгалтеру, поступает входящий видеозвонок в мессенджере от первого лица компании. Далее это «лицо» требует срочно провести транзакцию в адрес такого-то юрлица.

Исполнительному сотруднику бывает тяжело воспринимать такие указания с холодной головой, когда он живую видит человека со знакомыми мимикой и голосом.

На что нужно обращать внимание в такой ситуации? Проверить, нет ли уведомлений о том, что это новый контакт в мессенджере, когда он последний раз был в сети и есть ли общие группы в рамках чатов. Можно проверить, был ли у вас ранее диалог с этим пользователем, даже если он представляется официальным лицом, которое должно вызывать доверие.

В любой современной компании есть прямые контакты, куда можно позвонить и уточнить, подтвердить личность человека в мессенджере. Даже если руководитель недоступен, можно через какое-то время повторно связаться по прямой линии для подтверждения. Тем более, что объемы мошеннических транзакций в подобных случаях оказываются достаточно велики.

И, наконец, третий тренд — это рост роли современных технологий в виде систем на базе ИИ и ИИ-агентов для кибербезопасности. Без этих инструментов собирать и анализировать огромные массивы информации сегодня просто невозможно.

Внедрение агентных систем на каждом из этапов сбора информации, актуализация правил выявления мошенничества, — все это заметно снижает время реагирования и повышает точность, а ведь для мошенников время — это всегда деньги.

Как только мы усложняем путь к чужому кошельку, мошенники либо просто теряют интерес к клиенту и переключаются на другого, либо просто прерывают контакт с потенциальной жертвой. Поэтому сегодня скорость выявления и анализа подозрительных действий становится одним из ключевых факторов в борьбе с киберпреступниками.

В этих условиях особую роль начинают играть технологии на базе ИИ. Работа с искусственным интеллектом в плане борьбы с мошенничеством — это то, на чем сейчас надо базировать свои системы. Не забываем, что те же мошенники для формирования дипфейков тоже пользуются специальными сервисами на базе ИИ.

В заключение еще раз отмечу, что в рамках профессионального сообщества необходимо обязательно стремиться к партнерству. Сегодня мошенники, как правило, действуют сразу через несколько каналов. Поэтому эффективное противодействие таким схемам невозможно без совместной работы участников рынка.

ПЛАС

Инвестиции коллекторов в долги микрофинансовых организаций (МФО) сравниваются с банковскими в 2027 году

Инвестиции коллекторов в покупку долгов микрофинансовых организаций сравниваются с тратами на приобретение банковских долгов в 2027 году и составят 26–27 млрд рублей, стало известно из прогноза аналитиков «Эксперт РА».

В 2025 году инвестиции в портфели банковских долгов составили 24 млрд рублей, в портфели МФО — 21 млрд, в 2024-м — 21 и 15 млрд соответственно.

При этом в прошлом году коллекторы заплатили за микрофинансовые и банковские долги сопоставимую сумму, несмотря на трехкратную разницу номинала: объем купленной просрочки банков — 325 млрд рублей, МФО — 113 млрд.



Сбер, ВТБ, Т-Банк и Альфа-Банк готовятся к запуску криптосервисов

Крупнейшие банки в преддверии принятия закона о цифровой валюте начинают формировать соответствующую инфраструктуру. О начале тестовых торгов криптовалютой и планах создания цифрового депозитария заявил Альфа-Банк. Аналогичные планы имеют Сбербанк, ВТБ и Т-Банк.

Альфа-Банк начал тестирование торгов криптовалютой в приложении «Альфа-Инвестиции». Полноценные операции начнутся до конца 2026 года,

после вступления в силу закона «О цифровой валюте и цифровых правах».

Самым сложным элементом является создание цифрового депозитария для хранения и учета цифровых активов.

Согласно законопроекту, его можно трансформировать из оператора информационных систем (ОИС), которые уже имеют крупнейшие банки.

В реестре ЦБ — 24 организации, собственные ОИС есть у Сбербанка, ВТБ, Альфа-Банка, Т-Банка, ПСБ и других. В Альфа-Банке планируют завершить формирование депозитария к концу года.

Для брокеров без собственных ОИС создание депозитария будет сложнее. Интеграция цифровых активов в приложения брокеров в составе банковских групп даст инвестору единое окно и прозрачное налоговое администрирование.

При этом у российских участников ограничен выбор контрагентов. «Перенаправлять клиентов на иностранные биржи — значит сознательно подвергать их повышенным рискам», — отмечают в ВТБ. Замыкание крипторынка внутри России опасно: при резких колебаниях котировок может не хватать ликвидности.

Альфа-Банк запустил оплату по биометрии через универсальный сервис НСПК

Альфа-Банк совместно с Национальной системой платежных карт (НСПК) реализовал оплату по биометрии через универсальный сервис. Теперь клиенты банка могут расплачиваться взглядом не только на терминалах Альфа-Банка, но и на терминалах других банков, поддерживающих сервис.

В банке отмечают, что оплата взглядом занимает меньше времени, чем оплата картой или по QR-коду. Этот способ невозможно подделать или скопировать, а клиенту не нужно носить с собой карту или смартфон.

Подключение уже доступно для клиентов-физлиц в Альфа-Мобайл на Android и в интернет-банке, в ближайшее время планируется запуск на iOS. Для оплаты достаточно выбрать на терминале «Оплата взглядом» и посмотреть в камеру.

При этом сохраняется начисление кешбэка на тех же условиях, что и при оплате картой.

Юридические лица также могут принимать оплату по биометрии на терминалах Альфа-Банка.

Для бизнеса никаких дополнительных затрат не потребуется — операции проходят по стандартным тарифам эквайринга. Банк планирует обеспечить прием оплаты взглядом на 100% своего парка терминалов к концу года.

ЦБ с января 2027 года будет раскрывать данные о структуре собственности финорганизаций в обезличенном виде

Банк России с 1 января 2027 года возвращается к практике публикации сведений о структуре собственности финансовых организаций, но в новом формате — через набор критериев в обезличенном виде, следует из сообщения регулятора.

Обновленный формат коснется банков, НПФ, страховых организаций, управляющих компаний и микрофинансовых компаний. Раскрытие будет происходить по 14 критериям, включая перечень фактов об участниках структуры и сведения о предписаниях из-за неудовлетворительной деловой репутации или финансового положения.

Дополнительная нагрузка на участников рынка не предполагается — регулятор будет формировать структуры самостоятельно с учетом позиции организации. Подход обсуждался и был поддержан рынком. ЦБ считает, что это позволит получать информацию без увеличения санкционных рисков.

Сбер запустил игру-тренажер «Вижу подвох» для защиты от мошенников

Сбер запустил бесплатную онлайн-игру «Вижу подвох», которая помогает пользователям научиться распознавать мошеннические приемы и выбирать безопасную модель поведения.

В игре пользователю предлагают пройти несколько ситуаций, основанных на распространенных мошеннических схемах. Например, получить сообщение от близкого человека с просьбой перейти по ссылке, звонок от курьера с требованием назвать код из СМС или срочное поручение от руководителя, который пишет с нового номера.

В каждом случае необходимо выбрать один из вариантов действий. После ответа тренажер объясняет, в чем заключается мошенническая уловка и как правильно вести себя в подобной ситуации. Такой формат позволяет не просто прочитать правила кибербезопасности, а применить их на практике в комфортной игровой среде.

Перед началом игры пользователь выбирает одного из персонажей. Сценарии учитывают ситуации, с которыми могут столкнуться люди разного возраста: молодежь, взрослые и представители старшего поколения. По итогам прохождения участник получает оценку своих навыков и может обратиться к разделу «Безопасность» в приложении СберБанк Онлайн за дополнительными рекомендациями о том, как защититься от мошенников себя и близких.

Иван Кузьмин, вице-президент — директор департамента данных и рекомендательных систем В2С Сбербанка:

«Мошенники используют множество сценариев для обмана и стараются заставить человека врасплох: торопят, вызывают страх, представляются близкими, сотрудниками банков, государственных организаций или компаний. Знать основные правила безопасности



важно, но еще полезнее заранее потренироваться применять их в ситуации, приближенной к реальной.

Именно поэтому мы выбрали игровой формат. Он помогает спокойно разбирать разные схемы, увидеть возможные ловушки и понять, какое действие будет безопасным. Первые результаты показывают, что такой подход востребован: игру уже прошли тысячи пользователей, оставивших оценку, отозвались о ней положительно. Особенно ценно, что люди не только благодарят за тренажер, но и предлагают новые ситуации, которые стоит в него добавить».

ЦБ предлагает запретить подросткам самостоятельно регистрировать электронные кошельки

Центробанк прорабатывает запрет на самостоятельную регистрацию электронных кошельков для подростков от 14 до 18 лет — инициатива включена в третий антимошеннический пакет «Антифрод 3.0». Минцифры направило документ на межведомственное согласование.

Регулятор хочет распространить на электронные средства платежа правило, уже действующее для банковских счетов: с августа 2025 года открыть счет и получить карту несовершеннолетний может лишь с письменного согласия родителей. Под новые ограничения могут попасть не только классические кошельки, но и встроенные платежные функции маркетплейсов, игровых платформ и месенджеров.

ВТБ присоединился к Кодексу этики ИИ Банка России

ВТБ подписал меморандум о присоединении к Кодексу этики в сфере разработки и применения искусственного интеллекта на финансовом рынке. Документ разработан Банком России и носит рекомендательный характер.

Основная цель документа ЦБ — повысить доверие клиентов к использованию ИИ банками и стимулировать развитие технологии на финансовом рынке, одновременно снижая риски, связанные с ее разработкой и применением. Присоединение к Кодексу также означает готовность ВТБ делиться опытом использования ИИ с другими участниками рынка и участвовать в выработке отраслевых стандартов.

Кодекс ЦБ рекомендует банкам информировать клиентов о рисках, связанных с применением ИИ, в ряде случаев предоставлять клиентам возможность отказаться от взаимодействия с ИИ, а также ряд других мер, чтобы сделать применение технологии более прозрачным и человекоцентричным. В дальнейшем положения кодекса будут учитываться при внедрении и использовании ИИ-технологий в работе банка.

Московская биржа внедряет ИИ для борьбы с «серыми» схемами и инсайдом

Московская биржа внедряет ИИ-алгоритмы как дополнительный аналитический слой комплаенса. Системы будут искать аномалии в торговом поведении и помогать быстрее выявлять возможные манипуляции и злоупотребление инсайдом.

Решения не блокируют сделки автоматически — они лишь отбирают кейсы для последующей проверки специалистами.

Для рынка это означает усиление контроля и снижение возможностей для «серых» схем — паттернов, которые раньше было проще маскировать.

Венчур и таланты — главный капитал XXI века. Почему Узбекистану нужно спешить

Как построить результативную венчурную экосистему? Чем может помочь Узбекистану опыт таких лидеров данного направления, как США, Израиль, ОАЭ и Китай? Как благодаря венчурным инвестициям достичь конкурентного преимущества в инновациях? Об этом журнал «ПЛАС» беседует с основателем и управляющим партнером R136 Ventures, инвестором Кремниевой долины Виктором Орловским, который в качестве специального гостя принял активное участие в Международном ПЛАС-Форуме Digital Uzbekistan.



Виктор Орловский

ПЛАС: Начнем с простого, но очень важного для понимания темы нашей беседы вопроса — а зачем вообще Узбекистану становиться международным хабом для венчурного капитала?

В. Орловский: Капитал в нашем мире обладает особой текучестью и постоянно движется туда, где условия лучше. За последние 20 лет перетекать капиталу стало тяжелее, потому что появилось больше ограничений. Тем не менее, любой капитал — и человеческий, и финансовый — остается достаточно ликвидным. При этом венчурный капитал в силу своей специфики ориентирован на постоянный рост. И расти ему нужно очень быстро и эффективно.

Ярким примером здесь являются США. По данным Национальной ассоциации венчурного капитала (National Venture Capital Association) в 2023 году в США насчитывалось около 3,4 тыс. активных венчурных структур, а совокупный объем средств, которыми они управляют (AUM — assets under management), по состоянию на 2025 год составил всего примерно 1,25 трлн долларов. Для сравнения — активы под управлением BlackRock — одной из крупнейших инвестиционных компаний — достигли 13,9 трлн долларов (!) в первом квартале 2026 года. Иными словами, они превышают совокупные капиталы всех венчурных фондов, которые инвестируют в экономику США.

Если же посмотреть на венчурный бизнес в целом, можно увидеть, что все семь самых крупных компаний в мире, т. н. «Великолепная семерка»: Apple, Microsoft, Amazon, Alphabet, Meta, Nvidia и Tesla — были созданы при непосредственном участии венчурного капитала. Это же справедливо и в отношении недавно вышедшего на биржевой рынок SpaceX и двух ключевых игроков в сфере искусственного интеллекта: OpenAI и Anthropic.

Итак, как можно убедиться, венчурный рынок очень небольшой по размеру, но является ключевым движком множества других рынков. И он предполагает стремительный рост. Потому что кредитные деньги и иное подобное финансирование заточены на медленный рост, а венчурная экосистема — основа стремительного роста экономики.

Именно поэтому, если экономика хочет активно развиваться, ей нужны венчурные деньги. Да, это всегда очень большой риск, непредсказуемость, но, в конце концов, все инновации в мире — это риск и непредсказуемость.

Итак, я возвращаюсь к вашему вопросу: «Зачем Узбекистану становиться венчурным хабом?». Или, перефразируя, «Зачем этой центрально-азиатской стране развивать инновационную экономику?». Ответ очевиден — чтобы расти и становиться конкурентоспособным рынком, чтобы бизнесы становились более глобальными, а таланты развивали свой потенциал. Достаточно посмо-

треть на стремительный рост ОАЭ или на то, как трансформировался за последние пару десятилетий Китай, чтобы понять, что может принести валовый рост экономики на 10–20% в год.

ПЛАС: Вы привели в качестве примера использование венчурного капитала в США, Китае, Израиле. Почему именно эти страны интересны и перспективны как базовые площадки для развития рынков венчурного капитала — в чем их секреты?

В. Орловский: Что касается США, то здесь все очень просто: венчурный капитал — это прежде всего изобретение игроков из Кремниевой долины. Он появился там еще в середине 60-х годов прошлого века. И появился отнюдь не на пустом месте. За относительно короткий промежуток времени там стало возможно вырастить компанию из очень маленькой, крошечной (в несколько человек) команды до гигантской международной корпорации.

Экономика стала ускоряться, когда появились компьютеры, т. е. первые кремниевые чипы. Образовались компании, которые смогли очень быстро масштабировать собственный бизнес. Почему? Во-первых, если вы сделали хороший чип, то сначала вы его долго проектировали, создавали, но потом очень быстро запустили в серийное производство. Поэтому компании, такие как Intel, стали очень быстро расти.

Во-вторых, появились бизнесмены, которые поняли, что на этом можно очень быстро заработать, и стали давать деньги таким стартапам. Так и появился новый тип капитала.

Потом появилось программное обеспечение. И оказалось, что создание ПО имеет гораздо более высокий потенциал, чем производство и поставка чипов. Потому что тиражирование ПО — это еще более простой и быстро масштабируемый бизнес.

Сначала венчурный капитал, привлекаемый в Кремниевую долину, был невелик. Потому что имелось еще очень мало областей, где были нужны программное обеспечение и чипы. Но очень скоро все изменилось. Вспомним фразу, которую произнес американский инженер, инвестор и предприниматель Марк Андрессен в 2011 году: «Software is eating the world» («Программное обеспечение поедает мир»). Таким образом, он сформулировал идею о том, что программное обеспечение перестает быть просто инструментом и становится фундаментальным ресурсом, который перестраивает экономику и трансформирует практически все отрасли. Программные продукты стали определять, как создается ценность, как компания зарабатывает и в чем ее конкурентное преимущество.

Вот именно туда и стали поступать венчурные деньги. И сейчас Tesla — это практически компьютер на колесах. Спутник, который запускает Илон Маск, — это космический компьютер. В спутниках Starlink стоят специали-

зированные чипы AMD Versal AI Core. И т. д., и т. п. Везде работает программное обеспечение. Так использовали и используют венчурный капитал в США.

Вторая страна в мире, где венчурный капитал тоже оказался очень востребован, это, конечно же, Китай. Но там работает в большей степени государственный капитал. Вот вам пример: две мощнейшие экономики в мире, куда поступали и поступают венчурные деньги. В США это в большей степени частный капитал, в Китае — государственный. Да, и государство, как ни странно, иногда тоже может заниматься венчурным инвестированием, но делает это опосредованно, через какие-либо структуры.

Во всем остальном мире венчурный капитал значительно меньше вовлечен в экономику, чем в США и в Китае.

Однако необходимо сказать несколько слов и про Израиль. Эта маленькая страна активно использует венчурное финансирование. Процент венчурных стартапов и компаний в экономике там очень высок. И именно Израиль, на мой взгляд, является примером для Узбекистана. Данный опыт показывает, что стать венчурными экономиками способны не только огромные государства, такие как США и Китай, но и страна масштаба Израиля.

Самый главный ресурс — это таланты. Это то, за чем приходит венчурный капитал. Так случилось, что в Израиле благодаря приезду значительного количества очень талантливых инженеров из Советского Союза появились идеальные условия для возникновения результативных фаундеров, после чего началось проникновение туда венчурного капитала. И сейчас израильтяне занимают третью строчку в мире по количеству стартапов-единорогов, то есть достигших оценки в 1 млрд долларов.

Стране, которая хочет развивать экономику активно, нужно завозить и выращивать таланты. Надо создавать условия для того, чтобы туда пришел венчурный капитал. Для этого нужны свободные экономические зоны. Поэтому стартаперы Узбекистана должны комфортно работать, открывать новые бизнесы и привлекать специалистов из-за рубежа.

Узбекистан сегодня потрясюще позиционирован. Это страна, где проживает огромное количество молодых людей, очень низкий средний возраст населения, очень высокая рождаемость. Стартаперов всегда больше среди молодых. Но требуется хорошее обучение. Хорошие школы, в основном математические, продвинутые вузы. Нужна компьютеризация, большие вычислительные мощности, которые эти стартапы смогут использовать.

Также нужно поощрять своих стартаперов к выезду за границы Узбекистана. Да-да, тот же Израиль построен как раз на том, что часть фаундеров уезжает из страны, они создают собственные хабы в США, там, где большой рынок, или же в Европе, а также в Азии. Рынок Израиля очень мал, более того, его почти нет. Поэтому израильские стартапы стремятся сразу стать международными компания-

ми. Но после успешной международной экспансии они везут привлеченные средства назад в Израиль, где нанимают инженеров и других квалифицированных сотрудников. Эти сотрудники взрослеют, набираются опыта, и многие из них со временем сами становятся предпринимателями. Именно так работает эта схема.

Предпринимательство, особенно стартаперское, — штука заразная. И если у вас есть компания, в которой работают четыре инженера, а потом их стало 40, а еще позже — 400 или 4000, то будьте уверены: из 4000 инженеров получится 40 хороших бизнесменов, которые поймут, как на самом деле можно делать бизнес, пойдут и создадут 40 стартапов. Естественно, 30 из них обанкротятся, но 10 смогут сделать хороший бизнес, а 3–5 достигнут очень высоких результатов.

Таким образом, венчурная экономика строится и на людях, и на опыте. И это то, что сейчас следует делать Узбекистану, — строить такую экосистему, привлекать таланты и, благодаря им, венчурный капитал.

ПЛАС: Если говорить об Узбекистане, о роли регуляторной политики, стимулирующей деятельность государства — что уже делается в этом направлении в стране? И что должно быть сделано, на ваш экспертный взгляд, в самое ближайшее время?

В. Орловский: Насколько я вижу, делается очень многое. Во-первых, в июне 2026 года стартовало строительство IT-парка, в котором участвуют, в том числе, инвесторы из Китая. Это государственная инициатива по развитию IT-сферы Узбекистана.

Во-вторых, государство вводит удобные налоговые режимы. Есть хороший прогресс в том, чтобы стартаперы из разных стран, не только из ближнего зарубежья, но и из дальнего, смогли получить долгосрочные визы, закрепиться и комфортно жить в стране. Создается инфраструктура. Ташкент — современный, безопасный, комфортный для проживания город, который становится все более привлекательным. Это тоже важно для специалистов, которые приезжают издалека. Напоминаю — нужно привозить в страну таланты.

Жизненно важно создавать условия для того, чтобы венчурный капитал стремился в страну. Например, узбекские банки, страховые компании сегодня не могут эффективно инвестировать деньги в венчурные фонды. Напомню, в США банки и страховые компании — это главные доноры венчурного бизнеса, в Китае же главный донор — это государство. Но появление иных профессиональных игроков тоже очень важно.

Например, я не сторонник того, чтобы корпорации занимались венчурным инвестированием. В США был опыт, когда автомобильные и нефтяные компании пытались самостоятельно создавать венчурные фонды. Ничего хорошего из этого не получилось. Эра корпоративных венчурных фондов подходит к концу, и корпорациям

выгоднее отдавать деньги в управление профессиональным венчурным фондам.

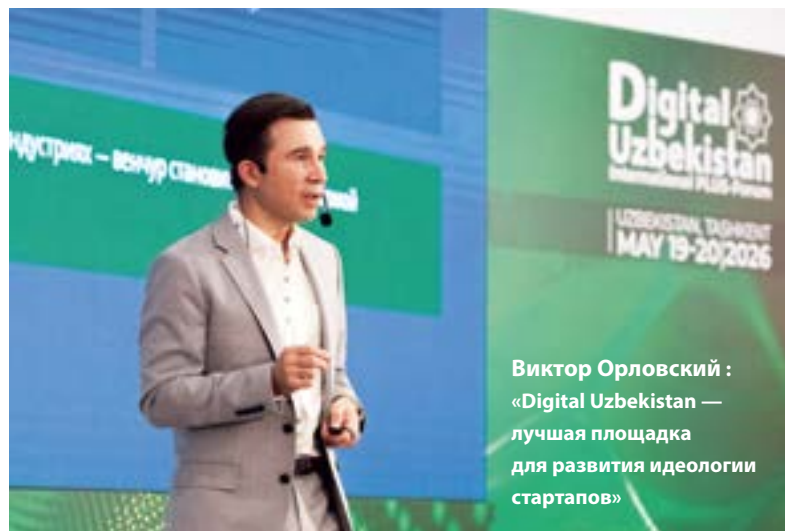
В США таких фондов очень много, например, R136 Ventures и другие, а в Узбекистане их нет совсем. Поэтому необходимо наладить переток денег от больших корпораций, в особенности банков и страховых компаний, пенсионных фондов, в хорошо управляемые венчурные фонды. Это как раз та задача, которую Узбекистан должен решать прямо сейчас. Ее решение также поможет становлению узбекских стартапов.

Например, в Казахстане уже есть удачный проект Higgsfield, он базируется в Алматы, и его оценивают в 5 млрд долларов. Это ИИ-стартап, который создает платформу для генерации видео, которая позволяет превращать текст в ролики с помощью нейросетей. Его создали Ерзат Дулат (инженер и исследователь в области ИИ из Казахстана) и Алекс Машрабов (бывший руководитель направления генеративного ИИ в Snap), который работал в Кремниевой долине. Важно выращивать и привлекать со стороны таких талантливых людей. И это — тоже одна из первоочередных задач Узбекистана.

ПЛАС: В мае 2026 года вы принимали участие в одном из знаковых мероприятий финансовой сферы Центральной Азии — в Международном ПЛАС-Форуме Digital Uzbekistan. Как, по вашему мнению, влияют такие площадки на развитие экономики стран региона?

В. Орловский: Я впервые был участником этого мероприятия и хочу отметить, что Digital Uzbekistan — это замечательная платформа для обмена мнениями, для того чтобы корпорации, стартаперы, инвесторы могли результативно общаться. Общение — залог взаимопонимания, способ найти интересных партнеров и эффективные точки роста.

Узбекистан славен своим гостеприимством и высокой толерантностью к разным культурам, разным человеческим ценностям. Страна создает все условия для



Виктор Орловский :
«Digital Uzbekistan —
лучшая площадка
для развития идеологии
стартапов»

того, чтобы деловое общение было конструктивным и взаимодополняющим.

Уверен, что ПЛАС-Форум Digital Uzbekistan будет год от года только расширяться. Почему Кремниевая долина так быстро дала результаты в сфере венчурной экономики? Там очень высокая, в отличие от многих других аналогичных площадок, скорость взаимодействия людей между собой. Там можно зайти в кафе попить кофе, а выйти с бизнес-идеей и даже с новым бизнес-партнером.

Я вижу высокий потенциал, которым обладает ПЛАС-Форум Digital Uzbekistan, и нужно продолжать его развивать, достигать все более высокой скорости обмена мнениями, информацией, создания новых ценностей. Масштаб мероприятия и количество профессионалов рынка впечатляют, на Форум можно прийти не просто с идеей, а с решением и найти здесь единомышленников. ПЛАС-Форум Digital Uzbekistan — это площадка, которая реально способствует развитию экономики Узбекистана и стран Центральной Азии.

ПЛАС: В ходе второго дня ПЛАС-Форума Digital Uzbekistan вы приняли участие в сессии уникального формата — Start-up Elevator's pitch. Поделитесь своими впечатлениями от живого общения с представителями стартапов Узбекистана — что у них уже есть для успеха, а чего не хватает? В частности, вы говорили о такой типичной ошибке, как ориентация исключительно на локальный рынок республики, — как, на ваш взгляд, ее исправить?

В. Орловский: Во-первых, меня очень порадовали состав и проекты стартапов, которые были представлены на Start-up Elevator's pitch в рамках ПЛАС-Форума Digital Uzbekistan. Видно было, что отобрали лучших, и они показали себя очень достойно.

Во-вторых, нужно понимать, что амбиции — это двигатель любого бизнеса. И я уверен, что стартаперам в Узбекистане надо сразу думать о том, чтобы строить прежде всего большой международный бизнес, а не локальный — ориентированный только на рынок Узбекистана. Молодым бизнесменам нужно максимально сосредоточиться на тех проектах, которые они продвигают. Это то, что по-английски называется full-time job — полноценная работа, а не факультатив. Это вопрос выживания стартапа. Такой подход помогает глубже погрузиться в понимание проблематики. На мой взгляд, стартаперы должны быть влюблены не в свои решения, а в проблему. Именно искренняя любовь и проникновение в проблему, в ее суть, дают потом хорошее решение. Уверен, стартаперы в Узбекистане поймут меня и станут еще более пристально анализировать свою работу.

ПЛАС: На еще одном знаковом событии Digital Uzbekistan 2026 — закрытом бизнес-завтраке «Развитие безналичных платежей. Достижения, итоги

и план» для топ-менеджеров банков, национальных и международных платежных систем, маркетплейсов и торгового ритейла — вы заявили о необходимости создания фонда венчурного финансирования для стран Центральной Азии. Поделитесь, пожалуйста, деталями этой инициативы.

В. Орловский: Мы сейчас прорабатываем возможности для создания такого фонда, но пока не можем публично раскрывать детали. Могу лишь сказать, что в рамках этого фонда хотелось бы создать небольшой, но значимый для всего региона Центральной Азии инвестиционный пул, который поможет привлекать средства в стартапы, обеспечивая им в дальнейшем выход на международный рынок, прежде всего на рынок США. Надеюсь, мы найдем интересные компании, которым сможем помочь не только деньгами, но и нашим опытом, чтобы привезти их в США и помочь развиваться на том рынке, где они смогут действительно очень сильно вырасти. И, кстати, это поможет Узбекистану стать именно инновационной экономикой.

Как я уже говорил, даже такая небольшая страна, как Израиль, смогла стать большой венчурной экономикой.

Рынок Узбекистана также невелик. Поэтому наша задача вырастить здесь единорогов с фаундерами. Подспорьем для этого станет израильский фонд, куда мы обычно инвестируем, с небольшой, но существенной локацией для регионов Центральной Азии. Надеюсь, у нас все получится, но больше деталей, к сожалению, раскрыть пока не могу.

Я уверен, Узбекистану нужно поторопиться с подобными инициативами, поскольку в мире существует высококонкурентное окружение, и велик риск опоздать, не получив того эффекта, который изначально заложен в потенциале данного региона. Я не считаю, что Узбекистан может конкурировать за лидерство в венчурном бизнесе с США или Китаем. Но эта страна может стать заметным региональным хабом. Уточню, что под регионом в данном случае я понимаю достаточно большую территорию — от Турции до Египта, Индии и Пакистана.

Узбекистан всегда был в центре Шелкового пути, на пересечении торговых маршрутов. Здесь всегда существовал уникальный сплав культур и традиций: местной, славянской, турецкой, арабской. Эти сферы очень тесно объединены историческими, культурными и экономическими связями, что дает стране целый ряд преимуществ. В первом квартале 2026 года рост экономики Узбекистана ускорился до 8,7% год к году. Если экономика будет расти хотя бы 5–7 лет такими темпами, мы увидим колоссальный прирост экономического потенциала страны. Через 10 лет Узбекистан может стать региональным лидером. Главное — заявить о себе на инновационном поприще с помощью венчурных фондов и талантливых стартаперов. Но делать это необходимо уже сейчас.

ПЛАС

Финтех-парадоксы Центральной Азии. Почему взрывной рост упирается в инфраструктурный потолок



Антон Устинов

В Узбекистане сейчас очень быстро развиваются цифровые платежи. Потребители массово переходят на безналичные расчеты, а приложения вроде Click, Payme и Uzum пользуются почти все. Но при этом рынок столкнулся с серьезной проблемой: инфраструктура перестала успевать за стремительным ростом сервисов. Банковские приложения пока не могут полноценно конкурировать за клиентов, а крупным экосистемам не хватает единых технических стандартов для масштабирования. О причинах журналу «ПЛАС» рассказал СТО & Enterprise FinTech Системный Архитектор, Exante Антон Устинов.

Центральная Азия как альтернативная модель развития финтеха

У Центральной Азии свой путь развития финансовых технологий, который отличается от привычных западных моделей. В США и Европе все строилось вокруг банков и карточных систем. В России банки сами создали огромные экосистемы, где в одном приложении собрано все, от переводов до покупок.

В свою очередь в Казахстане появился уникальный пример в лице Kaspi.kz, который фактически объединил в себе весь путь до покупателя.

У Узбекистана — еще один сценарий. Здесь население изначально начало активно пользоваться не столько банковскими продуктами, сколько независимыми платежными сервисами, такими как Click и Payme. Эти приложения не зависели от конкретного банка, позволяли добавлять любые карты и предлагали понятный интерфейс для переводов и оплаты услуг. В итоге платежные сервисы заняли рынок быстрее, чем традиционные банки успели отреагировать.

К 2024 году уже около половины населения республики пользовалось цифровыми финансами, а количество безналичных платежей росло очень быстро.

Но за быстрым успехом обнаружилась серьезная проблема. Техническая база часто не справлялась с таким наплывом пользователей. Национальные процессинговые системы, банковские системы дистанционного обслуживания начинали падать в дни выдачи зарплат или во время крупных акций. Если человек не может отправить деньги в нужный момент, он моментально теряет доверие к приложению. Вернуть это доверие потом очень сложно, какие бы бюджеты ни тратились на рекламу.

Финтех — это не только красивая картинка на экране телефона. За каждым действием стоит сложная техническая система, которая должна работать без сбоев в любое время. Когда количество пользователей исчисляется миллионами, надежность инфраструктуры превращается из технической задачи в вопрос выживания бизнеса.

В этом и состоит главная сложность текущей ситуации в Узбекистане. Платежные услуги развились быстрее, чем инфраструктурные технические мощности, которые должны их поддерживать. Получилось так, что быстрый успех на старте теперь стал барьером для дальнейшего развития рынка.

Уникальная архитектура: феномен двух национальных платежных систем

Обычно на страновых рынках либо работает одна национальная платежная система, либо рынок полностью занимают международные игроки. Узбекистан в этом плане стал исключением.

Как сложилась двойная система

Сначала в 2014 году банки запустили UZCARD как коммерческий проект, и к 2018 году через него проходила почти вся местная оплата. Затем Центральный банк создал еще одну систему — HUMO. Она была государственной и предназначалась в первую очередь для выплаты пенсий, пособий и зарплат бюджетникам. Прежнюю систему сворачивать не стали, поэтому сейчас в стране работают два параллельных платежных контура.

На 1 мая 2026 года, по информации Центрального банка РУз, в обращении находилось 72,7 млн банковских карт. Основную массу эмиссии по-прежнему обеспечи-

вают две национальные платежные системы — UZCARD и HUMO (на конец 2025 года на них приходилось около 25 млн и 17 млн карт соответственно). Многие пользователи держат карты обеих систем — таких клиентов 35–40%. Годовой оборот по национальным процессингам по итогам 2025 года превысил 350 трлн сумов (29,1 млрд долларов США), а доля безналичных платежей в розничном обороте приблизилась к 55%. Только за январь–апрель 2026 года через платежные терминалы прошло 177,5 трлн сумов (14,78 млрд долларов США) — это больше, чем за тот же период годом ранее, и подтверждает, что рынок продолжает расти опережающими темпами. (Информация из источника: Центральный банк РУз, «Информация о банковских пластиковых картах, терминалах, банкоматах и инфокиосках в обращении по состоянию на 1 мая 2026 года, а также поступлениях через платежные терминалы в течение января–апреля 2026 года»).

Технические и операционные издержки двойной системы

Когда рынок переходит от простых платежей к полноценным платформам, устаревшая архитектура начинает мешать.

Во-первых, это сильно усложняет интеграцию. Чтобы финтех-сервис поддерживал карты обеих систем, нужно дважды проходить сертификацию, настраивать два разных API и проводить тесты в двух разных контурах. Для небольшой компании это лишние полгода-год работы и дополнительные расходы.

Во-вторых, задерживается запуск глобальных сервисов. Apple Pay и Google Pay до сих пор не присутствуют в Узбекистане. Причина в регуляторных правилах Узбекистана — только в марте 2026-го внесены изменения в Закон «О персональных данных», которые снимают ограничения для внешних платежных систем.

«Двойная» система UZCARD и HUMO помогла стране быстро развить безналичные платежи. Но теперь эта же структура создает ограничения. Для современных финансовых сервисов важнее не конкуренция между двумя процессингами, а возможность работать через единый стандарт и общие протоколы данных.

Финтех-платформы становятся новыми экосистемами

Финтех-платформы постепенно превращаются в полноценные экосистемы. Еще лет пять-семь назад Click или Payme использовались в основном как удобные способы оплатить мобильную связь или интернет. Сегодня это уже не просто приложения для платежей,

а огромные платформы, которые охватывают почти все стороны жизни.

Этот путь напоминает развитие крупных зарубежных сервисов вроде Alipay. Например, Uzum с самого начала задумывался как экосистема: в нее вошли маркетплейс, логистика, собственный банк, рассрочка, кредиты, страхование и программы лояльности. Click тоже прошел большой путь: от оплаты коммунальных услуг до денежных переводов, инвестиций и даже доступа к государственным услугам. Другие игроки, такие как Payme, Apelsin или Oson, тоже постоянно добавляют новые функции — от доставки еды до покупки билетов.

Обычно такие сервисы развиваются по одной схеме: сначала это просто платежи и переводы, потом добавляется продажа товаров, рассрочка, кредиты и разные дополнительные услуги для жизни.

Количество людей, которые пользуются популярными финтех-сервисами, уже почти сравнялось с числом всех работающих жителей страны. При этом ежемесячная аудитория самого крупного банковского приложения в разы меньше, чем у ведущих небанковских платформ. Большинство розничных цифровых плате-

жей сейчас проходит именно через финтех, а банки все чаще остаются в тени, выполняя роль простой технической базы для расчетов.

Для банков ситуация сейчас складывается двоякая. Крупные государственные банки все больше уходят в тень и становятся просто технической опорой: они хранят деньги и отвечают за безопасность, но с самими клиентами почти не контактируют. Вся информация о покупках и предпочтениях людей

остается у торговых площадок, а банки видят только итоговые суммы.

При этом коммерческие банки выбирают другой путь. Они стараются сохранить прямой контакт с пользователем, развивают свои приложения и предлагают сервисы в обход крупных платформ. В итоге борьба идет уже не просто за выдачу зарплатных карт, а за то, кто будет сопровождать клиента на каждом шагу. Стратегии у всех разные, и каждый игрок пытается занять свое место в этой новой схеме.

Инфраструктурный потолок: почему экосистемам становится сложно расти

Казалось бы, при такой скорости развития рынок должен расширяться бесконечно. Но как только платформы начали предлагать сложные финансовые услуги, они столкнулись с тремя серьезными проблемами.

Во-первых, это разрозненность API. Сейчас каждый банк и каждая платформа вынуждены настраивать связь

друг с другом индивидуально. Единого стандарта обмена данными в индустрии просто нет. Пока участников мало, это еще как-то работает. Но когда их десятки, создание каждой новой связи растягивается на месяцы, а расходы на поддержку растут слишком быстро.

Во-вторых, мешает «двойная» платежная архитектура. Как уже упоминалось, любому необанку или финтех-проекту придется отдельно подключаться и к UZCARD, и к HUMO.

Главная проблема здесь не столько в самой сертификации, сколько в том, что процессинги не предоставляют единого стандартного интерфейса (ISO), а вместо этого выставляют собственные API middleware. Это означает, что разработчикам приходится поддерживать два совершенно разных API, с разной логикой запросов и обработки ошибок.

Ситуацию усугубляет то, что еще пару лет назад у этих процессингов не было полноценных STAGE-стендов, где версия API совпадала бы с боевым контуром, — тестирование превращалось в лотерею. Из-за этого запуск новых проектов обходится дороже, а рост уже существующих идет медленнее.

Сценарии: от простых платежей к открытым финансам

Финтех в Узбекистане уже прошел этапы простых платежей, массовых мобильных сервисов и создания экосистем. Сейчас рынок стоит на пороге перехода к концепции Открытых финансов (Open Finance), когда данные клиента могут свободно, но безопасно передаваться между разными компаниями с его согласия.

Этому мешают два барьера. Во-первых, нет закона, который обязал бы банки открывать свои API для других (как это сделано в Европе). Сейчас у банков нет никаких обязательств делиться данными через открытые интерфейсы — регулятор этого не требует. Обсуждение стратегии развития финтеха на 2026–2030 годы только начнется, и пока это просто общая концепция, а не закон.

Во-вторых, сами крупные экосистемы по понятным причинам не хотят делиться данными с конкурентами, предпочитая держать пользователей внутри своих закрытых систем.

Раньше разговоры об Open Finance в Узбекистане больше напоминали гадания на кофейной гуще. Было неясно, нужен ли он вообще, когда его ждать и кто возьмет на себя роль главного архитектора. Теперь неопределенности стало меньше. Постановление Президента РУз, принятое в конце 2025 года, установило четкий срок: инфраструктура открытого банкинга должна заработать до 1 сентября 2026 года. Власти официально утвердили переход на открытые API и безопасный обмен данными между банками и финтехом. Для этого при Центральном банке создали два инструмента: венчурный фонд на 50 млн долларов и инновационный хаб.

Однако здесь важно учитывать очень тонкий момент: законов, регулирующих этот процесс, пока нет, как нет и самой инфраструктуры. Фактически указанный срок остается ориентировочным, и совсем не факт, что к 1 сентября 2026 года все элементы заработают в полном объеме.

Сейчас дискуссия перешла из плоскости сомнений в практическую сторону. Основной вопрос теперь не в том, запустят ли проект, а в том, как именно это сделают.

Сценарии развития Open Finance в Узбекистане

Инерционный сценарий

К жесткому дедлайну 1 сентября 2026 года инфраструктура открытого банкинга запускается... но только на бумаге. Поскольку детальных технических стандартов и разъяснений от Центрального банка к этому моменту, вероятнее всего, не появится, банки открывают «номинальные» открытые API с урезанным функционалом, чтобы просто избежать штрафов. Реальный обмен данными не происходит, а сам процесс скатывается в привычное для региона русло: долгое согласование каждого регламента и затяжные обсуждения в рабочих группах. Открытые финансы превращаются в проект, который «запустили», но забыли дать к нему рабочую инструкцию.

«Асимметричный финтех» (Экосистемное лобби)

Пока регулятор медлит с разъяснениями, а крупные неповоротливые банки ждут официальных циркуляров, лидеры рынка берут инициативу в свои руки. Крупные частные экосистемы и коммерческие банки не ждут инструкций сверху, а начинают строить двусторонние интеграционные API по собственным стандартам. Рынок монополизируется: гиганты создают свой «закрытый клуб» обмена данными, а мелкие финтех-стартапы остаются за бортом, так как у них нет ресурсов годами ждать, пока Центральный банк стандартизирует API для всех остальных.

«Регуляторный долгострой» (Оптимистичный, но медленный сценарий)

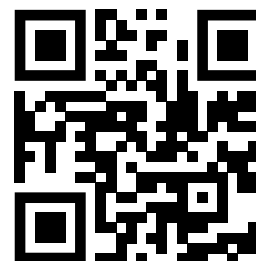
Центральный банк через свой новый Инновационный хаб и венчурный фонд на 50 млн долларов начинает планомерно дожимать рынок. Появляются четкие стандарты, похожие на европейский PSD2. Однако реальное внедрение растягивается на 2–3 года (до 2028–2029 гг.). Причина — технологический долг самих банков. Выясняется, что legacy-системы и монопольные «коробки» локальных АБС физически не способны отдавать данные по API в режиме реального времени без риска «уронить» весь банк. Итак, рынок переходит на открытые рельсы, но со скоростью самого медленного поезда. ПЛАС

Международный ПЛАС-Форум Digital Uzbekistan

Digital
Uzbekistan
International PLUS-Forum

UZBEKISTAN, TASHKENT
MAY 26-27|2027

26–27 мая 2027,
Ташкент — 7-й раз
главная цифровая
площадка региона.
Банкинг, финтех,
e-commerce,
криптоиндустрия.
Будьте среди тех, кто
формирует цифровое
будущее Узбекистана!



2600+
участников

100+
спонсоров

130+
спикеров

AZIMUT Grand Hotel Tashkent, Узбекистан

Крипта в законе. Обзор ситуации с регулированием цифровых активов в разных странах мира

По каким принципам в разных странах и регионах мира государство работает с цифровыми активами и что новые нормы регулирования означают для участников рынка — в своем обзоре делится **Алёна Нариниани**, эксперт в сфере цифровых активов, генеральный директор Агентства независимой журналистики (АНЖ).



За последние годы многие потребители, компании и даже целые страны по всему миру стали использовать криптовалюту как полноценный платежный инструмент: где-то биткоином можно расплатиться за кофе, а где-то цифровые активы используются для трансграничных расчетов с зарубежными партнерами. Государство относится к криптовалюте по-разному: одни страны легализуют ее, другие — оставляют вне правового поля. Попробуем разобраться, почему власть активно стремится регулировать эту сферу и как это происходит в разных странах.

Если еще несколько лет назад на разных уровнях власти активно велись разговоры на тему «разрешать или запрещать крипту», то сегодня вопрос уже ставится иначе: что может сделать государство, чтобы максимально эффективно контролировать движение средств между криптоэкономикой и фиатной системой. Тот факт, что цифровые активы уже стали неотъемлемой частью нашей жизни, признают все страны, и, откровенно говоря, все хотят в той или иной степени регулировать эту область. Последнее понятно, во-первых, сам рынок цифровых активов постоянно растет — увеличиваются объемы транзакций, число пользователей и роль криптоактивов в трансграничных расчетах.

Во-вторых, усиливается внимание к вопросам AML/CFT — крипта остается инструментом, который может использоваться для обхода санкций и сокрытия происхождения средств.

В-третьих, криптовалюты уже напрямую конкурируют с банковской инфраструктурой (что особенно заметно в сегменте стейблкоинов, которые начинают выполнять функции платежного инструмента и хранения ликвидности), и, наконец, государства стремятся вернуть рынок в ту плоскость, где деятельность всех участников прозрачна, а с каждой транзакции уплачиваются налоги.

Поэтому тренд 2026 года — это уже далеко не борьба с криптой, а ее институционализация через лицензирование и прозрачность. Это заметно и в Европе, и в ОАЭ, и в США, и в странах СНГ и ЕАЭС.

Как именно государства регулируют крипту?

Несмотря на общий тренд к легализации через контроль, страны подходят к регулированию по-разному. Сегодня можно выделить несколько устойчивых моделей, которые используются разными странами.

Первая — либерально-лицензионная. В ее рамках криптовалюта разрешена, но доступ к рынку возможен только через получение лицензии, соблюдение требований по комплаенсу и раскрытие информации. Наиболее системно эта модель реализована в Евросоюзе через регламент MiCA, разработанный при участии European Securities and Markets Authority. Документ вводит единые правила для всех криптопровайдеров: от требований к капиталу до защиты средств клиентов и раскрытия рисков. Тот, кто не соответствует требованиям, не может работать на рынке ЕС.

Вторая модель — специальные юрисдикции или регулируемые зоны. Она разрешает операции с цифровыми активами, но не на всей территории страны, а в рамках отдельных правовых режимов. Это позволяет государству одновременно развивать индустрию и ограничивать риски для остальной экономики.

Третья модель предполагает фрагментарное регулирование с сильным надзором. Она используется, например, в США, где нет одного «закона о криптовалютах», но есть целый набор регуляторов и нормативных актов, которые вместе формируют жесткую среду контроля.

«Регулирование крипты сегодня — это попытка встроить новую финансовую инфраструктуру в существующую систему, сохранив управляемость и контроль над движением капитала, — считает финансист Кайрат Бермуханов, президент хедж-фонда IBF TRUST (зарегистрирован в ОАЭ). — Это хорошо видно, например, если посмотреть на ОАЭ, где система работы с криптой строится не на запретах, а на допуске через правила: хочешь работать — получи лицензию, соблюдай требования, будь прозрачен, и все у тебя будет хорошо. По этому же пути идут регуляторы ЕС и некоторые страны СНГ, и, на мой взгляд, это одна из самых зрелых моделей сегодня: государство не пытается вытеснить крипту, а, наоборот, использует регулирование как инструмент привлечения бизнеса и капитала. По сути, создается понятная среда, где и криптокомпании, и банки могут работать в одном правовом поле».

ОАЭ: крипта как часть стратегии глобального финтех-хаба

Сегодня ОАЭ действительно подает один из самых показательных примеров того, как государство может не просто регулировать крипторынок, а использовать его как инструмент экономической стратегии. В отличие от многих стран, где регулирование развивается реактивно — вслед за ростом рынка и рисков, — в Эмиратах оно изначально строилось как часть более широкой задачи привлечения международного капитала и финтех-компаний.

Ключевую роль в этой системе играет Virtual Assets Regulatory Authority (VARA, независимый регулирующий орган, который осуществляет надзор за сферой финансовых услуг, обеспечивает соблюдение норм и поддерживает стабильность финансовой системы) — специализированный регулятор, созданный в Дубае именно для работы с виртуальными активами. Он отвечает за лицензирование всех участников этого рынка, включая криптобиржи, брокеров, кастодианов и других криптопровайдеров. Доступ к рынку открыт, но только для тех, кто прошел проверку и соответствует требованиям по комплаенсу, управлению рисками и защите клиентов. Такой подход делает рынок прозрачным и одновременно снижает барьеры для институциональных игроков.

В Абу-Даби действует собственная регулируемая зона — ADGM, где надзор осуществляет Financial Services Regulatory Authority. Здесь регулирование виртуальных активов внедрено уже не первый год, и оно во многом ориентировано на интеграцию криптоуслуг в традиционную финансовую систему. Это создает внутри страны своего рода конкуренцию юрисдикций, но предлагает бизнесу несколько понятных и легальных точек входа на рынок.

«Регулирование в Эмиратах не ограничивается только лицензированием, — комментирует Кайрат Бермуханов. — Оно охватывает требования к корпоративной структуре компаний, внутреннему контролю, процедурам KYC и AML, хранению клиентских средств и отчетности перед регулятором. По сути, криптокомпании здесь приравняются к финансовым институтам, что делает рынок более предсказуемым для инвесторов и партнеров. Именно поэтому Дубай и Абу-Даби сегодня активно конкурируют за статус глобальных центров крипто- и финтех-индустрии, привлекая как стартапы, так и крупные международные компании».

США: регулирование через надзор и финансовую стабильность

В США крипторегулирование развивается по одному из самых сложных и многослойных сценариев. Здесь нет единого закона, который бы системно описывал рынок цифровых активов, однако это не означает отсутствия контроля — скорее наоборот. Надзор распределен между несколькими регуляторами, каждый из которых отвечает за свою часть: от борьбы с финансовыми преступлениями до банковского регулирования и оценки рисков для финансовой системы.

Параллельно усиливается внимание к банковскому сектору. Office of the Comptroller of the Currency (независимое бюро в составе Министерства финансов США, которое регулирует национальные банки, федеральные сберегательные ассоциации, а также федеральные филиалы и агентства иностранных банков) продолжает развивать подходы к участию банков в криптоэкономике — в его ведении вопросы от хранения цифровых активов до создания специализированных trust-структур. Это показывает, что государство не исключает банки из криптоконтекста, а, наоборот, стремится встроить их в новую инфраструктуру.

Отдельное направление — финансовая стабильность. Federal Reserve System (FRS) рассматривает стейблкоины как потенциальный системный фактор, поскольку они могут конкурировать с банковскими депозитами и платежной системой.

«Также в США действует SEC — U.S. Securities and Exchange Commission — именно это ведомство определяет, какие криптоактивы могут считаться ценными бумагами, а значит — подпадают под требования классического финансового регулирования, — рассказывает Григорий Семух, СТО Crypto-A. — Американский подход строится не вокруг создания отдельного криптозакона, а вокруг адаптации существующих норм под новую реальность. Это делает систему сложнее для бизнеса, но при этом обеспечивает высокий уровень защиты инвесторов».

ЕС: единые правила и конец «серой зоны»

Если США развивают регулирование через существующие институты, то Европейский союз пошел по пути создания единой и формализованной системы. Ключевым элементом здесь стал регламент MiCA (Markets in Crypto-Assets) — именно он регулирует рынок криптоактивов на уровне сразу нескольких стран и вводит единые требования для всех провайдеров криптоуслуг, включая биржи, брокеров, кастодианов и эмитентов токенов. Компании обязаны получать лицензии, соблюдать требования к капиталу, обеспечивать защиту клиентских средств и раскрывать информацию о рисках.

Отдельное внимание уделяется стейблкоинам: для них предусмотрены более жесткие правила, включая требования к резервам и контролю со стороны регуляторов. Это связано с тем, что именно стейблкоины рассматриваются как потенциальный конкурент банковской системе и фактор финансовой стабильности.

MiCA создает единое пространство для работы криптокомпаний внутри ЕС. Получив лицензию в одной стране Евросоюза, компания может предоставлять услуги на всей территории ЕС. Это снижает регуляторные барьеры и делает рынок более привлекательным для крупных игроков, включая банки и институциональных инвесторов. В итоге ЕС формирует одну из самых структурированных моделей регулирования: крипто становится частью финансовой системы, но работает по тем же принципам, что и традиционные финансовые рынки.

Беларусь: от эксперимента к интеграции в финансовую систему

Беларусь стала одной из первых стран постсоветского пространства, которая не просто легализовала криптовалюты, а попыталась встроить их в экономику через специальный правовой режим. В рамках Hi-Tech Park Belarus был создан льготный режим для операций с цифровыми активами. Этот подход позволил стране привлечь криптокомпании и сформировать базовую инфраструктуру рынка задолго до появления аналогичных решений в соседних государствах.

Однако к 2026 году модель заметно изменилась. Подписание Декрета № 19 «О криптобанках и цифровых знаках» стало сигналом того, что государство переходит к режиму системного контроля и интеграции.

«При этом Беларусь не отказалась от своей первоначальной стратегии — крипто здесь по-прежнему разрешена и используется как инструмент привлечения инвестиций и технологий», — отмечает Григорий Семух. — Однако требования к участникам рынка повышаются, появляется более четкая связка с фи-

нансовым сектором. По сути, эксперимент с криптой в стране завершен, и сейчас государство переходит к институционализации этого сектора».

Казахстан: крипто через контролируруемую финансовую экосистему

Казахстан — хороший пример регулирования через модель ограниченного допуска: в стране создан Astana International Financial Centre, где действует собственный регулятор — Astana Financial Services Authority (AFSA), и именно здесь сосредоточена вся легальная инфраструктура работы с криптоактивами.

«В стране есть лицензирование криптоплатформ, предъявляются достаточно строгие требования к операционной деятельности, управлению рисками и взаимодействию с клиентами», — отмечает Кайрат Бермуканов. — При этом ключевой принцип остается неизменным: торговля цифровыми активами в Казахстане допускается только на лицензированных площадках. Это позволяет государству одновременно решать две задачи: с одной стороны, рынок развивается, с другой — все операции проходят в контролируемой среде. Отдельное внимание уделяется интеграции криптоактивов в финансовую систему. Казахстан последовательно выстраивает модель, при которой цифровые активы не существуют отдельно, а становятся частью международного финансового хаба, ориентированного на инвесторов и институциональных игроков».

Кыргызстан: работа с собственными цифровыми активами

Кыргызстан первым из стран СНГ выпустил национальный цифровой токен. Речь идет о USDKG — стейблкоине, обеспеченном золотом и привязанном к доллару США. Эмиссию осуществляет компания со стопроцентным государственным участием, и власти планируют активно развивать это направление. А значит, важно развивать и законодательную базу по работе с цифровыми активами в регионе.

Регулирование работы с криптовалютами осуществляется в стране на основе Закона «О виртуальных активах», и оно во многом следует мировым стандартам: работать с криптой можно, если компания лицензирована и соответствует требованиям, предъявляемым государством.

Кейс Кыргызстана показывает, что работа с цифровыми активами уже не является прерогативой крупных финансовых центров: даже страны с менее развитой инфраструктурой стремятся создать собственную нормативную базу и встроиться в глобальную цифровую экономику.

Что это значит для банков

Все описанные модели регулирования сходятся в одном: крипто перестает быть внешним по отношению к банковской системе явлением. Напротив, государства последовательно возвращают банки в центр новой финансовой инфраструктуры.

«Во многих странах регуляторы не исключают банки из этой системы, а, наоборот, стремятся интегрировать их в криптоконтур», — отмечает Кайрат Бемуканов. — Это происходит через несколько направлений: развитие услуг по хранению цифровых активов (custody), участие в токенизации активов, обслуживание лицензированных криптопровайдеров, а также контроль и мониторинг транзакций. В США, например, рассматриваются модели, при которых банки могут работать с цифровыми активами в рамках существующих лицензий или через специализированные структуры».

Для банков это означает необходимость трансформации: от классических финансовых посредников — к участникам гибридной системы, где традиционные и цифровые активы существуют параллельно.

Что это значит для финтеха

Для финтех-компаний 2026 год стал точкой, в которой крипто окончательно перестала быть нишевой историей «для энтузиастов» и превратилась в полноценный инфраструктурный слой. Ее используют (или планируют использовать) не только для торговли, но и для платежей, расчетов, хранения стоимости, создания новых финансовых продуктов. Однако вместе с этим исчезает и иллюзия «свободного рынка без правил».

ПЛАС



Инвесторы в России могут получить доступ к иностранным стейблкоинам с 1 сентября

Квалифицированные инвесторы с 1 сентября 2026 года смогут приобретать через российскую инфраструктуру иностранные стейблкоины (включая USDT и USDC), а также другие иностранные беспоставочные цифровые инструменты. Поправки подготовлены ко второму чтению законопроекта «О цифровых валютах и цифровых правах».

В редакции, принятой в первом чтении, законопроект легализует обращение криптовалют. Граждане и компании смогут покупать и продавать их через лицензированных операторов обмена из реестра ЦБ, брокеров и доверительных управляющих.

Однако стейблкоины USDT и USDC могут не подпасть под определение цифровой валюты, так как их эмитенты принимают обязательства по поддержанию стоимости и выкупу. Ко второму чтению в законопроект введены понятия «иностранная цифровая валюта» и «беспоставочная иностранная цифровая валюта».

Под определение беспоставочного инструмента подпадают иностранные обеспеченные стейблкоины. Их владельцы могут требовать погашения токенов деньгами по номиналу, при этом сам стейблкоин не является ценной бумагой.

В докладе ЦБ «Стейблкоины: направления развития в России» регулятор относит USDT и USDC к иностранным цифровым правам, а не криптовалютам. На них приходится около 89% мирового рынка стейблкоинов. ЦБ отмечает, что расчеты в USDT проходят практически мгновенно, тогда как SWIFT-перевод может занимать более пяти дней.

Приобретать иностранные цифровые инструменты смогут квалифицированные инвесторы. Для неквалифицированных доступ возможен только по решению ЦБ, за исключением расчетов по внешнеторговым договорам.

Биткоин останется в диапазоне 64 000–67 000 долларов без позитивных драйверов

Региональный руководитель криптобиржи CoinEx в СНГ Адиль Алиев заявил, что биткоин останется в диапазоне \$64 000–\$67 000 при отсутствии позитивных драйверов. По его словам, на рост курса могут повлиять принятие Clarity Act и стабилизация цен на нефть.

В июле биткоин демонстрирует устойчивость к геополитике, глобальному регулированию, продажам со стороны крупных институциональных инвесторов и к перетоку капитала в акции ИИ-компаний. Под давлением этих факторов биткоин с начала года потерял 33%, опустившись с \$87 500 до \$58 200.

Использование стейблкоинов для трансграничных B2B-платежей резко возросло

Компания Paybis опубликовала отчет об инфраструктуре стейблкоинов, который впервые был представлен на конференции Money20/20 Europe. В документе отмечено, что 23% предприятий используют или планируют использовать стейблкоины для трансграничных платежей.



В отчете используются данные платформы Paybis и отдельного бизнес-исследования, показывающие значительные изменения в структуре активности стейблкоинов на платформе за последние три года. В апреле 2026 года на стейблкоины приходилось 86% от общего объема криптовалютных операций, обработанных Paybis, по сравнению с 12% в июле 2023 года. Общий объем операций со стейблкоинами на платформе достиг 2,81 млрд долларов США в мае 2026 года, а годовой объем в 2025 году увеличился в 7,2 раза. С января по апрель 2026 года объем операций со стейблкоинами вырос на 135% по сравнению с аналогичным периодом 2025 года.

Теперь в объеме операций на платформе доминирует активность сегмента B2B

Рост операций со стейблкоинами сопровождался заметным сдвигом в сторону использования в сегменте B2B. В 2023 году на транзакции B2B приходилось 36% объема операций со стейблкоинами на Paybis, в 2024 году эта доля выросла до 70,1%, а в 2025 году — до 96,9%. В период с января по апрель 2026 года на потоки B2B приходилось 97,8% объема операций со стейблкоинами на платформе, что является заметным изменением для провайдера, который также предлагает продукты для розничной торговли.

Данные Paybis по секторам охватывают объем B2B-продаж стейблкоинов с апреля 2024 года. Лидером стали цифровые товары (21,4%), за ними следуют бизнес виртуальных активов (15,8%), технологии (15,1%), розничная торговля и электронная коммерция (14,5%) и финансовые технологии

(11,6%). Вместе эти пять секторов составили 78,4% объема B2B-продаж в стейблкоинах за этот период.

Полученные результаты соответствуют более широким сигналам из отрасли относительно внедрения стейблкоинов в платежную инфраструктуру. Нормативные документы, такие как регламент ЕС о рынках криптоактивов (MiCA), начали предоставлять более четкие условия работы для эмитентов стейблкоинов и поставщиков платежных услуг в Европе, что может способствовать росту доверия бизнеса к расчетам на основе стейблкоинов.

Недостаток осведомленности может сдерживать внедрение

Несмотря на рост использования стейблкоинов, в отчете отмечается сохраняющийся пробел в знаниях среди лиц, принимающих бизнес-решения. В ходе опроса 53% респондентов ожидали моментального проведения международных переводов стейблкоинов, 47% — проведения расчетов в течение от одного часа до суток, а 17,4% — в течение одних суток. На практике расчеты по стейблкоинам обычно происходят в течение секунд или минут, в зависимости от используемой блокчейн-сети.

Ожидания относительно стоимости также разделились. Из 1068 респондентов 33,3% ожидали комиссию за перевод в размере около 3%, а 32% — 0,01%. Ответы в целом разделились между более высокими оценками комиссий в 3% или 1% и более низкими оценками в 0,5% или 0,01%. Учитывая, что стоимость платежей в стейблкоинах обычно оценивается ниже 1%, завышенная оценка как сумм комиссий, так и времени расчетов может привести к тому, что компании будут недооценивать практические преимущества систем стейблкоинов по сравнению с традиционными корреспондентскими банковскими маршрутами.

Константин Василенко, соучредитель и директор по развитию бизнеса Paybis, отметил, что в настоящее время основная часть объема сделок на платформе приходится на B2B, поскольку компании хотят, чтобы трансграничные расчеты и перемещения казначейских средств осуществлялись быстрее. Компания охарактеризовала стейблкоины как новый расчетный формат в рамках более широкой финансовой системы, особенно актуальный для трансграничных расчетов и международных казначейских операций.

По материалам thepaypers.com; PLUSworld.ru

Международный ПЛАС-Форум «Платежный бизнес и денежное обращение»



PAYMENTS & CASH CIRCULATION International PLUS-Forum

RUSSIA, MOSCOW SEPTEMBER 7-8|2027



7–8 сентября 2027 года Москва станет центром притяжения финансового сектора России и ближнего зарубежья. Банки, платёжные системы, регуляторы — все на одной площадке. Не пропустите главное событие года!



3000+ участников

150+ спонсоров

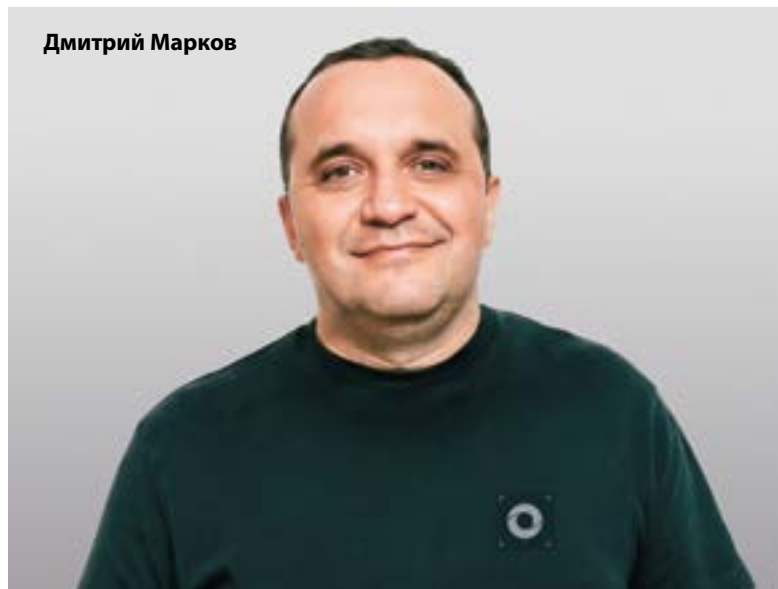
120+ спикеров

«Рэдиссон Славянская», Москва

Когда платят не люди. Финансовая инфраструктура в эпоху ИИ-агентов — необходимые трансформации

Еще несколько лет назад искусственный интеллект воспринимался прежде всего как инструмент для анализа данных, генерации контента и автоматизации отдельных процессов. Сегодня на рынок выходят ИИ-агенты — автономные цифровые системы, способные самостоятельно выполнять задачи, принимать решения, взаимодействовать с другими сервисами... и совершать платежи. На текущем этапе главной задачей является создание инфраструктуры, которая позволит делать это безопасно и надежно при любом объеме транзакций. О том, как может выглядеть подобная инфраструктура, которая изменит мировую экономику, рассуждает Дмитрий Марков, генеральный директор VisionLabs.

Дмитрий Марков



По данным Deloitte, около 30% компаний изучают возможности агентного ИИ и 38% запустили пилотные проекты в этой сфере. При этом Gartner прогнозирует, что к 2028 году 15% повседневных бизнес-решений будут принимать ИИ-агенты, и они будут использоваться в 33% корпоративного ПО.

Такие агенты уже могут найти поставщика, согласовать условия сделки, подготовить документы, забронировать услугу. Однако существовало фундаментальное ограничение: любой сценарий заканчивался там, где требовалось непосредственно совершить платеж, — в этот момент вмешивался человек.

Следующий этап развития цифровой экономики — трансформация платежной инфраструктуры под автономные системы. И он уже начался: крупнейшие игроки финансового рынка создают инфраструктуру для агентских платежей. Visa и Mastercard разработали системы, которые позволяют привязывать платежные данные к конкретному ИИ-агенту с заранее заданными ограничениями (платформа Intelligent Commerce и протокол Trusted Agent

Protocol у Visa, проекты Agent Pay и Agent Pay for Machines у Mastercard).

Google создала открытый стандарт авторизации агентских платежей AP2 (Agent Payments Protocol), PayPal — библиотеку Agent Toolkit, позволяющую ИИ-агентам работать с заказами, подписками и платежами, American Express — платформу Agentic Commerce Experiences, которая объединяет регистрацию агентов, токенизированные платежные данные и проверку намерений пользователя. Также компания первой представила механизм защиты клиента при ошибках, совершенных ИИ-агентом.

Платежная система Stripe создала инфраструктуру из нескольких элементов:

- систему общих платежных токенов (Shared Payment Token): токен привязан к конкретному продавцу и сумме покупки, что позволяет агенту инициировать платеж, не раскрывая данных карты;
- виртуальные карты для ИИ-агентов;
- кошелек Link для оплаты агентами;
- систему Agentic Commerce Suite для интеграции с различными агентами.

При этом разработки часто сталкиваются с ограничениями сегодняшней инфраструктуры. Например, Stripe совместно с OpenAI создала протокол ACP (Agentic Commerce Protocol) для покупок через ChatGPT. Функция стала доступна в конце прошлого года для пользователей из США, но через несколько месяцев ее убрали из-за сложностей с подключением продавцов, поддержкой актуальных каталогов товаров и обработкой корзин с разными товарами.

Когда агенты платят агентам: в чем сложность

Современная финансовая инфраструктура проектировалась вокруг человека. Номера банковских счетов, карты, интернет-банкинг, процедуры идентификации клиентов, механизмы подтверждения операций и разре-

шения споров — все эти элементы предполагают наличие конкретного пользователя, который принимает решение и несет ответственность за транзакцию.

Такая модель прекрасно работает в мире, где платежи иницируют люди. Но она оказывается недостаточно эффективной, когда платят ИИ-агенты. Например, люди могут неделями обсуждать условия сделки и согласовывать документы перед переводом денег — ИИ способен принимать аналогичные решения за секунды. В результате скорость бизнес-процессов начинает ограничиваться платежной инфраструктурой.

Когда мы говорим об агентских платежах, мы имеем в виду не только сценарии, в которых ИИ оплачивает товары и услуги от имени человека, но и ситуации, когда агенты взаимодействуют между собой. Например, агенту поручили создать сайт. Для этого он обращается к специализированным системам: одна отвечает за дизайн, другая — за разработку, третья — за тестирование, четвертая — за маркетинговый контент. Каждый из этих сервисов может принадлежать разным компаниям и иметь разную стоимость.

При такой модели необходимы мгновенные расчеты между цифровыми участниками процесса. Так появляется новая агентная экономика, где платеж перестает быть отдельным действием человека и превращается в программную функцию.

Какие проблемы предстоит решить

Переход к агентным платежам ставит перед финансовой отраслью ряд новых вопросов.

Первый — идентификация. Если сегодня банк «знает своего клиента», то завтра ему предстоит понимать, какой агент совершает транзакцию, от чьего имени действует и какие у него полномочия.

Второй вопрос связан с ответственностью. Если агент сам выбрал поставщика или услугу, а пользователя не устроил результат, то кто должен за это отвечать?

Третья проблема — безопасность. Современные антифрод-системы обучены выявлять отклонения в поведении людей, а поведение ИИ-агентов будет существенно отличаться. Это потребует совершенно новых моделей оценки рисков и обнаружения мошенничества. Кроме того, возникает вопрос доверия между самими агентами. Если автономная система взаимодействует с тысячами неизвестных контрагентов по всему миру, ей необходимы механизмы проверки репутации и надежности другой стороны.

Как будет устроена новая инфраструктура

Платежную инфраструктуру будущего можно построить вокруг специализированных цифровых кошельков

для агентов. Каждый агент получает ограниченный объем полномочий и доступ к определенной части средств. Компании могут устанавливать детальные правила расходования средств: лимиты, категории разрешенных операций, перечни доверенных контрагентов и требования дополнительного согласования — не передавая контроль над корпоративным счетом полностью.

Это программируемая финансовая среда, где правила управления деньгами становятся частью кода.

Важную роль будут играть инструменты наблюдемости и аудита. Любое решение агента должно быть прозрачным и объяснимым, чтобы человек всегда мог восстановить цепочку действий и понять, почему агент совершил конкретную транзакцию.

Платежи должны стать мгновенными

Одна из ключевых особенностей ИИ-экономики в том, что она будет значительно более глобальной. Для агента не существует привычных географических ограничений. Если наиболее подходящий подрядчик находится в другой стране, система выберет именно его.

Это приведет к резкому росту количества международных транзакций. В таких условиях традиционные платежные механизмы с длительными сроками проведения операций и высокими комиссиями начнут терять эффективность.

Инфраструктура будущего должна обеспечивать практически мгновенное подтверждение платежей, минимальные издержки и возможность переключаться между разными финансовыми системами и юрисдикциями. Платежи должны стать такими же быстрыми, как обмен данными между программами.

Что это означает для финансовой отрасли

Когда-то интернет-платежи тоже были незнакомым рынку инструментом с неподтвержденной безопасностью и вызвали опасения, но сегодня это основа мировой экономики. Аналогичный путь должны пройти агентные платежи.

По мере распространения автономных систем финансовому сектору предстоит создать новую инфраструктуру — не для людей, а для машин. Она должна обеспечить идентификацию, доверие, безопасность, прозрачность и мгновенные расчеты между цифровыми участниками экономики.

В конечном итоге речь идет не просто о новом платежном инструменте. Мы увидим, как будет формироваться финансовая система, в которой ИИ-агенты самостоятельно договариваются, принимают решения и рассчитываются друг с другом. Именно она станет одним из ключевых элементов экономики следующего десятилетия.

ПЛАС

RegTech. Как новая архитектура взаимодействия банков и регулятора меняет подход к данным

Регуляторная отчетность банков давно перестала быть просто процессом подготовки форм. Сегодня это зеркало, которое отражает — или не отражает — реальное качество данных внутри организации. Регуляторы все точнее формулируют требования к тому, как именно данные должны собираться, обрабатываться и подтверждаться. И именно здесь большинство банков сталкиваются с системным разрывом между тем, что есть, и тем, что требуется. Подробнее рассказывает Алексей Карнаухов, ex-CDO Ипотека Банк, эксперт в области Data Governance и RegTech-трансформации.

Почему существующая архитектура перестает работать

Большинство банков сегодня работают в том, что можно назвать «отчетной» архитектурой данных. Отчеты формируются из разных систем, каждая из которых живет по собственным правилам. Бизнес-правила расчета показателей распределены между десятками ETL-процессов (ETL, Extract, Transform, Load — ключевой процесс интеграции данных), и никто не может с уверенностью сказать, какое правило является эталонным. Ручные корректировки при подготовке отчетности — не исключение, а норма.

Последствия этого системного устройства хорошо известны практикам. Один и тот же показатель — например, просроченная задолженность — может давать три разных значения в кредитном модуле, бухгалтерии и DWH, потому что каждая система применяет собственную методологию расчета. Отчеты нельзя воспроизвести из первичных данных, потому что между источником и итоговой цифрой есть ручные правки, о которых никто уже давно не помнит. Регулятор приходит с вопросом об источнике конкретного числа — и банк не может дать ответ за разумное время.

Deutsche Bank заплатил 150 млн долларов штрафа регуляторам США не за мошенничество — за качество регуляторной отчетности. Плохие данные стоят дорого.

Международный стандарт BCBS 239, устанавливающий требования к агрегации данных о рисках и регуляторной отчетности, был введен в 2013 году. Более десяти лет спустя большинство банков по-прежнему не соответствуют ему в полной мере. Это не вопрос желания — это вопрос архитектуры, которую нельзя починить точечными мерами.

RegTech как архитектурный переход

RegTech в широком смысле — это переход от отчетной архитектуры к управляемой архитектуре данных. Суть перехода можно описать через пять изменений, которые происходят одновременно.



Алексей Карнаухов

Первое — переход от разных источников к единой модели данных. Вместо того чтобы каждая система формировала отчеты по-своему, создается единый слой данных — с централизованными определениями атрибутов, едиными справочниками и общей логикой расчета показателей.

Второе изменение — переход от распределенных правил к централизованным расчетам. Бизнес-правила перестают жить в разных ETL-процессах и переносятся в единый регуляторный data layer поверх DWH. Одно правило — один результат для всех отчетов.

Третье — переход от отсутствия lineage к полной прослеживаемости. Каждый показатель в регуляторном отчете должен быть прослежен до первоисточника автоматически — через технический, атрибутивный и transformation lineage. Это не документация ради документации, это инструмент защиты при аудите.

Четвертое изменение — от ручных корректировок к certification layer. Перед публикацией каждого отчета данные проходят формализованный процесс сертификации: автоматические DQ-проверки, подтверждение lineage, бизнес-контроль и финальная виза Data Owner.

Пятое — переход от отчетов из систем к управляемой отчетности из DWH. Вся регуляторная отчетность формируется из хранилища данных — никогда напрямую из операционных систем. Это единственный способ обеспечить воспроизводимость и единообразие.

Архитектура: как это устроено на практике

Целевая архитектура RegTech строится на принципе централизации: операционные системы банка остаются неизменными, над ними выстраивается трехуровневое хранилище (ODS — DDS — DM), а поверх витрин формируется регуляторный data layer — специализированный слой, в котором централизованы все бизнес-правила расчета регуляторных показателей. Именно здесь происходит унификация методологий, устраняющая расхождения между разными системами банка.

На вершине архитектуры — KPI-слой с регуляторными показателями, готовыми к публикации. Вся отчетность формируется из него автоматически. Никогда — напрямую из операционных систем. Это единственный способ обеспечить воспроизводимость и единообразие показателей.

Параллельно с технической частью выстраивается Data Governance. Без нее архитектура не работает: можно построить идеальное хранилище, но если у атрибутов нет владельцев, нет единых определений и нет процесса управления изменениями, качество данных деградирует под давлением операционной реальности.

Data Governance: операционная модель, а не методология

Data Governance в контексте RegTech — это не набор политик, а операционная модель управления регуляторными данными, которая работает ежедневно. На практике именно ее отсутствие чаще всего становится причиной провала трансформации.

Data Owners — бизнес-лидеры, несущие персональную ответственность за корректность данных в своих доменах. Не IT, не CDO Office — именно бизнес. Без этого данные остаются «ничьими», и любой вопрос регулятора превращается в расследование без ответственного.

Business Glossary — единый словарь терминов, утвержденный всеми департаментами. Именно расхождение в определениях — когда кредитный аналитик, бухгалтер и аналитик DWH понимают «просроченную задолженность» по-разному — является источником большинства регуляторных инцидентов. По оценкам Accenture, в 85% случаев причина таких инцидентов в банках — не технический сбой, а ошибки в данных и отсутствие единых определений.

Certification Layer — обязательный этап перед публикацией отчетности: автоматическая проверка качества

данных, подтверждение lineage, бизнес-контроль соответствия расчетов и финальное подтверждение Data Owner. Без прохождения всех четырех шагов отчет не публикуется.

Классификация данных: риск-ориентированный подход

Не все данные требуют одинакового уровня контроля. Попытка применить максимальные требования ко всему приводит к операционному параличу. Эффективная система RegTech строится на риск-ориентированной классификации трех уровней.

Критические надзорные данные, влияющие на регуляторные нормативы, требуют полного lineage, обязательной сертификации и SLA в один день. Значимые финансовые данные — базовых DQ-проверок, частичного lineage и SLA — до трех дней. Вспомогательные данные — базового мониторинга с SLA — до пяти дней.

Аналогичная логика применяется на уровне атрибутов: регуляторные атрибуты первого типа требуют полного lineage, reconciliation и строгих DQ-правил; расчетные — умеренного контроля; справочные — базового мониторинга. Такой подход позволяет концентрировать ресурсы там, где это действительно важно.

Организационные барьеры: где буксует трансформация

Технологическая часть RegTech-трансформации, как правило, решается. Сложнее — организационная. Практика показывает, что именно здесь большинство проектов теряют темп.

Первый барьер — размытая ответственность. Данные воспринимаются как «общий ресурс», конкретных владельцев нет, и когда возникает вопрос о качестве атрибута, начинается многоуровневое выяснение того, кто за это отвечает.

Второй — разрыв между бизнесом и IT. IT-специалисты не понимают бизнес-контекст полей. Бизнес не осознает технических ограничений систем. Без выстроенного взаимодействия governance не работает.

Третий — сопротивление переходу от ручного контроля к автоматизированному. Люди, годами применявшие ручные корректировки, воспринимают автоматизацию как угрозу — потому что она делает проблемы данных видимыми.

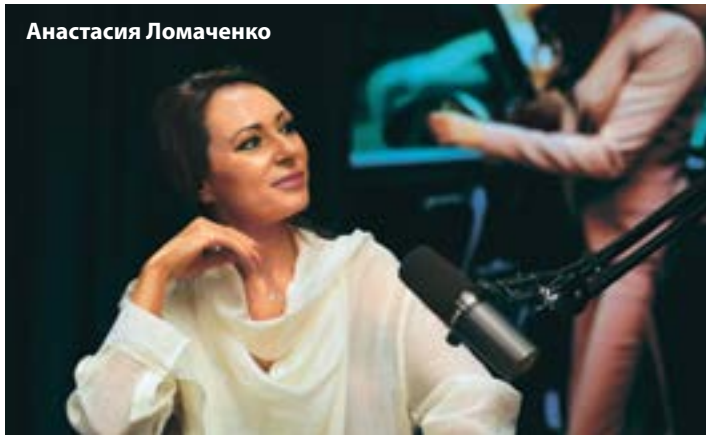
Трансформация RegTech буксует не из-за технологий, а из-за людей и процессов. Успех требует устранения разрывов в ответственности, коммуникации и операционных моделях.

Эти барьеры не уникальны для RegTech — они характерны для любой data-трансформации. Но в регуляторном контексте цена их игнорирования выше: на кону не только операционная эффективность, но и отношения с надзорным органом.

Авторынок и e-commerce: синергия на новом этапе

Перспективы встраивания авторынка в сегмент электронной коммерции обсудили директор по маркетингу компании АВТОРУСЬ Анастасия Ломаченко и директор бизнес-направления «Запчасти и Автосервисы» компании Авито Алексей Головин в подкасте VLADIS SHOW «Авито x АВТОРУСЬ – Одна ошибка, и машина встала. Что скрывает рынок автозапчастей?».

Анастасия Ломаченко



А. Ломаченко: Электронная коммерция работает по своим, более жестким правилам. Если доля рынка на маркетплейсах ранее была 22%, потом достигла 38%, то в 2026 году вообще ожидают 50%. Для меня как в большей степени офлайн-игрока это тревожная тенденция. Потому что 50% онлайн — это очень много.

А. Головин: У нас формат скорее гибридный. Ведь люди могут найти товар у нас, а купить в офлайн-магазине. Но если в целом обсуждать проникновение e-commerce в рынок запчастей — сейчас мы наблюдаем активный рост онлайн-сегмента: на сегодняшний день на него приходится уже 30% продаж, и я думаю, что в течение следующих трех лет эта доля может увеличиться вдвое. И если сравнивать ситуацию с другими сегментами ритейла, например, с одеждой, электроникой и т. д., то там, безусловно, проникновение e-com уже больше 50%.

Есть структурные причины, почему на нашем рынке иная тенденция:

1. Нужно понимать и видеть лично, подходит ли определенная запчасть к автомобилю.
2. Нужна гарантия — на маркетплейсах до конца непонятно, как вернуть товар.

Условно говоря: клиент заказал себе кроссовки, товар приехал на ПВЗ, человек их померил, они не подошли, он их вернул. Но как в такой ситуации быть, например,

с тормозами? Примерить и сдать обратно? По закону это, конечно, можно сделать, но сколько будет потрачено времени и нервов? В связи с этим пользователи доверяют продавцу, его экспертизе и зачастую предпочитают увидеть товар «лицом», получить офлайн-гарантию того, что все точно подойдет. Поэтому офлайн еще долго будет иметь большую долю на нашем рынке, по крайней мере в 2027 году точно. Даже несмотря на то, что рынок стагнирует и идет большой переток в онлайн.

А. Ломаченко: Да, продажи — дело сложное, особенно когда рынок схлопывается, и покупательская способность падает. Самое проблематичное — это когда что-то возвращается после ремонта у нас, потому что вновь вышло из строя у потребителя.

А еще возникают мелкие проблемы с неподходящим товаром — клиент в пункте самообслуживания покупает универсальную щетку с переходниками, вроде самую простую вещь, а в моменте оказывается, что она не универсальная, и не на любую машину ее можно поставить. И тогда клиенту приходится возвращаться, чтобы в сервисе подобрали товар под конкретную машину.

Но самая дорогая ошибка для нас — это когда клиент не возвращается. Такое, хотя и нечасто, но бывает. Например, когда к нам приходят мастера-новички. Если говорить про железо, то самая дорогая ошибка для клиента — когда ему приходится заезжать в ремонтный цех дважды. Например, замена цепи ГРМ на том же «Киа Рио» влечет за собой целый комплекс работ. Зачастую клиенты выбирают просто замену цепи ГРМ и игнорируют дополнительные услуги — те, что мы им аргументированно советуем. И по причине того, что в моменте они не согласились, например, на замену сальника переднего коленвала или прокладки помпы, через месяц им приходится возвращаться и делать весь комплекс снова. Получается, клиент платит за работу мастера дважды.

А. Головин: С точки зрения e-commerce, у потребителей есть определенные барьеры при покупке запчастей онлайн. В первую очередь это вопрос совместимости — подойдет или не подойдет купленная запчасть к конкретному автомобилю. Это один из самых распространенных моментов. Потому что есть огромное множество различных предложений, и при этом большое количество разных марок, моделей и модификаций. То есть у условного «Киа Рио» есть двигатель 1,4, а есть двигатель 1,6, и туда идут абсолютно разные запчасти в зависимости от модификации. Обычный пользователь, конечно, этого может не знать. Второй момент — это гарантия качества товара, то есть либо это какой-то хороший аналог, либо это оригинал.

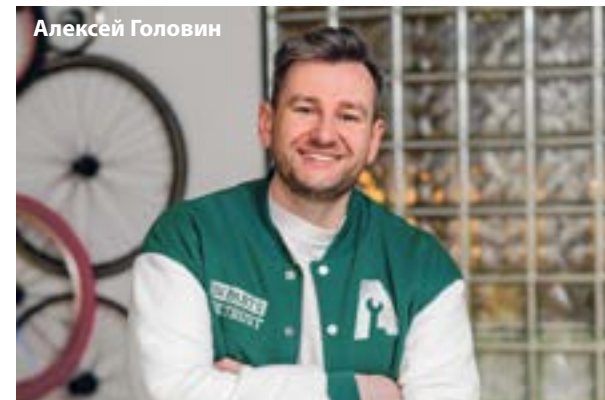
И третий момент — как это все потом при случае возвращать. Люди просто не понимают, как работать с воз-

вратами. Даже с учетом того, что онлайн-площадки уже всесторонне проработали вопросы возвратов, все очень понятно и доступно прописали, все в соответствии с Законом о защите прав потребителей и т. д. Все равно для потребителя это огромный барьер. Он думает: «Если что-то не подойдет, я потрачу время, будет простой автомобиля, потом нужно будет все возвращать, потом снова заказывать...»

Все эти моменты и транзакционные издержки приводят к тому, что иногда потребителю проще поехать в сервис или к какому-то знакомому мастеру, чтобы ему сразу в моменте все подсказали, рассказали, подобрали. И за это потребитель готов переплачивать.

А. Ломаченко: Безусловно, клиент часто приходит с некоторым недоверием. Чаше всего клиент боится, что ему придется переплатить. И нужно понимать, что предварительный расчет мы делаем, когда машина еще не на подъемнике и не разобрана — и мастер не может точно сказать, что нужно сделать. А замена даже одной детали обычно влечет за собой целый комплекс работ, причем цена может отличаться в зависимости от машины.

Алексей Головин



Но такая ситуация сложилась, к сожалению, в целом на рынке. Хотя мне кажется, что в последние годы она начинает меняться, клиенты становятся лояльнее, особенно те, что приезжают постоянно.

В 2026 году мы убедились, что клиенты проявляют лояльность даже в вопросах, которые изначально подразумевали конфликт. И зачастую любую ситуацию решает диалог. Как только ты объясняешь все нюансы, клиент действительно начинает слышать мастера.

А. Головин: Есть разные виды потребителей. Существует классическая сегментация:

1. Клиенты «do it for me» — те, кто покупает запчасти сам и устанавливает их в сервисе.
2. Клиенты «full package» — те, кто вообще не хочет разбираться и полностью делегирует всю ответственность автосервису.

Но мы пошли дальше и смотрим на поведенческие особенности данных сегментов. И мы определили, что существует еще один подсегмент — «беспомощные автовладельцы». Из названия в целом понятно, что это люди, которые не разбираются именно в ремонте автомобиля. И таких порядка 60%. То есть больше половины потребителей. И понятно, что в два раза переплачивать никто не будет, но есть разумная переплата с целью снизить риски — когда человек не разбирается, но ему важно гарантировать успех. Этот сегмент, скорее всего, будет готов переплатить, но только если вы гарантируете качественный сервис, дадите гарантии и хорошую консультацию.

А бывает, что сами продавцы на площадке подрывают доверие клиентов. И это достаточно сложный вопрос. Во-первых, наши покупатели всегда смотрят на рейтинг и отзывы продавца. Потому что, если предложения одинаковые, цены плюс-минус одинаковые — траст-фактор будет перевешивать все остальное. То есть самое главное — это доверие к продавцу через отзывы, через рейтинги, как он общается с клиентом в чате, как консультирует.

И как раз мы в этом плане очень сильно отличаемся от маркетплейсов, потому что 97% наших сделок проходят через плотное общение. Сделок без общения очень мало, их почти нет. То есть здесь важен социальный контакт, некая консультация — это наше основополагающее отличительное преимущество. И то, как продавец общается, зачастую определяет, будет ли сделан выбор в его пользу.

А. Ломаченко: Согласна. Если человеку не уделили внимания — это всегда конфликт. В отзывах это видно сразу. Конструктивные отзывы, где описана конкретная проблема, звучат уже без эмоций.

А. Головин: Вот как раз из «сухих», но ценных по содержанию отзывов мы поняли: большинство проблем — типовые. Нам стало очевидно, как важно не просто читать такие отзывы, а превращать их в алгоритмы. Так родилась идея активно внедрять ИИ. У нас развиваются помощники на базе ИИ и агрегированного каталога совместимости (работаем с Laximo, VINPIN и т. д.). Пользователь может зайти в ИИ-помощника и подобрать запчасть. Мы увеличиваем трафик постепенно — пока только 1–1,5% клиентов общаются с ИИ-ассистентом, потому что у ИИ все еще случаются ошибки. Но в любом случае конверсия выше, и это сокращает временные затраты продавцов на общение. Это будущее, и значение ИИ в мире автозапчастей огромно. Тем не менее пока мы уверены: часть работы, конечно, сделает ИИ, но дополнительные консультации клиенты все равно продолжают в чате с продавцом, особенно если речь идет о ранее упомянутых конфликтных ситуациях. Людям, и прежде всего клиентам, по-прежнему нужны внимание и живое общение.

ПЛАС

Банки без интернета. Кто и как даст клиентам доступ к деньгам?

Сценарий полного отключения глобальной сети на региональном или национальном уровне пока не проработан ни в одном публичном стресс-тесте российских банков. Какова реальная готовность к нему банковского сектора? Свои ответы на этот неудобный, но, к сожалению, крайне актуальный сегодня вопрос предлагает наш постоянный автор **Тимур Аитов, член Совета ТПП РФ по финансовому рынку и инвестициям, председатель комиссии по безопасности финансового рынка, руководитель Центра компетенций «Цифровизация финансовых технологий».**

Представьте стандартное утро: клиент открывает мобильное приложение, чтобы проверить баланс или перевести средства. И вместо загрузки — бесконечный спиннер. Сайт банка недоступен, мессенджеры молчат, SMS приходят с многоминутной задержкой. Причина — проблемы с интернетом. И неизвестно, когда связь восстановится.

Этот сценарий перестал быть гипотетическим. В зонах военных конфликтов и на приграничных территориях перебои с интернетом и мобильной связью — уже реальность. Однако российские банки, по экспертным оценкам, к такому развитию событий не готовы. Вопрос в том, почему сложилась такая ситуация и какие инструменты могут обеспечить доступ к деньгам в кризис.

Важно различать два принципиально разных сценария отключения. Первый — глобальный интернет недоступен, но сотовая сеть и каналы голосовой связи сохраняют работоспособность. В этом случае спасти ситуацию могут SMS, USSD-запросы и DTMF-меню.

Во втором сценарии причиной выступает физическое уничтожение вышек сотовой связи и оптоволоконка, когда ни интернет, ни мобильная связь не работают. Здесь единственными резервами остаются спутниковые каналы, проводная телефония или собственные изолированные сети (pLTE). Наш дальнейший анализ исходит именно из этого разделения.

Системная зависимость: как мы оказались в уязвимом положении

Сбои интернета продолжительностью от нескольких часов до суток фиксировались в России уже в 2024 году. Их последствия были ощутимы: клиенты теряли доступ к счетам, платежи зависали, контакт-центры не справлялись с потоком обращений. Однако сценарий полного отключения глобальной сети на региональном или национальном уровне пока не проработан ни в одном публичном стресс-тесте российских банков.



Тимур Аитов

Какова готовность банковского сектора к такому сценарию?

Современные банковские платформы построены на API-шлюзах, облачных провайдерах и распределенных ЦОД. При отключении интернета сразу перестают функционировать:

- авторизация по биометрии;
- подтверждение операций через push-уведомления;
- мгновенные переводы по СБП;
- чат-боты и голосовые помощники на базе ИИ.

Остаются только голосовые звонки и SMS. Сегодня банки сократили инвестиции в эти каналы, переведя клиентов в мессенджеры и пуш-уведомления, — это в разы дешевле. В результате пропускная способность SMS-шлюзов снижена до штатного уровня и не рассчитана на десятикратный рост трафика.

Нормативная база нуждается в развитии. Положение № 716-П регулирует общие принципы непрерывности, но не конкретизирует технологии. ЦБ в 2024–2025 годах выпустил ряд рекомендаций по усилению киберустойчивости (в том числе в части резервирования каналов). Правда, они не носят обязательного характера, но важны для дальнейшего развития. В отличие от России в Евросоюзе действует стандарт DORA, обязывающий тестировать экстремальные сценарии.

В рамках цифровой трансформации появляется все больше централизованных инфраструктурных элементов, таких как, например, ЕСИА. На эти сервисы завязаны многие критичные процессы. Но и они перестанут работать в случае потери связи с ними.

Многие крупные финансовые компании и банки создают распределенную микросервисную архитектуру. При нарушении связности сети такая архитектура также, скорее всего, перестанет функционировать.

Нарушен может быть не только интернет — мобильная связь также может быть уничтожена. Это значит, что в качестве резервного канала неплохо бы иметь даже обычную проводную телефонию. Остается открытым вопрос: есть ли в банках эксперты, несущие персональную ответственность за проектирование действительно надежной архитектуры?

Старые, но не забытые

Инструменты, которые банки массово сворачивали в 2010-х, сегодня вновь обретают актуальность. SMS, USSD-запросы и тоновый набор DTMF не требуют интернета, работают при минимальном уровне сигнала и доступны на любых устройствах, включая кнопочные телефоны.

Крупные банки имеют спутниковые резервы; средние и малые игроки такой возможности лишены. Доля SMS в клиентских коммуникациях упала с 65% в 2020 году до 22% в 2025-м. В кризис именно SMS становится основным каналом — и его текущая пропускная способность недостаточна.

Альтернативы SMS известны. USSD-запросы (комбинации * и #) позволяют выполнять базовые операции: проверку баланса, блокировку карты, подтверждение платежей. В Африке и Юго-Восточной Азии этот канал остается основным для мобильных финансов.

DTMF-меню (тоновый набор) дает возможность автоматизировать до 70% типовых запросов через голосовое меню, минуя оператора.

В странах с высокими военными рисками резервные каналы закреплены нормативно. В Израиле банки обязаны иметь минимум два независимых канала, один из которых должен функционировать без использования интернета.

В России таких требований нет.

Изолированные сети как стратегический резерв

Помимо восстановления устаревших каналов (SMS, USSD) отрасль может совершить технологический рывок. Речь идет о создании банками собственных изолированных сетей pLTE (Private LTE).

Private LTE (pLTE) — это частная сеть 4G, полностью контролируемая предприятием и не зависящая от публичных вышек мобильных операторов.

Специальное программное обеспечение (СПО) системы управления такой сетью уже появилось в реестре отечественного ПО (запись № 33790 от 18.06.2026). СПО позволяет построить «частное ядро» мобильной связи. СПО предназначено для реализации программно-аппаратного взаимодействия оборудования связи при построении изолированных сетей для нужд организаций и предприятий неоператорского класса в соответствии с требованиями ИБ по КИИ.

Что важно? Такое решение дает банку собственный канал связи, полностью независимый от публичного интернета и операторов. В ядре на перспективу заложены опции, позволяющие выступать в роли брокера онлайн-транзакций на платформу цифрового рубля (ЦР), и используется идея привязки CBDC к мобильной среде. Это позволяет создать в будущем защищенную среду для обмена офлайн-транзакциями между кошельками клиентов и ядром банка, моментально синхронизируя данные при восстановлении связи.

pLTE — сколько стоит альтернатива?

Создание частной сети pLTE — это инвестиции совершенно иного масштаба, чем восстановление SMS или USSD. По данным аналитического агентства Telecom Daily, в 2024–2025 годах стоимость проектов заметно варьируется:

- Компактное решение (несколько базовых станций, ограниченная территория) — 50–90 млн рублей.
- Крупный инфраструктурный проект (масштабное покрытие, интеграция с ИТ-системами) — от 200 млн рублей.
- Серьезный проект (с полным импортозамещением оборудования, резервированием и поддержкой) — затраты могут превышать 500 млн рублей.

Как пример: строительство pLTE-сети в Сочинском аэропорту на 1500 абонентов было оценено в 61,5 млн рублей. Подчеркнем: pLTE — это капитальные вложения в инфраструктуру, которые окупаются не экономией на звонках, а гарантией непрерывности работы в условиях, когда SMS и USSD уже не помогут. **Конечно, стоимость в 500 млн рублей для большинства игроков сопоставима с годовым ИТ-бюджетом, поэтому pLTE-решение подходит только для топ-10 банков с федеральным масштабом.**

Контакт-центры: последний рубеж

При исчезновении интернета голосовая связь становится единственным каналом взаимодействия с клиентом. Однако контакт-центры, которые сегодня чаще полагаются на чат-ботов и голосовых помощников, могут не выдержать лавинообразного роста нагрузки.

Стандартный контакт-центр системообразующего банка рассчитан на 20–30 тыс. звонков в день. При локальных сбоях нагрузка возрастает до 50–60 тыс., критический порог — 100–150 тыс. При полном отключении интернета число звонков может вырасти в 10–15 раз.

Кадровый аспект усугубляет ситуацию. Контакт-центры планомерно переводили общение с клиентами на чат-бот-платформы — человек в этой схеме оказался слишком дорог. **Для обслуживания 10 млн клиентов в первые сутки потребуется 30–40 тыс. обученных сотрудников — таких резервов нет ни у одного банка.**

Голосовые роботы, обрабатывающие в штатном режиме до 70% запросов, также зависят от интернета (облачные ядра). Резервные on-premise-решения имеют ограниченную емкость — по оценкам, не более 10–15% пиковой нагрузки.

В случае чрезвычайной ситуации придется срочно набирать операторов и запускать цепочку с нуля:

- 1. Найти резервное количество людей — и это еще полбеды.
- 2. Обучить их — процесс небыстрый и требующий эффективных методик.
- 3. Подготовить площадку. Крупные компании склоняются к выделенным центрам, а не к работе из дома: для «домашнего» варианта потребуются дополнительные каналы связи и контроль.
- 4. Приобрести лицензии для расширения числа операторов и выполнить масштабирование существующего решения под возросшую нагрузку.
- 5. Тем, кто полностью перевел клиентов на ботов, потребуется внедрение отдельного специализированного решения для голосового обслуживания.

Финансирование: кто должен платить

Инфраструктура дистанционного обслуживания держится на трех сторонах: операторы связи, интернет-провайдеры и банки. Вопрос распределения ответственности за доступ клиентов остается открытым.

Действующее законодательство (161-ФЗ) требует доступности платежных услуг, но не конкретизирует каналы. Положение ЦБ № 716-П трактует непрерывность как «поддержание работоспособности» без технологических требований. Операторы имеют резервные каналы для нужд силовых структур, но банковский трафик не приоритизирован. Государственная поддержка в России отсутствует. В Израиле, Южной Корее и Германии во-

просам резервирования каналов в финансовом секторе уделяется повышенное внимание на регуляторном уровне, а в некоторых случаях обсуждаются формы государственной поддержки критической инфраструктуры.

Российские же банки, за исключением крупнейших, действуют по принципу «сами разберемся», что создает зону неопределенности.

Что можно сделать уже сегодня

Ожидание регуляторных требований может обойтись дорого — потерей клиентской базы и репутации. Банкам разумно начать с малого:

- провести аудит договоров с операторами на предмет наличия резервного переключения;
- выполнить сегментацию клиентской базы с выделением критических групп (пенсионеры, получатели социальных выплат);
- разработать комплект внутренних регламентов и памяток для персонала;
- и самое важное — проинформировать клиентов о резервных каналах (USSD, DTMF, SMS) — без этого они останутся невостребованными.

Для среднего банка затраты на реновации небольшие, но чувствительные:

- Восстановление SMS-шлюзов — 1–3 млн руб.
- Интеграция USSD-платформы — 2–5 млн руб.
- Доработка DTMF-меню — 2–3 млн руб.
- Аудит контакт-центра — 3–5 млн руб.

Важное уточнение: наличие технической возможности канала (SMS-шлюз, USSD-платформа, DTMF-меню) — это только половина дела. Для каждого из этих каналов банку потребуется разработать или доработать клиентские приложения (мобильное приложение, USSD-интерфейс, голосовое меню), чтобы клиенты могли ими пользоваться. Сейчас у большинства банков таких приложений нет. Интеграция USSD-интерфейса или DTMF-меню с бэк-офисом у крупного банка со зрелым API может занять 2–3 месяца. С другой стороны, для банков с «монолитной» архитектурой — это полгода минимум.

По деньгам затраты невелики — в пределах 3–8 млн рублей на весь комплекс, но время — критический ресурс. Начинать этот процесс лучше заранее, чтобы к моменту сбоя каналы были не просто настроены, а действительно готовы к использованию клиентами.

Для крупных банков аналогичный бюджет серьезнее, это 50–150 млн рублей, он подразумевает:

- резервные ЦОДы с автономным питанием;
- спутниковые терминалы;
- гибридные маршрутизаторы с автоматическим переключением.

Особняком стоит рLTE: для системообразующих банков это может стать единственным способом гарантировать доступность услуг при полной потере внешней

связи. Однако, как уже отмечалось, такие проекты требуют бюджетов от 50–90 млн рублей для пилотных зон и до 500+ млн для полноценного покрытия. Это уже не «быстрый фикс», а стратегическое решение, которое должно приниматься на уровне совета директоров.

Ключевой вывод автора — поводов для паники нет, но начинать следует не откладывая.

От редакции PLUSworld

Представленный материал поднимает проблему, которая до сих пор находилась вне публичного обсуждения. Зависимость банковского обслуживания от интернет-каналов достигла уровня, при котором сбой глобальной сети способен парализовать значительную часть финансовых услуг.

Редколлегия считает, что вопрос резервирования требует не только технологических, но и регуляторных решений. Отсутствие четких требований ЦБ и размытая ответственность между банками, операторами и государством формируют зону неопределенности, которая в кризисной ситуации может дорого обойтись и клиентам, и финансовым институтам.

Кадровый аспект также заслуживает особого внимания: контакт-центры находятся в зоне хронического дефицита персонала. Без системных решений на уровне отрасли эта проблема неразрешима.

На этом фоне редакция полагает целесообразным обратиться к регулятору с предложением ускорить разработку нормативных требований по резервированию каналов дистанционного обслуживания.

ПЛАС



Тимур Аитов

США готовят новые ограничения против российских банков и ЦБ

Новый американский законопроект о санкциях против России предусматривает введение ограничений против Банка России, а также Сбербанка, ВТБ и Газпромбанка.

Документ обязывает президента США ввести по меньшей мере две санкционные меры против Банка России и полный пакет ограничений против трех крупнейших банков. Американским физическим и юридическим лицам запретят любые операции с этими банками, включая открытие и использование корреспондентских счетов в США. Среди других мер — блокировка активов под юрисдикцией США, а также ограничения на кредиты, экспортные лицензии и инвестиции.

При этом Минфин США может освободить от санкций иностранный банк, проводящий крупные операции с указанными российскими организациями, если сочтет это противоречащим интересам США.

Yandex B2B Tech открыла бизнесу доступ к ИИ-агентам-исследователям

Yandex B2B Tech дала компаниям возможность создавать собственных агентов-исследователей в Yandex AI Studio. Они формируют несколько поисковых запросов, отбирают релевантные источники и собирают структурированный ответ — от текста до таблиц и презентаций. Инструмент работает на обновленном Web Search.

Новый функционал позволяет бизнесу быстро собрать агента под конкретные задачи: конкурентный анализ, мониторинг бренда, поиск кандидатов или исследование рынка. Сейчас веб-поиском Yandex AI Studio пользуются более 11 тыс. компаний, которые отправляют около 400 тыс. запросов в месяц.

WB Taxi перешел в коммерческую эксплуатацию в Беларуси

Сервис заказа такси WB Taxi завершил нагрузочное тестирование и перешел в режим коммерческой эксплуатации в Минске. Теперь приложение доступно всем жителям и гостям столицы, сообщили в компании.

Зарегистрироваться в сервисе могут абоненты белорусских мобильных операторов через приложение WB Taxi, которое доступно в Google Play или App Store. В дальнейшем компания планирует совершенствовать пользовательский опыт и расширять географию работы.

WB Taxi предлагает несколько тарифов, программу лояльности и круглосуточную поддержку в чате. Для перевозчиков предусмотрены прозрачные условия сотрудничества, регулярные выплаты и возможность дополнительного заработка.

Банки без интернета — 2. ЦОД под землей, чипы и реальные приоритеты

Готовность банков к полному отключению глобальной сети на региональном или национальном уровне продолжает рассматривать наш постоянный автор Тимур Аитов, член Совета ТПП РФ по финансовому рынку и инвестициям, председатель комиссии по безопасности финансового рынка, руководитель Центра компетенций «Цифровизация финансовых технологий».

В первой части публикации мы разобрали зависимость банковской «цифры» от трех китов: электрической розетки, оптоволокну и дизельного топлива. На примере USSD-шлюзов и 4G-сетей было показано, что эти решения не панацея, а лишь фрагменты сложной мозаики.

Однако за рамками разговора остались еще два сценария, которые также требуют внимания. Первый касается физической уязвимости наземной инфраструктуры ЦОДов. Второй — возможных программно-аппаратных рисков, связанных с иностранной элементной базой. Оба сценария — не футурология, но и не повод для паники. Это вопросы из серии «какова вероятность» и «сколько мы готовы за это заплатить».

ЦОД под землей: не бункер, а разумная страховка

В первой части материала были рассмотрены риски физического уничтожения вышек и кабелей, однако предложенный спектр решений — спутниковые каналы, радиорелейка, 4G — защищает только каналы связи. Сами ЦОДы, где «живут» процессинговые ядра, по-прежнему остаются наземными стеклянными коробками в деловых центрах. Это действительно уязвимость, но не столько для «диверсантов», сколько для повседневных реалий: пока в девяти случаях из десяти кабель или системы охлаждения выходят из строя из-за некорректной работы строительной техники, обледенения или скачков напряжения.

Что дает заглубление ЦОДа на 15–20 метров? Защиту. И в первую очередь — тепловую инерцию. Массив грунта работает как естественный демпфер: при отключении активного охлаждения температура в зале растет не за 5–10 минут, как в наземном здании, а в течение 20–30 минут, а при сниженной нагрузке — до 40–50 минут. Это не панацея, но критический запас времени, чтобы запустить дублирующие системы охлаждения или переключить нагрузку на резервную площадку. Кроме того, подземный ЦОД неуязвим для большинства случайных внешних повреждений — экскаватора, упавшего дерева или обледенения вентиляционных шахт. Грунт также по-

могает ослабить помехи от атмосферных разрядов, хотя от мощного электромагнитного импульса только одно заглубление не спасет — здесь нужна дополнительная экранировка стен.

Что все это значит на практике? Строительство заглубленного ЦОДа обходится дороже наземного аналога примерно на 30–40%. Хотя подземный ЦОД дешевле охлаждать зимой, и он не требует обслуживания фасадов, заглубление — конечно, не обязательная норма для всех, а высший пилотаж для критического процессингового ядра системообразующих банков. Для большинства игроков гораздо реальнее иметь два-три наземных ЦОДа в разных регионах с автоматическим переключением между ними. Это дешевле и покрывает подавляющее большинство сценариев отказов — от блэкаута до локального ЧП.



Тимур Аитов

Аппаратные риски: гипотеза и реальность

В первой части публикации мы исходили из предположения, что отказ каналов — результат внешнего воздействия на инфраструктуру: порван кабель, отключена вышка, кончилось топливо. Это «любовой» сценарий. Он замечен, мгновенно вызывает реакцию, у банка заготовлен план действий. Гораздо сложнее «тихий» сценарий — активация скрытых режимов, заложенных в зарубежную элементную базу на этапе производства. И вот почему сегодня этот сценарий также заслуживает внимания.

Легитимность сбоя. Если «отрубился» интернет — это видно всем, это форс-мажор. Если же в чипах активируется недокументированный режим (например, принудительная деградация производительности через скрытые микрокоманды), то внешне это выглядит как обычная перегрузка: высокий пинг, потеря пакетов, приложения то открываются, то нет. Клиенты начинают чаще генерировать запросы, создавая лавину трафика, а системы безопасности могут принять это за DDoS-атаку и начать блокировать уже легитимные операции. Система мониторинга видит: процессор загружен на 20%, но транзакция идет 5 секунд вместо 0,5. Никто не сможет мгновенно доказать, что это внешнее воздействие, а не «внезапный рост нагрузки» или «ошибка в новом релизе». Банк попытается «лечить» софт, но не получит результата: аппаратная закладка продолжит свою работу.

Возможная картина атаки. В пиковые часы процессинг проходит 8–10 тыс. транзакций в секунду. В штатном режиме 95% операций по картам и СБП укладываются в 300–400 мс. Если активируется «тихий» сценарий, время принятия решения по каждой транзакции искусственно увеличивается на 150–200 мс. Переводы по СБП между людьми начинают уходить не за пару секунд, а за 15–20. Пользователи дублируют платежи, создают лавину запросов. Банк смотрит на свои системы: ни один дашборд не показывает атаку. Просто «все стало тормозить». Такой сценарий действительно опаснее обрыва кабеля — он маскируется под внутреннюю проблему.

Тем не менее отметим следующее. Внедрение аппаратной закладки в промышленные партии процессоров требует колоссальных затрат. Поэтому такой инструмент — скорее оружие стратегического сдерживания, и его вряд ли станут раскрывать ради точечного удара по сервису СБП. Противнику дешевле и эффективнее атаковать через софт, ошибки в обновлениях или человеческий фактор. Кроме того, даже если заменить центральный процессор на отечественный, остаются сетевые карты, контроллеры дисков и управляющие микросхемы — все они обычно импортные и потенциально содержат аналогичные риски. Здесь угроза исходит не от самих карт, а от микрокода, который выполняется на ARM-процессорах.

Основная здесь иллюзия — «мы все проверили». Прежде всего нужно признать — проверка зарубежной элементной базы на наличие скрытых триггеров в промышленных масштабах невозможна. Это требует вскрытия кристаллов и анализа на уровне схемотехники и микрокода — процедуры, которая на один чип занимает недели, но которую никто не проводит на десятках тысяч серверов. Сертификаты ФСТЭК, которые есть у большинства импортных устройств, подтверждают поведение в штатных режимах, но не являются гарантией от скрытых триггеров. Это тоже важный нюанс.

Отметим и самое главное: в текущих геополитических условиях она может рассматриваться как штатный инструмент давления. Противник, теоретически, может сделать любой крупный банк ненадежным для клиентов, не взрывая ЦОД и не глуша связь. И все это — без единого выстрела, без красных лампочек на дашбордах. Это оружие, результат применения которого выглядит как «технический сбой». И полностью сегодня исключать, что такие механизмы уже заложены в оборудование, неосмотрительно.

Что делать? Две параллельные линии обороны

Из сказанного следует простой и неудобный вывод: в рамках анализа для полной уверенности банкам нужны две независимые линии защиты, и они лежат в разных плоскостях.

Линия первая — физическая. Для ее организации следует выносить критичные ЦОДы под землю. Не в подвалы бизнес-центров, а именно в заглубленные сооружения с автономным охлаждением, топливным хозяйством на 72 часа и экранированием. Это дорого. Но это страховка от блэкаута, физического уничтожения и, в сочетании с экранированием, — от ЭМИ.

Выносить критичные ЦОДы также можно и на географически распределенные площадки — в разные регионы. Использовать при этом следует не одну платформу, а несколько: часть нагрузки на одном «железе», часть — на другом. Если один сегмент «замедляется» или выходит из строя, нагрузка автоматически перетекает к другим. Эта схема дешевле строительства бункеров и покрывает большинство физических рисков. (Хотя, если взять 3D-карту России, на ней можно увидеть огромное количество уже существующих заглубленных объектов, различных выработок и т.д., т.п. Что может приятно удивить тех, кто будет вынужден взяться за реализацию данной проблемы.) К слову, Банк России в своих рекомендациях по обеспечению непрерывности деятельности (в частности, в подходах к построению системно значимых объектов) ориентирует кредитные организации именно на территориальную распределенность критичных мощностей.

Линия вторая — аппаратная. Выводить ядро процессинга (авторизация, расчет лимитов, обработка транзак-

ций) на проверяемые аппаратные платформы с доверенным российским чипом либо на изолированные кластеры (там, где это критично). На все не получится сразу — но хотя бы на критический минимум, без которого банк не работает в принципе. Это уже шаг в нужную сторону и не «импортозамещение ради отчетности». Вторая линия важна — без нее мы рискуем построить сверхнадежный бункер, который потенциально может быть «выключен» одним микрокодом дистанционно, даже без какого-либо физического воздействия.

Конечно, и остальные привычные меры противодействия (копирование баз данных, ограничители запросов на входе в систему, контроль за действиями администраторов, регулярные проверки и вход по паролю плюс ключ-токен (двухфакторная аутентификация) также никто не отменял.

От редакции PLUSworld

Электрическая розетка, оптоволокно, дизельное топливо — три фундаментальных элемента, на которых держится сегодня банковская «цифра». Это основа. Но это лишь самый нижний, базовый уровень пирамиды устойчивости.

Над ним располагается уровень защиты данных и приложений — резервное копирование баз, ограничители запросов, автоматическое отключение «тормозящих» сервисов, контроль целостности ПО. Это то, что привычно называют «софтом» и что регулярно проверяют в рамках пентестов.

Выше — уровень физической инфраструктуры: несколько географически распределенных ЦОДов, разные типы серверного оборудования, чтобы не зависеть от единой платформы и единой точки отказа.

А на самом глубоком, фундаментальном уровне — аппаратная платформа: процессоры, контроллеры ввода-вывода, управляющие микросхемы, микрокод. Именно здесь сегодня зияет главная неизвестность: мы не знаем, что заложено в импортные чипы на этапе их производства, и не можем это проверить в промышленных масштабах. Сертификаты ФСТЭК подтверждают поведение в штатных режимах, но не гарантируют отсутствия скрытых триггеров, которые могут быть активированы удаленно. Этот фундаментальный уровень — самый сложный для контроля, но именно он определяет, можно ли доверять всей надстройке.

А вот на самом верху, на поверхности, — каналы связи, USSD-шлюзы, контакт-центры, спутниковые терминалы. Все то, что сегодня активно обсуждается на отраслевых форумах и куда преимущественно направляются бюджеты.

При этом три нижних уровня, образующие фундамент, без которого все остальное бессмысленно, остаются за рамками публичных стресс-тестов и реальных инвестиционных приоритетов. Пришла пора менять всю эту конструкцию. Но не потому что «завтра война», а потому что

повседневные риски случаются регулярно: экскаватор порвал кабель, в дата-центре отключилось охлаждение, обновление привело к лавинному росту ошибок. Именно эти сценарии — не гипотетические, а реальные — составляют 95% инцидентов.

Банк России, последовательно ужесточая требования к обеспечению непрерывности и информационной безопасности (в частности, в Положении 716-П и методических рекомендациях по системно значимым объектам), смещает фокус с формальных отчетов на доказательство реальной устойчивости сервисов. А значит, приоритеты, о которых говорится в этом материале, — не абстрактные рассуждения, а формирующийся регуляторный тренд, который в ближайшие 2–3 года станет обязательным требованием для всех системообразующих кредитных организаций.

ПЛАС

КАЛЕЙДОСКОП

В июне 2026 года доля отказов по заявкам на POS-кредиты составила 86,1%

По данным НБКИ, доля отказов по заявкам на POS-кредиты (кредиты гражданам, предоставленные в торговых точках) в июне 2026 года составила 86,1%, увеличившись по сравнению с предыдущим месяцем на 1,2 процентного пункта (п.п.) (в мае 2026 года — 84,9%).

В то же время по сравнению с аналогичным периодом 2025 года данный показатель, напротив, сократился на 1,1 п.п. (в июне 2025 года — 87,1%).

Наибольшие доли отказов по заявкам на POS-кредиты в регионах РФ (среди 30 регионов-лидеров по количеству заявок на данные кредиты) в июне 2026 года были отмечены в Ставропольском (87,3%), Краснодарском (87,0%) и Забайкальском (86,9%) краях, а также в Оренбургской (86,9%) и Челябинской (86,9%) областях. В свою очередь наименьшие доли отказов по заявкам на POS-кредиты в топ-30 регионов в июне были зафиксированы в Москве (82,8%), Санкт-Петербурге (82,9%), Приморском крае (83,0%), Воронежской области (83,6%) и Хабаровском крае (83,8%). Относительно низкий показатель отказов в них свидетельствует о более качественном потоке заявителей и/или более мягкой скоринговой политике банков в этих регионах.

При этом наиболее серьезная динамика роста доли отказов по заявкам на POS-кредиты (среди 30 регионов-лидеров по количеству заявок на данные кредиты) в июне 2026 года по сравнению с предыдущим месяцем была отмечена в Приморском крае (+2,9 п.п.), Республике Татарстан (+2,1 п.п.) и Нижегородской области (+1,8 п.п.), а также в Алтайском крае (+1,7 п.п.) и Ленинградской области (+1,6).



ПОЛНЫЙ ЦИКЛ
ОРГАНИЗАЦИИ
ДЕЛОВЫХ
МЕРОПРИЯТИЙ



ПОЧЕМУ ВЫБИРАЮТ НАС?

- Авторитетность
- Популярность
- Актуальность
- Влияние
- Медийность
- Широкая отраслевая и массовая медиаподдержка
- Вовлеченность
- Интерес
- Коммуникации

ВЕБИНАРЫ
КРУГЛЫЕ СТОЛЫ
КОНФЕРЕНЦИИ
СТРАТЕГИЧЕСКИЕ СЕССИИ
ПРЕСС-КОНФЕРЕНЦИИ
БИЗНЕС-ЗАВТРАКИ

ПРЕВРАЩАЕМ ИДЕИ
В МАСШТАБНЫЕ СОБЫТИЯ

Идеальное событие начинается задолго до приглашения

Кредит в цифровых рублях? — А зачем мне они?
Большинство участников опроса, проведенного с 2 по 9 июня 2026 года в нашем Телеграм-канале, пока не рассматривают возможность оформления кредита в цифровых рублях.

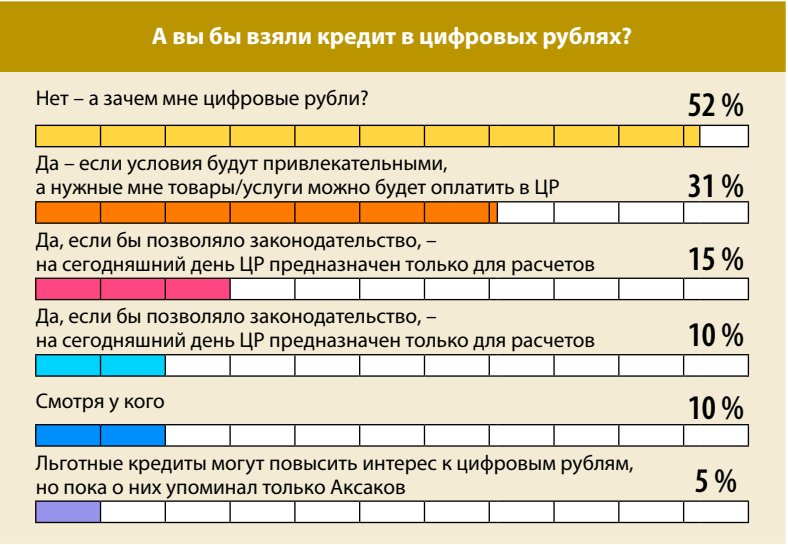
52% респондентов заявили, что не видят для себя необходимости в использовании цифрового рубля и не готовы оформлять займы в российской ЦВЦБ.

В то же время почти треть опрошенных (31%) допускают возможность получения кредита в цифровых рублях при условии, что условия кредитования окажутся привлекательными, а приобретаемые товары и услуги можно будет оплачивать с использованием цифрового рубля. Это свидетельствует о том, что интерес к новому финансовому инструменту во многом зависит от развития инфраструктуры его применения и практических преимуществ для потребителей.

С ними согласны еще 15% участников ПЛАС-Опроса, которые готовы рассмотреть такой кредит, если процентная ставка окажется ниже, чем по аналогичным займам в традиционных рублях. Таким образом, экономическая выгода остается одним из ключевых факторов, способных стимулировать спрос на новые финансовые продукты.

При этом 10% респондентов отметили, что воспользовались бы кредитом в цифровых рублях, если бы это позволяло действующее законодательство. Сегодня цифровой рубль предназначен исключительно для расчетных операций, а механизмы кредитования в этой форме валюты не предусмотрены.

Еще 10% участников исследования заявили, что их решение будет зависеть от статуса конкретного кредитора, что указывает на сохраняющуюся важность доверия к финансовым организациям независимо от формы денег.



Отдельно 5% опрошенных отметили, что интерес к цифровому рублю могли бы повысить льготные кредитные программы. Однако пока подобные инициативы остаются на уровне обсуждений. В частности, возможность предоставления льготных кредитов в цифровых рублях ранее упоминалась главой Комитета Госдумы по финансовому рынку Анатолием Аксаковым.

Эксперты отмечают, что результаты опроса демонстрируют осторожное отношение граждан к новым финансовым технологиям. Несмотря на высокий уровень скепсиса, почти каждый второй респондент в той или иной степени готов рассматривать кредиты в цифровых рублях при наличии понятных ему преимуществ — более низких ставок, выгодных условий использования или расширения сфер применения цифровой валюты. Это говорит о том, что дальнейшее развитие цифрового рубля будет во многом зависеть от его практической ценности для населения и формирования привлекательных пользовательских сценариев.

В какой мере все это сбудется — поживем-увидим!

Шестидесятикратный рост стоимости SMS-оповещения банковских клиентов – результат монополии телеком-операторов
Как показывают результаты ПЛАС-Опроса, проведенного PLUSworld с 27 мая по 2 июня 2026 года в нашем Телеграм-канале, большинство респондентов связывают 60-кратное удорожание SMS-уведомлений для банков с проблемами конкуренции на телекоммуникационном рынке.

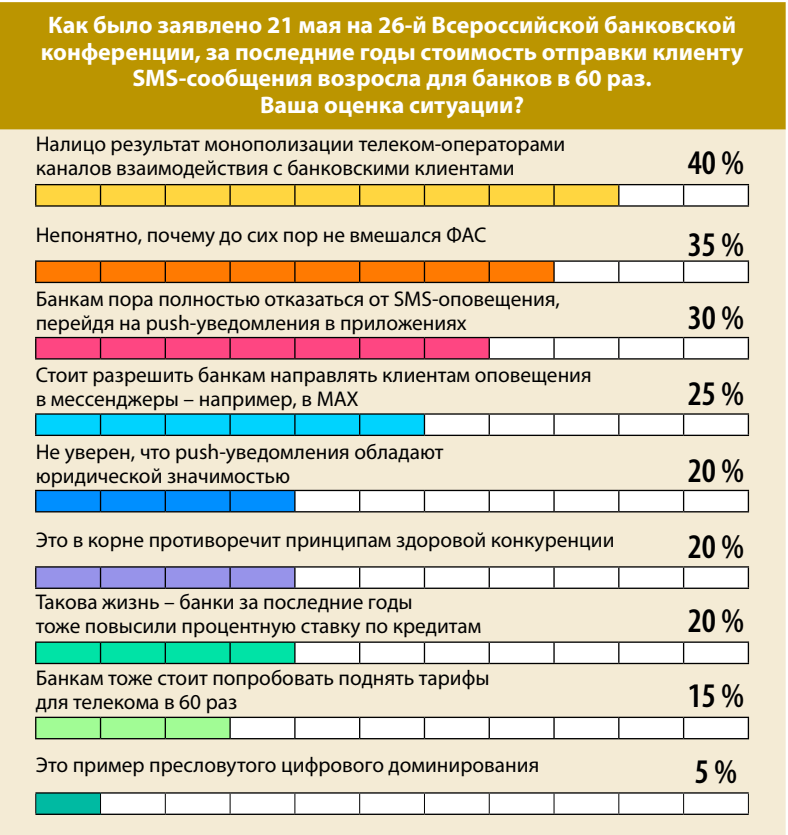
Наиболее популярным ответом стала версия о монополизации телеком-операторами каналов взаимодействия с банковскими клиентами — ее поддержали 40% респондентов. Еще 35% участников отметили, что не понимают, почему в ситуацию до сих пор не вмешалась Федеральная антимонопольная служба. Таким образом, значительная часть аудитории рассматривает проблему не как рыночный процесс, а как следствие недостаточной конкуренции и регулирования.

Одновременно заметна поддержка технологических альтернатив традиционным SMS. Треть опрошенных (30%) считают, что банкам следует полностью отказаться от SMS-информирования и перейти на push-уведомления в мобильных приложениях. Еще 25% выступают за расширение каналов коммуникации и предлагают разрешить банкам направлять клиентские уведомления через мессенджеры, включая отечественные платформы.

Принимайте участие в ПЛАС-Опросах!

Ваше мнение важно для банковского и финтех-сообщества.

Участвуйте в независимых экспертных оценках тенденций, событий и проблем рынка!



При этом отношение к отказу от SMS остается неоднозначным. Каждый пятый респондент (20%) сомневается в достаточной юридической значимости push-уведомлений. Это свидетельствует о сохраняющихся опасениях относительно правового статуса цифровых каналов связи и их способности заменить SMS в вопросах официального информирования клиентов.

Также 20% участников опроса считают сложившуюся ситуацию противоречащей принципам здоровой конкуренции. Еще столько же придерживаются более прагматичного подхода, отмечая, что банки сами за последние годы повышали стоимость кредитов, поэтому рост тарифов со стороны телеком-операторов выглядит закономерным рыночным процессом.

Наименее популярными оказались эмоциональные и радикальные оценки. Лишь 15% респондентов поддержали идею зеркального повышения банками тарифов для телеком-компаний, а 5% назвали происходящее примером «цифрового доминирования».

В целом результаты опроса демонстрируют, что общественное мнение склоняется к восприятию резкого роста стоимости SMS-рассылок как следствия ограниченной конкуренции на рынке коммуникационных услуг. Одновременно респонденты видят перспективу в развитии альтернативных каналов взаимодействия банков с клиентами.

Насколько они правы — поживем-увидим!

Деньги должен контролировать человек, а не ИИ
Большинство читателей PLUSworld пока не готовы передать искусственному интеллекту полный контроль над оплатой покупок. Это следует из результатов опроса, проведенного PLUSworld с 18 по 27 мая 2026 года в нашем Телеграм-канале, о готовности пользователей доверить ИИ самостоятельные платежи от своего имени.

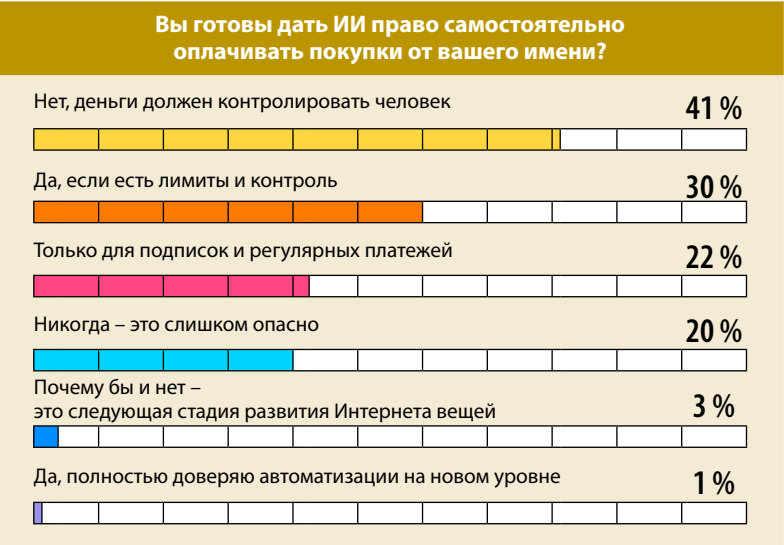
Самым популярным ответом оказался вариант «деньги должен контролировать человек» — его выбрали 41% участников. Еще 20% респондентов заявили, что никогда не согласятся на подобный сценарий, считая его слишком опасным. Таким образом, более половины опрошенных воспринимают финансовую автономность ИИ скорее как риск, чем как удобство.

При этом заметна и другая тенденция: пользователи готовы делегировать ИИ отдельные функции, если сохраняется возможность контроля. Так, 30% респондентов согласны доверить оплату алгоритмам при наличии лимитов и механизмов подтверждения операций. Еще 22% готовы использовать ИИ только для подписок и регулярных платежей — то есть в предсказуемых и повторяющихся сценариях.

Полностью доверяют автоматизации лишь единицы: 3% считают подобный подход следующим этапом развития интернета вещей, а 1% готовы передать ИИ финансовые решения практически без ограничений.

Насколько они правы — поживем-увидим!

По мнению ряда наших внешних экспертов, результаты показывают, что подавляющее большинство головосававших пока еще абсолютно не в теме. Исключение составляют, пожалуй, тот 1% опрошенных, кто ответил, что абсолютно доверяет ИИ в вопросах оплаты покупок. Разумеется, на самом деле риски имеются, но вполне контролируемые. На самом деле схема агентных платежей построена как раз на том, что необходимости в каком-либо доверии к агенту нет.





Блокировка Telegram — борьба с ветряными мельницами

Итак, почти половина наших читателей (46%) на вопрос, как блокировка Telegram скажется на их работе, ответила: все как обычно — борются не с причинами, а с ветряными мельницами. Таковы результаты ПЛАС-Опроса, проведенного с 23 марта по 30 марта 2026 года в нашем Телеграм-канале.

Чуть больше трети респондентов (25%) призналась: часть процессов встанет, но переходить на другие платформы они пока не готовы.

В свою очередь, 18% читателей считают, что тем, кто отвечает за данное направление создания собственных национальных мессенджеров и задачи миграции на них, нужно было думать гораздо раньше, а теперь решение проблемы прикрывают заботой о безопасности.

При этом 16% наших читателей уже приняли простое решение перейти на отечественный аналог Telegram, несмотря на ожидаемые значительные потери клиентов и другие негативные последствия данной миграции.

8% счастливичиков отметили, что вопрос для них неактуален: «Наша компания — резидент страны, где работа Telegram не блокируется».

И, наконец, 6% не опасаются, что блокировка Telegram помешает их работе «в силу ее специфики». Таким образом, спокойно воспринимают блокировку Telegram в общей сложности 14% опрошенных, да и то в силу географических и профессиональных моментов.

Не слишком ли они оптимистично настроены? Поживем-увидим!

Ждет ли нас в 2026 году системный банковский кризис?

Итак, почти четверть наших читателей (21%) придерживается мнения: все зависит от ситуации в экономике — пока банки подъедают «накоплен-

ный жирок», но он не вечен. Таковы результаты ПЛАС-Опроса, проведенного PLUSworld с 10 по 29 декабря 2025 года в нашем Телеграм-канале.

При этом 18% респондентов уверены, что кризис вероятен, а 9% — неизбежен при сохранении текущих трендов, включая рост доли проблемных кредитов.

Впрочем, 16% уверены, что кризиса, скорее всего, не будет, и столько же — что все зависит от геополитической ситуации.

Те же 16% затрудняются ответить, но «хотели бы знать реальное мнение Эльвиры Набиуллиной».

12% уверены, что все зависит от ЦБ. И, наконец, только 3% читателей выбрали ответ «Все зависит от удовлетворенности руководства страны политикой ЦБ».

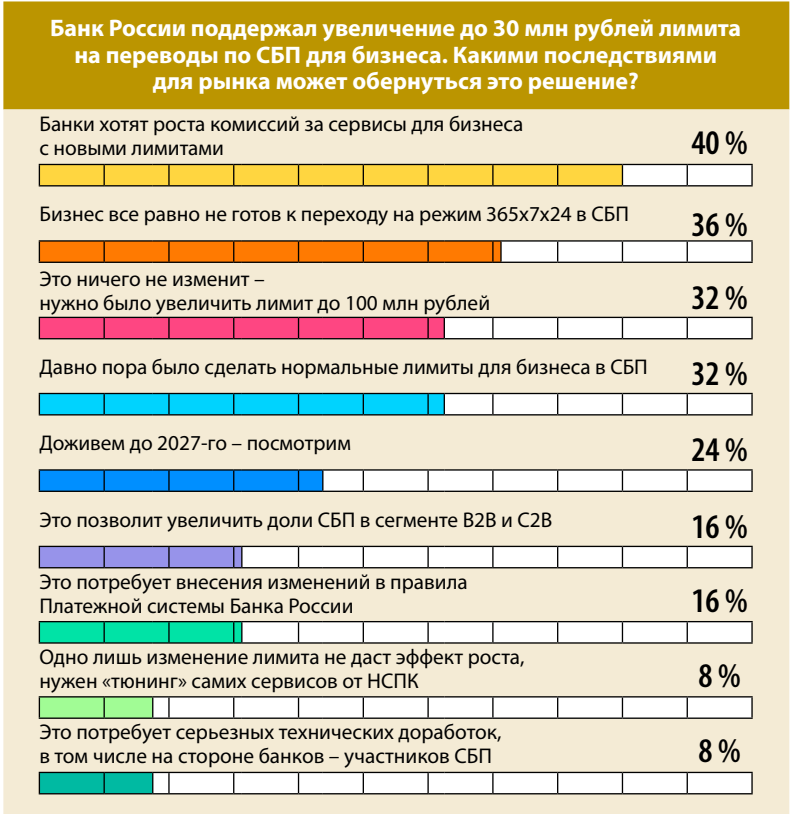
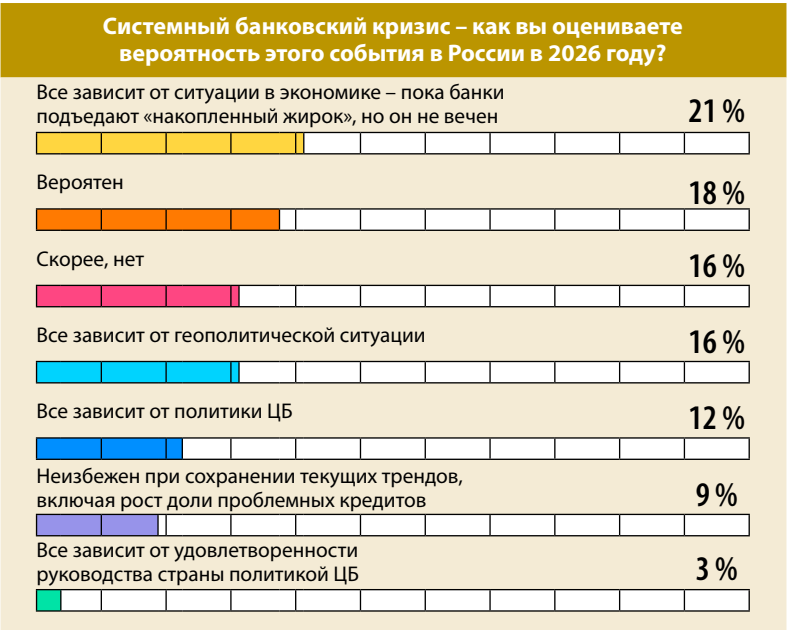
Зависит ли что-то от удовлетворенности нас с вами, — поживем-увидим!

До 30 млн рублей — новый лимит СБП-переводов для бизнеса. Банки хотят роста комиссий

Итак, большинство респондентов (40%), отвечая на вопрос «Какими последствиями для рынка может обернуться решение увеличить до 30 млн рублей лимит на переводы по СБП для бизнеса, которое поддержал ЦБ», ответили, что дело в банках, которые хотят роста комиссий за сервисы для бизнеса с новыми лимитами. Таковы результаты ПЛАС-Опроса, проведенного PLUSworld с 13 по 18 мая 2026 года в нашем Телеграм-канале.

При этом 36% читателей заметили, что бизнес все равно не готов к переходу на режим 365x7x24 в СБП. А 32% уверены, что новая цифра ничего не изменит — нужно было увеличить лимит для бизнеса до 100 млн рублей.

Столько же опрошенных (32%) уверены, что давно пора было сделать нормальные лимиты для бизнеса



в СБП, а вдвое меньше (16%) считают, что это позволит увеличить доли СБП в сегменте B2B и C2B.

Реалисты напоминают, что новые лимиты потребуют внесения изменений в правила Платежной системы Банка России (16%), а также серьезных технических доработок, в том числе на стороне банков — участников СБП (8%). Максималисты уверены, что одно лишь изменение лимита не даст эффект роста, нужен «тюнинг» самих сервисов от НСПК (8%). И при этом почти каждый четвертый участник опроса (24%) проявил осторожность, выбрав вариант: «Доживем до 2027-го — посмотрим». Что ж, действительно — поживем-увидим!

Борьба с кибермошенничеством — реального прогресса на горизонте трех лет достичь не удастся

Ровно треть респондентов (33%) убеждена: реального прогресса в борьбе с кибермошенничеством на гори-

зонте трех лет достичь не удастся, возможна лишь его минимизация, да и то на ограниченный срок. Таковы результаты ПЛАС-Опроса, проведенного PLUSworld с 27 февраля по 10 марта 2026 года в нашем Телеграм-канале.

Чуть меньшая доля экспертов (29%) заняла менее категоричную позицию по поводу заданного вопроса — прогресса достичь скорее удастся, чем нет.

В свою очередь, четверть опрошенных (25%) выбрали симметричный ответ «Скорее нет, чем да».

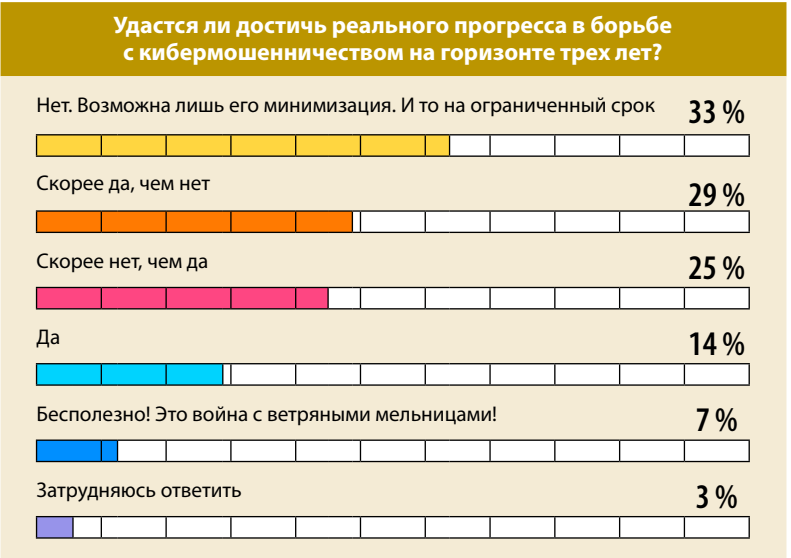
«Бесполезно, противодействие кибермошенничеству — это война с ветряными мельницами!» — этот вариант ответа популярен у 7% наших читателей.

Таким образом, в общей сложности усомнились в возможности достижения цели 65% читателей (напоминаем, голосование позволяло выбрать несколько вариантов ответа, выбравших «Скорее да, чем нет» мы в суммарную долю по понятным причинам не включили).

И только 14% респондентов показали себя оптимистами, сказав твердое «да» в отношении перспектив прогресса в борьбе с кибермошенниками.

Характерно, что 3% опрошенных затруднились ответить на поставленный вопрос.

Правы ли эти осторожные эксперты на фоне сегодняшней во многом неопределенной ситуации на данном фронте? Поживем-увидим!



Данные вопросы наряду с другими актуальными темами будут рассматриваться в рамках наших ПЛАС-Форумов 2026 года!

Приглашаем Вас принять активное участие в нашей инициативе, позволяющей банковскому и финтех-сообществу, а также представителям регуляторов учитывать объективные и независимые экспертные оценки различных тенденций, событий и проблем рынка. Ждем Ваших встречных предложений по поводу тем, актуальных для проведения новых опросов.

Гарантируем размещение наиболее интересных вопросов в рамках нашего сервиса «ПЛАС-Опрос»!

Принимаем Ваши пожелания на адрес нашего единого новостного сервиса news@plus-alliance.com!

Анонимность — как личную, так и Вашей бизнес-структуры — наш бренд ПЛАС (Since 1993) гарантирует!

Журнал «ПЛАС (Платежи. Системы. Карточки). PLUS»
№ 07–08 (339–240) 2026

Учредитель – издательство ООО «ПЛАС»,
являющееся также учредителем электронных СМИ PLUSworld.ru
и Retail-Loyalty.org, издателем Толкового англо-русского
Словаря ПЛАС

Издатель: ООО «ПЛАС»
Генеральный директор: Александр Гризов
Маркетинг: Константин Гризов
Главный редактор: Михаил Свищёв
Редактор: Андрей Чернецов
Редактор новостей: Игорь Зайцев news@plusworld.ru
Главный художник: Сергей Лазарев
Корректор: Наталия Афанасьева
Фото на обложке: Илья Галиуллин, генеральный директор uniTodi

Адрес редакции: Россия, 117246, Москва, Научный пр-д, 19
телефон/факс: +7 495 961-10-65
email: marketing@plusworld.ru
web-site: PLUSworld.ru
англ. версия: PLUSworld.org

Отпечатано в ООО «ВИВА-СТАР»
107023, г. Москва, ул. Электrozаводская, д. 20, стр. 8,
этаж 2, помещение 1

Журнал зарегистрирован Министерством РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации **ПИ № 77-15554** от 20.05.2003.

Редакция не несет ответственности
за содержание рекламных материалов.

© **ООО «ПЛАС».**
Полное или частичное воспроизведение или размножение
материалов журнала допускается только с письменного
разрешения редакции.
Точка зрения авторов статей может не совпадать
с точкой зрения редакции.
При перепечатке ссылка на журнал обязательна.

Номер подписан в печать 24.08.26 Выход в свет: 04.09.26.
Цена свободная.



Фото
с Международного
ПЛАС-Форума
«Платежный
бизнес и денежное
обращение 2025»

РЕКЛАМА В НОМЕРЕ

uniTodi («ПБФ ДИСТРИБУЦИЯ» / ООО «Юнитоди») обл. 1
Info@unitodi.com
Unitodi.ru

PrintTrade стр. 22
inktrade.ru
Alisa.a@inktrade.ru
8 (896) 85779227

ART Fintech стр. 26
art-fintech.ru
+7 (495) 1206020

LIFE PAY
(ООО «ПЛАТЕЖНЫЙ СЕРВИС ПРОВАЙДЕР») обл. 2
life-pay.ru
max.ru/id9701010050_biz
t.me/lifepay_kassa
vk.ru/lifepay

Compliance Control
(ООО «КОМПЛАЙНС КОНТРОЛ») стр. 34
compliance-control.ru
info@compliance-control.ru
+7 499 136 2766

ООО «РусБИТех-Астра» / Группа Астра обл. 3
https://astra.ru/
8 (800) 222 07 00
info@astralinux.ru

ООО «ЭЙЧ.ЭС.АР» / HSR обл. 4
hhttps://hsrus.ru/
info@hsrus.ru
8 (800) 600-81-51



Реклама

astra.ru

HSR

ТЕХНОЛОГИИ ДЛЯ ФИНАНСОВОГО СЕКТОРА

“

НАДЕЖНОСТЬ.
ТЕХНОЛОГИИ.
ПАРТНЕРСТВО.

HSR-российская компания,
специализирующаяся на поставке,
разработке и сервисом обслуживании
для банков и финансовых организаций.



ПОСТАВКА

Надежное оборудование
от проверенных партнёров



СЕРВИСНОЕ ОБСЛУЖИВАНИЕ

Профессиональная поддержка
и техническое обслуживание
по всей России



КАСТОМИЗАЦИЯ БАНКОМАТОВ

Индивидуальные решения
под задачи вашего бизнеса



СКЛАД ЗАПАСНЫХ ЧАСТЕЙ

Широкий ассортимент
и оперативная доставка



СЧЕТНО-СОРТИРОВОЧНАЯ МАШИНА
CASHGEAR - СОБСТВЕННАЯ
РОССИЙСКАЯ РАЗРАБОТКА



E-MAIL
info@hsrus.ru



САЙТ
<https://hsrus.ru>



ТЕЛЕФОН
8 (800) 600-81-51

