

XXVI Всероссийская банковская конференция

Цифровая финансовая система России: цифровые валюты, токенизация и искусственный интеллект

Платёжная безопасность: от защиты транзакций к киберустойчивости бизнеса

Тимур Аитов

Член Совета ТПП РФ по финансовому рынку и инвестициям

Председатель комиссии по безопасности финансового рынка

Руководитель Центра компетенций «Цифровизация финансовых технологий»



Почему пора менять «оптику»?

Фокус мировой и российской практики сместился с классической технической защиты ИБ на **киберустойчивость (Cyber Resilience)**. Раньше в ИБ настраивали антивирусы и запрещали флешки. Сегодня ИБ — неотъемлемая часть бизнес-стратегии.

Ключевой вопрос теперь не «Можно ли нас взломать?», а «**Как пережить атаку и продолжить работу?**». Атаки и утечки признаются неизбежной частью реальности.

Потери при простое

бизнес-показатель

Скорость восстановления

метрика устойчивости

Доверие клиентов

главный актив

Устойчивость измеряется в конкретных бизнес-показателях: сколько компания потеряет при простое, как быстро восстановится и сохранит доверие клиентов.



Тактический срез: что говорит статистика

7,4 млрд ₽

похищено

1,8 трлн ₽

предотвращено

495,8 тыс.

заявлено клиентами

16,8 млн

отражено попыток

Ключевую роль в снижении потерь сыграл **«период охлаждения»** (Указание ЦБ № 6820-У) — клиент может отказаться от перевода в течение двух дней.

Банк России расширил перечень подозрительных признаков (до 7 ключевых). Система «Антифрод» заработала, банки перешли с реактивной на проактивную защиту. ИИ блокирует не транзакцию, а саму попытку.



Тревожная сторона: социальная инженерия

По данным ФинЦЕРТ, число инцидентов с методами социальной инженерии демонстрирует устойчивый **двузначный рост**. До 80% успешных атак — через обман человека, а не через взлом технологий.

Тактика меняется: холодный обзвон → точечный вишинг (voice phishing) с использованием ИИ, дипфейков и генеративных моделей. Злоумышленники изучают жертву, собирают цифровой след и готовят атаку.

 Возврат по картам
~10%

 Возврат по СБП
ещё ниже

 Электронные кошельки
менее 2%

Главный сдвиг: цель атаки — не деньги, а доверие к инструментам, подтверждающим платёж.



Стратегический горизонт: три направления атак на доверие

Злоумышленник понял: незачем ломать саму платёжную систему, если можно подорвать три основания, на которых держится доверие к любому платежу:

1. **Искусственный интеллект**, которому банки делегируют решение о легитимности платежа.
2. **Цифровая идентичность клиента**, которая подтверждает его личность.
3. **Каналы связи и межбанковское взаимодействие**, по которым передаются платёжные данные.

Противник целится не в деньги, а в нашу способность отличить клиента от мошенника.



Первое — атака на антифрод-ИИ

- **Состязательные атаки (adversarial attacks)** — злоумышленник изучает модель и формирует математически легитимную, но мошенническую транзакцию.
- **«Отравление» данных (data poisoning)** — на этапе обучения модели.

MITRE, NIST, а с декабря 2025 года и ФСТЭК включила эти угрозы в Банк данных угроз (БДУ) как класс угроз для объектов КИИ, в том числе для платёжной инфраструктуры.

«Вы учли риски для вашей AI-модели?» — спросят на аттестации. Не учли — предписание.

Рынок инструментов для обмана банковского ИИ только зарождается, но реагировать нужно уже сейчас.



Второе — дипфейки и подрыв биометрии

«Обман с использованием дипфейков — одна из ключевых угроз 2026 года» (зампред ЦБ)

Схема «фейк-босс» набирает обороты. Голос синтезируют по 3–5 секундам видео. От скриптовых роботов переходят к диалоговым ИИ-агентам. Привычные маркеры (акцент, пауза) скоро перестанут работать.

 Атака направлена не на банк, а на клиента. Мошенники собирают фото и голоса для обмана близких, друзей и коллег.

 Банковские системы от дипфейков защищены, но люди им верят. Появляются атаки, где к жертве обращается «удаленная» публичная личность.



Третье — компрометация каналов связи и межбанковского взаимодействия

- API-шлюзы, межбанковский трафик, DDoS на транспортную сеть.
- **Особенно уязвим мобильный канал:** устаревшие протоколы SS7 позволяют перехватывать SMS с кодами 2FA.

Решение: защищённые протоколы на основе российского стандарта криптографической защиты. В перспективе — защищённая мобильная инфраструктура БРИКС как часть независимой транзакционной архитектуры.

Переходим от защиты отдельной транзакции к защите всей цепи доверия: от клиента через банк до контрагента.



Можно ли применять глобальные рекомендации в России?

Доклад WEF + KPMG «AI and Cyber: Empowering Defenders» — **карта местности, а не навигатор.**



Что берём:

4 шага внедрения AI
Экономия \$1,9 млн на инциденте



Три ограничения:

1. Санкции + дефицит GPU NVIDIA
2. Регуляторика (Кодекс этики ИИ ЦБ, БДУ ФСТЭК)
3. «Зоопарк форматов» данных

Сначала фундамент (данные), потом ИИ — иначе модель «слепнет».



Дорожная карта для лидеров рынка

Крупные банки — три приоритета

1. Устойчивость ИИ: adversarial-тестирование как пентесты.
2. Биометрия нового поколения:
лицо+голос+поведение + детекция дипфейков.
3. Защита API и межбанковских каналов.

Можно ждать, когда рекомендации станут обязательными, а можно уже сейчас закладывать их в архитектуру. Второй путь — конкурентное преимущество.



Стратегия для малых банков: коллективная устойчивость

Позиция ЦБ: «Киберустойчивость всей системы определяется уровнем защиты её наименее защищённых участников» (Михаил Мамута).

Проблема: нет ресурсов на собственные лаборатории.

Их сила: скорость подключения к отраслевым решениям.

Что делать:

- ✓ Готовые сервисы на рынке
- ✓ Работа с ФинЦЕРТ — обмен индикаторами
- ✓ Цифровая гигиена сотрудников и клиентов

Главная ошибка: копировать стратегию гиганта на мизерном бюджете.



Заключение: от защиты к устойчивости

Что сделать уже завтра:

◆ Протестируйте антифрод-модель

◆ Приведите данные в порядок

Тактические победы не спасут от стратегического поражения.

Либо Мы строим киберустойчивость, либо её строят мошенники.

К 2030 году выбора не останется.

Тимур Аитов | ТПП РФ, комиссия по безопасности финансового рынка



