УДК 004.056:336.71

ТРАНСФОРМАЦИЯ СТРАТЕГИЙ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В БАНКАХ ПОД ВЛИЯНИЕМ НОВЫХ ТЕХНОЛОГИЙ ПРИ ПЕРЕДАЧЕ ДАННЫХ

Федорова П. А.[1]
Научный руководитель – преподаватель Волхонцев А. А.[1]
[1]Университет ИТМО
fedpol06@mail.ru

Введение

Современный банковский сектор переживает кардинальную трансформацию подходов к информационной безопасности (ИБ), вызванную стремительным развитием технологий передачи данных и ужесточением регуляторных требований [1]. Если ранее дискуссии фокусировались на внедрении новых технологий для повышения операционной эффективности, то в 2026 году на первый план выходит двойственная природа технологических изменений. Усложнение каналов передачи данных создает новые векторы атак, но также на основе передовых технологий формируется «цифровой иммунитет» кредитных организаций. Анализ зарубежного опыта показывает, что центральные банки активно реагируют на внедрение инноваций. В Евросоюзе вводятся обязательные требования к использованию стандарта ISO 20022 в платежных сообщениях, в Великобритании и Бразилии разрабатываются стандарты Открытых API, а Резервный банк Индии ограничивает деятельность иностранных компаний для защиты национального рынка [3; 4]. Банк России, в свою очередь, декларирует риск-ориентированный подход к внедрению искусственного интеллекта, делая акцент на мониторинге киберугроз. Однако для малых и средних банков, традиционно ограниченных в ресурсах, эти изменения создают критические риски, которые требуют пересмотра устоявшихся стратегий управления ИБ.

Основная часть

Ключевой особенностью текущего момента стало появление качественно новых угроз, эксплуатирующих доверие пользователей к привычным технологиям передачи данных. Одним из таких векторов выступает квишинг – тип фишинговой атаки с использованием QR-кодов для кражи учетных данных. Фундаментальные недостатки протокола SS7 позволяют перехватывать сообщения, а метод SIM-своп позволяет перевыпускать SIM-карты по поддельным документам, делая одноразовые пароли небезопасными [2]. SMS-подпись не обеспечивает целостность документа и не позволяет достоверно установить волеизъявление конкретного лица при передаче данных, что подтверждается определением Верховного суда РФ от 08.07.2005 года №78-КГ25-12-К3.

На устранение данных уязвимостей направлено вступившее в силу положение Банка России от 30.01.2025 № 851-П, которое требует от банков обеспечения целостности электронных сообщений с помощью усиленной электронной подписи или сертифицированных средств криптографической защиты информации (СКЗИ) и фактически запрещает использование SMS-кодов для подписания документов [1]. В России также активно внедряется стандарт ISO 20022, который уже используется в Системе быстрых платежей и Системе передачи финансовых сообщений [5].

Для малых и средних банков внедрение таких решений сопряжено с серьезными финансовыми барьерами. Стоимость внедрения усиленной подписи с использованием аппаратных модулей безопасности может достигать значительных сумм, а выпуск одной

усиленной подписи через удостоверяющий центр может обходиться в несколько тысяч рублей на клиента. Для сравнения, крупные банки, такие как Сбербанк, ВТБ, Т-Банк, инвестируют в новые технологические решения средства, сопоставимые с миллиардами рублей, тогда как малые банки ограничены в ресурсах, поэтому в данных условиях самостоятельная разработка собственных СКЗИ невозможна.

Принципиально новым фактором также становится введение персональной ответственности руководителей. Принятый законопроект предусматривает дисквалификацию на срок до 10 лет за грубые нарушения в сфере ИБ с запретом занимать аналогичные должности в финансовых организациях [1]. Это переводит риски передачи данных из ряда технических проблем в зону прямой ответственности топ-менеджмента.

В данных условиях разработаны практические рекомендации для малых и средних банков, включающие:

1. Обзор двух крупнейших российских вендорских платформ, предоставляющих сертифицированные СКЗИ и оптимальные по соотношению цены и безопасности решения;
2. Поэтапную дорожную карту внедрения, в которой на первом этапе производится установка IMSI-контроля для защиты от SIM-своп, а на втором – миграция на полномасштабную криптографию с использованием усиленной подписи;
3. Участие в коллективных платформах, таких как Платформа коммерческих согласий, разработанная Банком России, что позволяет распределить затраты на инфраструктуру управления согласиями клиентов;
4. Адаптацию внутренних политик через инвентаризацию протоколов передачи данных, регулярный аудит криптографических модулей и обучение персонала.

Выводы

Предложенный комплекс мер позволяет малым и средним банкам снизить технологическое неравенство, обеспечить выполнение требований положения Банка России № 851-П и стандарта ISO 20022 без непосильных инвестиций. Разработанные рекомендации могут быть использованы при формировании дорожных карт внедрения. Дальнейшие исследования целесообразно направить на сравнительный анализ экономической эффективности различных моделей внедрения защищенных каналов передачи данных.

Литература

1. Положение Банка России №851-П от 30.01.2025 [Электронный ресурс] // Центральный Банк Российской Федерации. – 2025. – С.1 – 33.
2. Баранов А. IMSI-check для банков: защита от SIM-swap без дорогостоящей криптографии // РБК Компании. 08.12.2025. [Электронный ресурс]. Режим доступа: https://clck.ru/3SSezU (дата обращения: 21.02.2026).
3. Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro // Official Journal of the European Union. – 2012. – L 94/22.
4. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) // Official Journal of the European Union. – 2015. – L 337/35.
5. Цифровизация платежей и внедрение инноваций на платежном рынке // Центральный банк Российской Федерации. – 2024. – С.6 – 18.