Родионова Анастасия Ивановна
магистрант
Научный руководитель
Савдерова Алина Федоровна
канд. экон. наук, доцент
ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

РИСКИ ДЕПОЗИТНОЙ ПОЛИТИКИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И МЕТОДЫ ИХ МИНИМИЗАЦИИ

Аннотация: *в статье рассматривается, как меняются риски депозитной политики банка под влиянием цифровизации. Выделены три основных вида рисков, которые становятся особенно заметными при переходе на дистанционное обслуживание. Это киберриски (утечка данных клиентов), операционные риски (сбои в работе приложений и систем) и риски ликвидности (быстрый отток денег через онлайн-каналы). Отдельно рассмотрен вопрос о том, как повлияет на депозиты внедрение цифрового рубля. В заключение предложены конкретные способы снижения этих рисков.*

Ключевые слова: *депозитная политика, цифровая трансформация, киберриск, операционный риск, риск ликвидности, цифровой рубль, ДБО.*

Банки все больше уходят в цифру. Это удобно для клиентов и выгодно для самих банков – меньше расходов на офисы и сотрудников. Но вместе с удобствами появляются и новые проблемы. Раньше главными рисками по вкладам были скачки процентных ставок или курсов валют. Сейчас к ним добавились риски, связанные с технологиями и поведением людей в интернете [1; 5; 6].

Актуальность темы подтверждается данными Банка России: в 2025 году злоумышленникам удалось совершить 1,5 млн успешных мошеннических операций, а общий объем похищенных средств достиг 29,3 млрд рублей, что на 6,4% больше, чем годом раннее. При этом банки с помощью антифрод-систем

предотвратили 134,2 млн попыток хищений, спасая 13,9 трлн рублей клиентов. Один серьезный сбой в мобильном приложении или утечка данных может вызвать массовый отток вкладов. Причём произойти это может буквально за несколько часов. В доцифровую эпоху такого не было – люди физически не могли так быстро забрать деньги из банка.

Под киберрисками мы понимаем вероятность того, что банк потеряет деньги или репутацию из-за взлома систем ДБО, кражи паролей клиентов или целенаправленных атак на депозитную инфраструктуру [6].

Цифровой вклад полностью обслуживается через приложение или личный кабинет. Клиент открывает его, пополняет и закрывает, не приходя в офис. Это удобно, но создаёт много точек входа для злоумышленников. По данным Банка России, основные угрозы – это сетевые атаки, слабая защита систем и действия недобросовестных сотрудников [1]. При этом основным источником убытков от операционных рисков остаётся внешнее мошенничество (59%).

На практике самое слабое звено – сам клиент. Люди ставят простые пароли, ведутся на фишинговые письма, сообщают коды из СМС мошенникам и если злоумышленник получает доступ к вкладу и выводит деньги, банку приходится возмещать ущерб. Но ещё хуже репутационные потери. Клиенты, которые пострадали или просто испугались, быстро уходят в другие банки. А как мы знаем, перевести деньги сейчас можно за пару кликов в приложении. Показательно, что средняя сумма одного хищения снизилась до 18,7 тыс. рублей (с 23 тыс. в 2024 г.), однако доля возвращённых средств клиентам упала до минимальных 5,2% (в 2024 г. – 9,6%)

Операционный риск в цифровой среде – это вероятность того, что приложение или сайт банка перестанут работать, и клиенты не смогут проводить операции по вкладам.

Основными причинами таких сбоев являются проблемы у интернет-провайдеров, ошибки при подключении к внешним сервисам (таким как Госуслуги, маркетплейсы), система не справляется с наплывом клиентов. Только в 1 квартале

2025 года количество жалоб на работу банков выросло на 36,8% по сравнению с аналогичным периодом прошлого года, достигнув 58,8 тыс.

Большая опасность тут в том, что сбой быстро перерастает в панику. Когда клиент не может зайти в приложение у него возникают мысли: «А всё ли в порядке с банком? Не закроют ли его?». В соцсетях и чатах такие страхи разносятся мгновенно. Люди бегут закрывать вклады, и у банка начинаются проблемы с ликвидностью. То есть чисто техническая проблема превращается в финансовую и репутационную. Яркий пример – массовый сбой в декабре 2025 года, когда количество жалоб на один из крупных банков (ВТБ) превысило 10 тысяч за сутки.

Если раньше риск ликвидности по вкладам означал, что клиенты могут досрочно забрать деньги, то в цифровую эпоху скорость этого процесса выросла в разы. Назовём его «цифровой текучестью», когда деньги очень легко и быстро перетекают из одного банка в другой.

Раньше, чтобы закрыть вклад, надо было идти в отделение с паспортом, стоять в очереди, писать заявление. Это останавливало от импульсивных решений. Сейчас всё иначе. Увидел ставку выше в другом банке – открыл приложение, нажал три кнопки, и деньги ушли. Это делает вкладчиков подвижными. Если у банка возникают даже временные трудности, отток может быть стремительным. По итогам 2025 года отток ликвидности из банков в наличную форму составил 1 трлн рублей, что в 5 раз больше, чем в 2024 году. При этом общий объем средств физических лиц в банках продолжает расти: за 2025 год он увеличился на 9,2 трлн рублей и на начало 2026 года достиг 75,8 трлн рублей.

Ещё один новый вызов – цифровой рубль [4]. По оценкам экспертов, после его запуска из банков может уйти от 5 до 20% вкладов. Для небольших банков удар будет сильнее т.к. цифровой рубль это обязательство Центрального банка, он надёжнее любого коммерческого банка. Да, по нему не платят проценты. Но для людей с крупными суммами безопасность может оказаться важнее доходности. К середине 2025 года уже открыто около 2,5 тыс. цифровых кошельков, проведено более 100 тыс. операций (включая 63 тыс. переводов). С 1 сентября

2026 года операции с цифровым рублём станут обязательными для крупнейших банков.

Получается, банкам придётся конкурировать за деньги клиентов не только между собой, но и с государством. А это уже совсем другой уровень задачи.

Проанализировав ситуацию, можем предложить несколько мер по каждому виду рисков.

Чтобы защититься от киберрисков, нужно ввести двухфакторную аутентификацию для операций с вкладами на крупные суммы. Например, пароль плюс подтверждение по биометрии. Также можно использовать антифрод-системы, которые отслеживают подозрительное поведение клиента. Когда операция нехарактерна для человека (другое время, другая геолокация), её лучше заблокировать до выяснения. И конечно, каждому клиенту раздать или отправить на почту памятки о том, как не попасться на уловки мошенников, реально работают.

При анализе операционных рисков, надежность IT-системы занимает центральное место в обеспечении стабильности банка. Резервные серверы должны находиться в разных географических точках, чтобы сбой в одном регионе не оставил без доступа к деньгам всю страну. Кроме этого у банка должен быть чёткий план действий на случай серьёзного сбоя, чтобы сотрудники знали куда звонить и что делать в первые минуты аварии. Также банку рекомендуется проводить стресс-тестирование. Они показывают способна ли система выдержать искусственную нагрузку и работать в экстремальных условиях.

Перейдём к риску ликвидности. Можно внедрить систему, которая на основе прошлых операций видит, что клиент закроет вклад досрочно и банк может заранее сделать ему персональное предложение и удержать. Вместе с тем банкам уже нужно думать о продуктах, которые смогут конкурировать с цифровым рублем. Например, предлагать клиентам повышенную страховую защиту или же включить вклад в экосистемные подписки с дополнительными бонусами. Главное здесь, чтобы клиенту было выгодно и спокойно держать деньги в банке.

Таким образом, мы пришли к нескольким выводам.

Во-первых, цифровизация депозитов меняет не только сервис, но и сами риски. Киберриски, операционные сбои и угрозы ликвидности теперь тесно связаны между собой [2, 3]. Проблема в одной сфере почти мгновенно перекидывается на другие. Управлять ими по отдельности, как раньше, уже не получается.

Во-вторых, цифровой рубль – это серьёзный вызов. Банкам не стоит недооценивать возможный отток вкладов.

В-третьих, из всех способов снижения рисков можно выделить три главных направления. Первое, создать в банке команду, которая будет отвечать за риски цифровых пассивов, чтобы службы безопасности и IT не работали вразнобой. Второе, банкам нужно вложиться в аналитику, которая предсказывает поведение клиентов. Это помогает удерживать людей до того, как они решат уйти. И третье, придумать новые депозитные продукты с учётом появления цифрового рубля. Клиенту должно быть выгодно и надёжно держать деньги именно в банке

Подводя итог хочется сказать, что цифровизация – это правильный путь. Но идти по нему надо с открытыми глазами, понимая все риски и заранее продумывая способы защиты.

Список литературы

1. Письмо Банка России от 07.12.2007 №197-Т «О рисках при дистанционном банковском обслуживании». – URL: https://www.consultant.ru/document/cons_doc_LAW_73368/?ysclid=mnx3jkn9h8121629197 (дата обращения: 14.04.2026).

2. Савдерова А.Ф. Тенденции и перспективы развития интернет-банкинга в России / А.Ф. Савдерова, Д.В. Журова // Вестник Чувашского университета. – 2013. – №4. – С. 395–399. – EDN RSXTGL.

3. Тихомирова Е.В. Киберустойчивость банковской системы: новые вызовы // Банковское дело. – 2025. – №2. – С. 18–24.

4. Цифровой рубль: текущий статус проекта. – URL: https://cbr.ru/Content/Document/File/177415/digital_ruble_30062025.pdf (дата обращения: 14.04.2026).

5. Шушаков А.И. Искусственный интеллект в анализе рисков кредитования коммерческими банками / А.И. Шушаков, А.Ф. Савдерова // Моделирование и прогнозирование развития отраслей социально-экономической сферы: сборник научных трудов по материалам международной научно-практической конференции (Курск, 28 мая 2024 года). – Курск: Курский государственный медицинский университет, 2024. – С. 264–266. – EDN FUDRCG.

6. Шушаков А.И. Сохранность конфиденциальности данных в банковской сфере при использовании искусственного интеллекта / А.И. Шушаков, А.Ф. Савдерова // Финансово-кредитный механизм регулирования социально-экономического развития в условиях демографической и структурной трансформации: сборник материалов Всероссийской научно-практической конференции. – Чебоксары: Среда, 2024. – С. 203–205. – EDN BGGHYB.

7. Противодействие кибермошенничеству: статистика хищений и обзор атак на финансовые организации // Центральный банк Российской Федерации. – URL: http://www.cbr.ru/press/event/?id=28300 (дата обращения: 14.04.2026).

8. Обзор финансовой стабильности. II–III кварталы 2025 года // Центральный банк Российской Федерации. – URL: https://www.cbr.ru/analytics/finstab/ofs/2q_3q_2025/ (дата обращения: 14.04.2026).

9. Results of monitoring of credit institutions' maximum interest rates // Bank of Russia. – URL: http://www.cbr.ru/eng/press/pr/?file=639023404594663482eng_bank_sector.htm (date of request: 14.04.2026).