УДК 336.717

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

С.П. Спиридонов, В.И. Меньщикова, А.В. Нечвеева
ФГБОУ ВО «Тамбовский государственный технический университет», Тамбов, email: spiridonov_sp@bk.ru, menshikova2907@mail.ru, nechweewa.a.22@gmail.com

Аннотация. *Статья посвящена исследованию развития системы дистанционного банковского обслуживания (ДБО) в Российской Федерации и анализу ключевых проблем ее безопасности. Актуальность темы обусловлена стремительной цифровизацией финансовых услуг и ростом связанных с ней киберрисков. На основе анализа статистических данных выявлена положительная динамика распространения ДБО, получившая дополнительный импульс в период пандемии COVID-19. Вместе с тем, автором констатируется, что расширение функциональности и доступности ДБО сопровождается увеличением объема и изощренности мошеннических операций. В работе проводится сравнительный анализ уязвимостей систем ДБО, разработанных собственными силами кредитных организаций и силами внешних вендоров. Установлено, что решения сторонних разработчиков демонстрируют более высокий уровень уязвимостей на уровне кода приложения, в то время как системы собственной разработки банков зачастую проигрывают в функциональности и удобстве интерфейса. В заключение сформулированы ключевые направления совершенствования ДБО: ужесточение требований к парольной политике и многофакторной аутентификации, развитие систем проактивного мониторинга транзакций, совершенствование нормативно-правовой базы и реализация программ повышения финансовой грамотности населения. Доказано, что только комплексный подход позволит обеспечить устойчивое и безопасное развитие дистанционного банковского обслуживания.*

Ключевые слова: *дистанционное банковское обслуживание, развитие, интернет-банкинг, мобильный банкинг, операции, финансы.*

PROBLEMS AND PROSPECTS OF REMOTE BANKING SYSTEM DEVELOPMENT

S.P. Spiridonov, V.I. Menshchikova, A.V. Nechveeva
Tambov State Technical University, Tambov, email: spiridonov_sp@bk.ru, menshikova2907@mail.ru, nechweewa.a.22@gmail.com

Abstract. *The article is devoted to the study of the development of the remote banking system in the Russian Federation and the analysis of key problems of its security. The relevance of the topic is due to the rapid digitalization of financial services and the growth of cyber risks associated with it. Based on the analysis of statistical data, a positive trend in the spread of TB has been revealed, which received an additional boost during the COVID-19 pandemic. At the same time, the author states that the expansion of the functionality and accessibility of RBS is accompanied by an increase in the volume and sophistication of fraudulent transactions. The paper provides a comparative analysis of the vulnerabilities of RBO systems developed by in-house credit institutions and external vendors. It has been found that third-party solutions demonstrate a higher level of vulnerabilities at the application code level, while banks' own-developed systems often lose out in functionality and user-friendliness. In conclusion, the key areas of improvement of the RBO are formulated: stricter requirements for password policy and multifactor authentication, the development of proactive transaction monitoring systems, the improvement of the regulatory framework and the implementation of programs to improve financial literacy of the population. It has been proven that only an integrated approach will ensure the sustainable and secure development of remote banking services.*

Keywords: *remote banking, development, internet banking, mobile banking, operations, finance.*

Дата поступления статьи в редакцию: 30.11.2025
Дата принятия статьи в печать: 26.12.2025

Введение

Каков самый ценный ресурс есть у человека? Конечно же, время. В век стремительного развития цифровых технологий экономить этот ресурс стало проще, большинство вопросов можно решить, не выходя из дома, в том числе и финансовые. На данный момент уже нет необходимости посещать банк, чтобы получить карту или открыть вклад, перевести средства или купить валюту, заняться инвестициями или оформить кредитный договор. Все это и многое другое теперь может быть осуществлено

посредством системы дистанционного обслуживания (далее ДБО). Система ДБО впервые была применена в России еще в 1998 году банком ПАО «Уралсиб», а по прошествии практически трех десятилетий ДБО значительным образом укоренилась в жизнедеятельности населения и даже в какой-то мере стала её неотъемлемой частью. Система дистанционного банкинга позволяет клиентам осуществлять различного рода банковские операции без визита в отделение банка посредством определенных каналов телекоммуникации, именно такое определение дает ДБО законодательство РФ.

Нельзя также не упомянуть о выгоде, которую извлекают банки, используя данную систему обслуживания. Во-первых, это сокращение затрат на содержание офисов, при условии того, что уже есть значительное количество банков, отказавшихся от очного обслуживания населения и полностью перешедших в онлайн-формат. Во-вторых, эта система позволяет обрабатывать колоссальный объем информации, что повышает эффективность деятельности организации.

Цель исследования

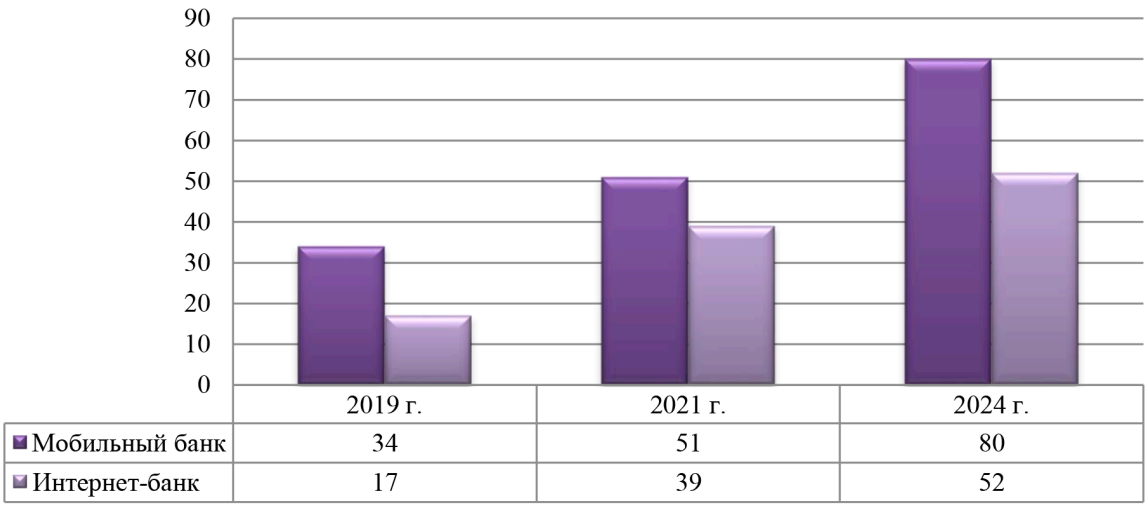
Цель исследования – провести комплексный анализ современного состояния системы дистанционного банковского обслуживания (ДБО) в России, выявить и систематизировать ключевые проблемы в области кибербезопасности, а также разработать научно-обоснованные направления по совершенствованию ее безопасности и эффективности

Материал и методы исследования

Для достижения поставленной цели в исследовании применялся комплекс общенаучных и специальных методов. для комплексного изучения системы ДБО как целостного явления, выявления ее структуры (каналы: интернет-банкинг, мобильный банкинг и т.д.) и взаимосвязей с внешней средой (влияние пандемии, уровень финансовой грамотности) был использован системный анализ; для сопоставления уровня безопасности и функциональности систем ДБО, разработанных собственными силами банков и сторонними вендорами, а также для выявления преимуществ и недостатков различных каналов ДБО – сравнительный анализ. Для наглядного представления результатов анализа в виде таблиц (например, карта рисков, проблемы и пути решения) и синтеза выводов на основе графического материала был применен метод визуализации данных. Данный набор методов позволяет обеспечить достоверность и полноту исследования, сочетая теоретическое осмысление проблемы с практическим анализом конкретных данных и статистических тенденций.

Результаты исследования

Согласно общепринятой классификации методик обслуживания система ДБО включает в себя следующие элементы: мобильный банкинг (СМС-уведомления), интернет-банкинг (приложение или сайт банка), ПК-банкинг, телефонный (колл-центр) и терминальный (банкоматы). Все перечисленное для наибольшей эффективности применяется системно, поскольку каждый элемент закрывает лишь часть потребностей клиента, но все же можно выделить наиболее значимые звенья в этой цепи, а именно, мобильный и интернет-банкинг. Для наибольшей наглядности необходимо изучить динамику величины пользователей цифровых сервисов банков (рис. 1).



	2019 г.	2021 г.	2024 г.
Мобильный банк	34	51	80
Интернет-банк	17	39	52

Рис. 1. *Доля пользователей мобильного и интернет-банкинга в России, %*

Исходя из приведенных данных, можно сделать сразу несколько выводов. Во-первых, за анализируемый период произошел резкий скачок как среди пользователей мобильного (на 135,3%), так и интернет-банка (на 205,9%). Данная тенденция может быть связана с влиянием, оказанным пандемией COVID-19, которая привела к временной самоизоляции многих граждан и сделала необходимым использование удаленных каналов доступа для решения вопросов в различных сферах жизнедеятельности, в том числе оказался и сектор финансовых услуг. Во-вторых, значительную роль в столь резком изменении исследуемых показателей сыграл рост финансовой грамотности населения [5].

Рассмотрим более детально структуру операций, осуществляемых пользователями системы ДБО (рис. 2).

Рис. 2. *Структура операций, совершаемых посредством интернет-банка, %*

Совершенствование каналов дистанционного банковского доступа позволяет совершать целый ряд банковских операций. Наиболее популярные операции, совершаемые клиентами посредством ДБО: формирование выписки по счету/карте, запрос баланса, оплата мобильной связи и ЖКУ, а также всевозможные переводы средств как внутри одного банка, так и в сторонние банки, что стало легче осуществить благодаря системе СБП [4].

Таблица 1

Карта рисков по видам ДБО

Вид ДБО	Оборудование	Риски по убыванию вероятности осуществления
Интернет-банкинг	Любой гаджет с интернет-подключением	риски, связанные с плохим доступом в сеть риски ненадежности транзакционного процесса риски, связанные с эксплуатирующим данный гаджет (невнимательность, незнание принципов работы гаджета) плохая защита у используемого гаджета электронное мошенничество
Телефонный банкинг	Стационарный телефон	телефонное мошенничество
Мобильный банкинг	Любой гаджет с мобильной сетью	телефонное мошенничество; риски, связанные с утратой гаджета; риски, связанные с эксплуатирующим данное устройство (разглашение конфиденциальной информации, плохой уровень владения устройством)
ПК-банкинг	ПК с установленным программным обеспечением	риски ненадежности ПК (в связи с пренебрежением антивирусами и т.п.); риск устаревания ПО (отсутствие важных обновлений и т.п.)
Терминальный банкинг	Банкомат, терминал и т.п.	риски, связанные с эксплуатирующим банкомат или терминал (возможность визуального доступа к конфиденциальной информации; совершение ошибок при вводе данных; риски, связанные с утратой карты

При этом можно не посещать офисы самого банка, но вместе с превосходством создается и огромный список проблем, которые так или иначе связаны с обеспечением безопасности совершаемых операций через интернет-банкинг и мобильный банкинг (табл. 1).

Наряду с цифровизацией всех сфер общественной жизни и экономики в частности развивается и преступная деятельность, нацеленная на получение конфиденциальных данных граждан с последующим хищением средств со счетов как частных лиц, так и крупных организаций (рис. 3).

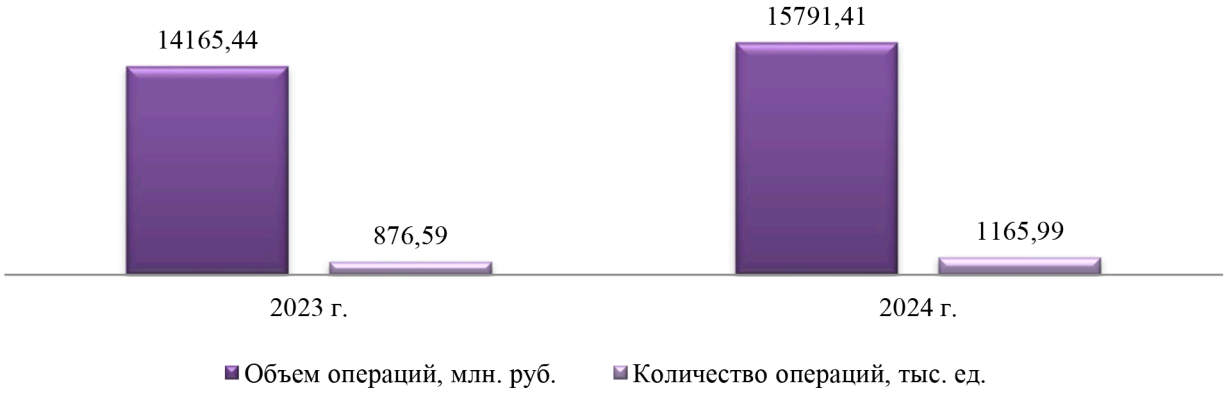


Рис. 3. *Динамика общего объема и количества операций без согласия клиентов*

В 2024 году со счетов физических лиц посредством каналов ДБО в результате мошеннических действий было произведено 1 165 операций по списанию средств на общую сумму 15 791 млн. руб., что на 11,5% больше, чем годом ранее [7].

Как показывает статистика, более надежными можно назвать системы дистанционного банкинга, разработанные собственными силами финансово-кредитных организаций. Именно так и поступают большинство банков, но одна треть все же пользуется услугами вендоров (разработчики ИТ-продуктов) (рис. 4).

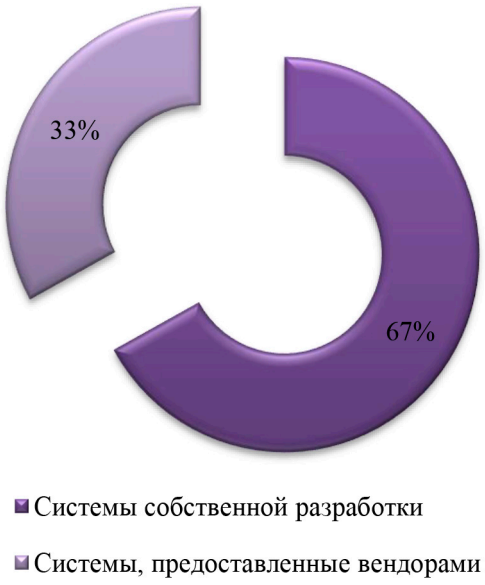


Рис. 4. *Типы исследованных систем*

При проведении анализа безопасности систем ДБО, разработанных подрядными организациями, было значительно большее количество нарушений, чем в том же продукте собственной разработки банка (рис. 5).

Исходя из анализируемых показателей, можно отметить, что системы ДБО, разработанные собственными силами финансово-кредитных организаций, проигрывают по большей части в функциональном плане, что, разумеется, тоже имеет вес при расчете потенциального дохода, ведь именно удобство пользователей и дружественный интерфейс приложения оказывает значительное влияние на привлечение новых клиентов и удержание действующих. Но, как правило, системы, разработанные подрядчиком, не гарантируют столь высокой степени безопасности, как системы собственной разработки банков.

К примеру, уязвимость на уровне кода приложения практически в 4 раза выше при разработке системы вендорами. Данный факт свидетельствует о том, что в вопросах качества исследуемой системы банкам не стоит полностью полагаться на организацию-разработчика [3].

При этом уровень риска при идентификации пользователей практически одинаково велик в обоих случаях разработки системы ДБО (рис. 6).

Рис. 5. *Уязвимости механизмов защиты систем ДБО, %*

Рис. 6. *Риски механизмов идентификации пользователей, %*

Наибольший риск при идентификации пользователя в более чем 40% исследуемых систем ДБО связан с недостаточно строгой парольной политикой. К сожалению, большинство банков устраивает четырехзначный код доступа, схожий с датой рождения клиента, к примеру, что в современных реалиях просто неприемлемо.

Недостатки системы защиты кроются и в автоподборе учетных данных клиента, большее проседание в данном направлении имеют как раз системы собственной разработки банков (33%).

Главная проблема в том, что мошенники пока еще идут на шаг впереди законодательства и службы безопасности любого банка, каждый день становится известно о все более новых и изощренных схемах, позволяющих недобросовестным образом завладеть средствами граждан [1].

Разумеется, безопасность не единственное направление, в котором необходимо совершенствовать систему ДБО, можно выделить также следующие параметры, которые оказывают значительное влияние на работу данной системы:

– производительность;
– информативность системы;
– простота использования;
– дружественность интерфейса;
– системный функционал.

Все эти критерии важно развивать комплексно, поскольку популярность банковской системы зависит от удобства пользования ею населением, а за это уже отвечает эффективная бесперебойная работа дистанционного банкинга, простота интерфейса и информативность, разумеется.

Представим рассмотренные выше проблемы функционирования системы ДБО в виде таблицы (табл. 2).

Таблица 2

Проблемы дистанционного банковского обслуживания в РФ и пути их решения

Проблема	Решение
Слабое развитие интернет-банкинга в розничном банковском секторе	Повышение квалификации работника, выполняющего эту задачу. Банкам необходимо постоянно осуществлять обучение сотрудников с целью повышения их квалификации
Проблема формирования штата	Предлагается решать посредством проведения профессиональной переподготовки
Финансовая неграмотность населения	Проведение образовательных программ, семинаров, тренингов и конференций по финансовой грамотности, создание специальных онлайн-ресурсов и порталов с полезной информацией о финансах
Безопасность систем интернет-банкинга	Основными технологиями обеспечения безопасности в современных платежных системах являются: – шифрование данных; – использование виртуальной клавиатуры в системах интернет-банкинга; – использование электронной цифровой подписи, удостоверяющей личность владельца счета; – использование системы временных паролей для подтверждения финансовых операций
Нестабильность правовой системы	Банкам необходимо не только своевременное реагировать на принимаемые Банком России положения, а также активно способствовать ему в их разработке, для обеспечения успешного развития и повышения эффективности деятельности систем ДБО

В связи с этим необходимо выделить ряд направлений совершенствования ДБО:
– повышение степени безопасности производимых операций;
– повышение финансовой грамотности населения;
– разработка законодательной базы регулирования ДБО.

В целях повышения безопасности банковских операций необходимо совершенствовать систему мониторинга операций, проводимых посредством ДБО. На данный момент огромная проблема заключается в том, что у большинства банков подозрение вызывает операция на ее финальном этапе, а именно, в момент совершения непосредственно транзакции, когда следовало бы проводить более тщательный мониторинг на предшествующих этапах (анализ истории операций, смена номера телефона, вход в мобильный банк с нового устройства и т.д.) [6].

Для повышения финансовой грамотности граждан необходимо первостепенно уделить должное внимание программам общего и среднего профессионального образования. В настоящее время дети в возрасте от 6 лет имеют возможность использовать банковские карты и ограниченный функционал мобильного банкинга, что вызывает острую необходимость образовательной системы шагать в ногу со временем и давать школьникам и, впоследствии, студентам колледжей и ВУЗов базовые знания в области финансовой грамотности. На государственном уровне необходимо обеспечить взаимодействие с предприятиями и финансово-кредитными организациями в целях проведения информационно-просветительской деятельности в проблемной области (социальная реклама в интернете, соцсетях и мессенджерах, а также других каналах информирования).

На данный момент государством не предусмотрено четкое регулирование безопасности банковского обслуживания в системе ДБО, финансово-кредитные организации могут руководствоваться только расплывчатыми рекомендациями от 31.03.2008 г. №36-Т. Законодательно необходимо обязать банки при обслуживании клиентов посредством ДБО:
– проводить обязательную двухфакторную аутентификацию пользователей,
– разрабатывать и внедрять процедуры мониторинга банковских операций, осуществляемых с применением систем интернет-банкинга;
– применять дополнительные способы подтверждения операций, связанных с переводами средств, открытием и закрытием вкладов, сменой клиентских данных, а также кредитованием граждан.

Выводы

В заключение следует отметить, что система ДБО в последние годы активным образом набирает популярность, поскольку нельзя не отметить удобство данного вида банковского обслуживания, но вместе с тем возникает и ряд проблем, касаемо безопасности проводимых в данном канале обслуживания финансовых операций. Но в случае обращения должного внимания на данную проблему со стороны государства и служб безопасности банковских учреждений в скором будущем удастся добиться внушительных результатов в данной отрасли финансовых услуг.

Литература

1. Конявский В.А. Обеспечение безопасности и распределение ответственности при организации удаленного доступа // Информационная безопасность. 2021. № 2. С. 33-35.

2. Мануйленко В.В., Вититникова Я.Ю., Конарева Ю.И. Влияние банковских инноваций на развитие теневых экономических отношений в регионе: монография / под науч. ред. В. В. Мануйленко. М.: Финансы и статистика, 2022. 283 с. ISBN: 978-5-00184-065-7 EDN: RDXAWR.

3. Полякова В.В., Почекутов М.П., Ревзон О.А., Сумбатян С.Л. Современное дистанционное банковское обслуживание в России: особенности и тенденции // Вестник Алтайской академии экономики и права. 2024. № 12-2. С. 298-303. DOI: 10.17513/vaael.3920 EDN: JITOQC.

4. Платонова Ю.Ю., Жерлицина А.И. Основные направления дистанционного банковского обслуживания» // Экономика и бизнес: теория и практика. 2022. № 11-2. С. 99-102. DOI: 10.24412/2411-0450-2022-11-2-99-102 EDN: CEZESG.

5. Ребрина Т.Г., Зверев А.В., Мишина М.Ю. Тенденции развития мобильного банкинга в России и за рубежом // Вестник Алтайской академии экономики и права. 2022. № 9-3. С. 416-420. DOI: 10.17513/vaael.2490 EDN: IQVPBU.

6. Тимин А.Н., Умарходжаева Д.Х. Перспективы банковского обслуживания граждан в России и возможности совершенствования современных банковских продуктов и услуг // Вектор экономики. 2023. № 10. EDN: IZQNWG.

7. Шелковникова К.А. Актуальные проблемы развития дистанционного банковского обслуживания в России // Молодой ученый. 2023. № 36 (483). С. 122-125. EDN: HNMCMI.