

УДК 336

ВЗАИМОЗАВИСИМОСТЬ ЭКОНОМИЧЕСКОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ИНТЕРНЕТ-БАНКИНГА

Н.А. Митрофанов

Российский университет кооперации, Мытищи, email: virtuscup@mail.ru

Аннотация. В данной статье исследуется взаимозависимость экономической и информационной безопасности в условиях развития интернет-банкинга. В ходе работы проводится анализ существенных характеристик экономической и информационной безопасности, а также рассматриваются риски, образующиеся вследствие развития и интеграции интернет-банкинга в различные сферы хозяйственной деятельности. Особое внимание уделяется рассмотрению практических кейсов из судебной практики, иллюстрирующих причинно-следственную связь между рассматриваемыми видами безопасности и последующими из-за нарушения данной связи событиями. В результате исследования формируются выводы о значимости соблюдения соразмерного уровня экономической и информационной безопасности в условиях развития интернет-банкинга, а также предлагается ряд практических рекомендаций по предотвращению выявленных в ходе настоящего исследования рисков и угроз. Полученные результаты могут являться полезным вкладом в будущие исследования в области экономической безопасности.

Ключевые слова: экономическая безопасность, информационная безопасность, интернет-банкинг, дистанционное банковское обслуживание, цифровизация.

THE INTERDEPENDENCE OF ECONOMIC AND INFORMATION SECURITY IN THE CONTEXT OF INTERNET BANKING DEVELOPMENT

N.A. Mitrofanov

Russian University of Cooperation, Mytishchi, email: virtuscup@mail.ru

Abstract. This article explores the interdependence of economic and information security in the context of the development of Internet banking. In the course of the work, the analysis of the essential characteristics of economic and information security is carried out, as well as the risks arising from the development and integration of Internet banking into various spheres of economic activity are considered. Particular attention is paid to the consideration of practical cases from judicial practice, illustrating the cause-and-effect relationship between the types of security under consideration and the events that follow due to the violation of this connection. As a result of the study, conclusions are drawn about the importance of observing a proportionate level of economic and information security in the context of the development of Internet banking, and a number of practical recommendations are offered to prevent the risks and threats identified in the course of this study. The results obtained can be a useful contribution to future research in the field of economic security.

Keywords: economic security, information security, internet banking, remote banking, digitalization.

Дата поступления статьи в редакцию: 05.03.2026

Дата принятия статьи в печать: 15.04.2026

Введение

В условиях глобальной цифровизации традиционные модели обеспечения безопасности организаций и общества с каждым годом становятся все менее эффективными. Повсеместно интегрируемые в различные области ноу-хау порождают новые вызовы и угрозы, наличие которых, в свою очередь, повышает количество требований к системам безопасности и заставляет их находиться в процессе постоянной модернизации.

Интернет-банкинг как раз является одной из форм подобных инноваций традиционно ассоциирующейся с банковской деятельностью, однако при этом также оказывающей значительное влияние и на организации иных отраслей. Переход в цифровое пространство, оказал значительное влияние на области экономической и информационной безопасности, выявив проблему, что большинство субъектов хозяйствования при использовании систем дистанцион-

ного банковского обслуживания не осознают уровень угроз от использования данной технологии, из-за чего несут значительные финансовые и репутационные потери при их наступлении.

Актуальность настоящего исследования обусловлена тем, что согласно статистическим данным публикуемых Банком России, по итогам 2025 года граждане и компании совершили 18,3 млрд операций при помощи системы быстрых платежей (далее по тексту СБП) на сумму в 103 трлн рублей, что превышает аналогичные показатели предшествующего года в 1,4 и 1,5 раза соответственно [6]. При этом согласно статистическим данным того же Банка России, в 2025 году количество операций без добровольного согласия клиентов, совершенных при помощи СБП, увеличилось по сравнению с предшествующим годом на 31,2% [7].

Цель исследования

Целью настоящего исследования является проведение комплексной и всесторонней оценки взаимозависимости экономической и информационной безопасности в условиях развития интернет-банкинга. Исследование проведено с акцентом на анализ практических кейсов из судебной и несудебной практики, иллюстрирующих данную взаимозависимость.

Для достижения поставленной в исследовании цели сформированы следующие задачи:

Определить взаимозависимость экономической и информационной безопасности в условиях развития интернет-банкинга;

Провести анализ практических кейсов из судебной и несудебной практики, иллюстрирующих причинно-следственную связь между рассматриваемыми видами безопасности и последующими из-за нарушения данной связи событиями;

Сформировать практические рекомендации по повышению уровня экономической и информационной безопасности.

Материал и методы исследования

Исследовательскую базу настоящего исследования составляют нормативно-правовые акты, действующие на территории Российской Федерации на момент проведения исследования, практические кейсы из судебной и несудебной практики, научные работы, опубликованные в рецензируемых журналах и сборниках.

Исследование проведено с применением логико-структурного метода научного познания и методов качественного анализа. Описание исследования по поставленным задачам имеет структуру, соответствующую алгоритму (методике) исследования.

Результаты исследования

В соответствии с пп. 3, п. 6, р. 1 «Стратегии национальной безопасности Российской Федерации», установлено, что данная Стратегия основана на неразрывной взаимозависимости между национальной безопасностью Российской Федерации и ее социально-экономическим развитием [1]. Также установлено, что сущностная характеристика понятия «национальная безопасность» включает в себя множество включенных в нее элементов, в том числе экономическую и информационную безопасность, которые в рамках данной системы рассматриваются как понятия единого уровня.

Согласно «Стратегии экономической безопасности Российской Федерации на период до 2030 года (далее по тексту: Стратегия)», под экономической безопасностью понимается: «...Состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации...» [2].

Под угрозой экономической безопасности, в соответствии с данной Стратегией, понимается: «...Совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере...» [2].

Понятие информационной безопасности, в свою очередь, раскрывается в «Доктрине информационной безопасности Российской Федерации», где под данным понятием понимается: «...Состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства...» [3].

Таким образом, в масштабе национальной безопасности важно учитывать взаимосвязь и взаимозависимость всех составляющих данной системы с целью предотвращения всех видов угроз, которые в свою очередь имеют широкую классификацию, наличие и необходимость которой, обусловлено различной природой рассматриваемых угроз и как следствие необходимостью в наличии различных механизмов по их предотвращению. Также данный подход реализуем и в более малом масштабе, например в масштабе отрасли или предприятия.

Интернет-банкинг является достаточно интересным видом инновации, которая несмотря на тесную связь с банковской отраслью, способна оказывать значительное влияние и на организации иных отраслей.

Согласно п. 1.1 Письма Банка России от 31.03.2008 № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» под интернет-банкингом понимается: «...способ дистанционного банковского обслуживания клиентов, осуществляемого кредитными организациями в сети Интернет и включающего информационное и операционное взаимодействие с ними...» [4], где под дистанционным банковским обслуживанием клиентов, согласно Письму Банка России от 26.10.2010 № 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания», понимается: «...совокупность установленных в кредитной организации аппаратно-программных средств, с помощью которых осуществляется дистанционное банковское обслуживание...» [5].

Интернет-банкинг в ходе своего становления сталкивался с большим количеством проблем, среди которых одной из наиболее значимых, по мнению автора, является необходимость одно-временной защиты интересов как банков, предоставляющих свои услуги, так и интересов конечных пользователей данной технологии в лице физических или юридических лиц. С увеличением доли технологий в банковском секторе вектор развития банковских систем безопасности постепенно смещался в сторону защиты информации и как следствие доля интегрированных в них решений из сферы информационной безопасности постоянно увеличивалась. Подобный подход в дальнейшем положил начало функционирования сферы финансовых технологий или сокращённо сферы «Финтех», которая на сегодняшний момент также активно развивается.

Смена парадигмы банковской безопасности и повышение значимости информационной безопасности также обусловлена наличием причинно-следственной связи между информацией и возможностями, открываемыми при владении ею. Как говорил Ротшильд М.А.: «...Кто владеет информацией, тот владеет миром...». Однако большое количество субъектов хозяйствования, руководствуясь данной мыслью, допускает ряд ошибок, которые в дальнейшем оказывают критическое влияние на результаты их хозяйственной деятельности.

Например, согласно официальной статистике публикуемой Банком России, за период с 2023 по 2025 год, количество операции по переводу денежных средств осуществлённых без согласия клиентов при помощи ДБО и СБП систематически увеличивается, что свидетельствует о необходимости проведения дальнейших работ по совершенствованию банковских систем безопасности. Статистические данные сгруппированы и представлены в Таблице 1.

Таблица 1

Количество операции по переводу денежных средств, осуществлённых с помощью ДБО и СБП, без согласия банковских клиентов за период с 2023 по 2025 год

Тип клиента	2023 год		2024 год		2025 год	
	Объем операций, млн. руб.	Количество операций, тыс. ед.	Объем операций, млн. руб.	Количество операций, тыс. ед.	Объем операций, млн. руб.	Количество операций, тыс. ед.
Физические лица	15 258,02	533,39	26 866,90	1 196,02	28 253,26	1 568,15
Юридические лица	1 164,33	1,66	667,40	1,43	1 054,37	2,82

Источник: составлено автором по статистическим данным публикуемым Банком России [7]



Также к концу 2025 года количество жалоб на банковские организации достигло отметки в 235 тыс., что, по мнению Банка России, является следствием усиления мер по противодействию отмыванию денежных средств и финансированию терроризма [8]. При этом большое количество жалоб со стороны клиентов наносит значительный репутационный ущерб банковским организациям, что в дальнейшем отрицательно сказывается на их финансовых результатах и как следствие снижает их инвестиционную привлекательность. Более того, если рассматривать подобную ситуацию со стороны клиента, то отсутствие возможности осуществить банковскую транзакцию, может привести к неисполнению обязанностей сторон, закрепленных в каком-либо договоре, и как следствие привести к ситуации, в рамках которой, одна из сторон обязана выплатить иной стороне неустойку.

Для минимизации подобных ситуаций Банк России реализует множество программ и публикует множество предписаний, среди которых особо важно отметить Положение ЦБ РФ от 17.08.2023 № 821-П и Положение ЦБ РФ от 30.01.2025 № 851-П. Данные положения устанавливают требования к системам и операторам электронных платформ по защите информации при осуществлении банковской деятельности с применением различных видов автоматизированных систем дистанционного банковского обслуживания. При этом, как усматривается из содержания данных документов, объектами защиты современных банковских систем безопасности в большей степени выступает информация, доступ к которой в соответствии с положениями отраженными в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и положениями отраженными в Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне» может быть ограничен ее правообладателем. В письме от 31 марта 2008 г. № 36-Т Банк России подчеркивает что в перечень рисков, связанных с применением систем ДБО, в том числе включены: «...Операционный риск, правовой, стратегический риск, репутационный риск и риск ликвидности...» [4], т.е. данный документ акцентирует внимание на том, что риски от ДБО не концентрируются только в сфере информационной безопасности и как следствие последствия от некорректно реализованной системы ДБО и интернет банкинга могут проявиться по разному, что также подтверждается практическими кейсами.

В качестве одного из практических кейсов, иллюстрирующих подобные последствия, может послужить арбитражное дело № А65-4246/2016, в рамках которого рассматривалась ситуация по неправомерному переводу злоумышленниками денежных средств с счета организации-клиента, без ее на то согласия, на счета третьих лиц на сумму свыше 30 млн. рублей. Позиция банковской организации строилась на том, что все операции на счете клиента осуществлялись только после прохождения верификации клиента с помощью ключа, направленного в его адрес при подписании договора на предоставление банковских услуг с помощью систем дистанционного обслуживания. Указанным ключом, в соответствии с условиями заключенного договора, могли распоряжаться только лица, имеющие право действовать от лица организации-клиента, в ином случае Банк не нес какой-либо ответственности за осуществленные операции. Суд, однако, встал на сторону организации-клиента, с счетов которой злоумышленниками были переведены денежные средства на счета третьих лиц. Подобное решение суд принял после получения заключения эксперта, в котором было отражено, что система безопасности банка не соответствовала всем установленным требованиям, вследствие чего Банк допустил возможность осуществления неправомерного перевода денежных средств со счета организации, без ее на то согласия, на счета третьих лиц [9]. Таким образом, недостаточный уровень информационной безопасности Банка отрицательно сказался как на уровне экономической безопасности самого Банка, так и на уровне экономической безопасности организации-клиента.

Иным примером может послужить арбитражное дело № А32-29429/2024. В рамках данного дела рассматривалась ситуация, в которой организация выступающая посредником (далее организация-посредник) столкнулась с неправомерной блокировкой своих банковских счетов в ходе исполнения своих договорных обязанностей из-за чего она была вынуждена уплачивать фиксированные процент неустойки за каждый день просрочки. Суд также встал на сторону организации-посредника и обязал банк выплатить полную сумму с учетом суммы неустойки клиенту в качестве компенсации. Однако, Банк, не согласившись с позицией суда, продолжил судебные тяжбы и добился пересмотра решения. Данное дело пред-

ставляет особый интерес по причине того, что позицию Банка разделила верховная Судебная коллегия по экономическим спорам Верховного Суда Российской Федерации (далее Коллегия), указав на тот факт, что установленная причинно-следственная связь между наложенными ограничениями о дистанционном обслуживании в отношении организация-посредника и возникшими у последнего расходами является ошибочной, вследствие чего Коллегия пришла к выводу, что все юридически значимые обстоятельства по делу судами установлены, но к ним неправильно применены нормы права [10]. Если оценивать произошедшую ситуацию с точки зрения действующей в сфере экономической безопасности практики, то перед принятием договорных обязательств организации всегда следует анализировать все риски и подготавливать мероприятия по их своевременному предотвращению. Таким образом, при условии наличия исправно функционирующей службы экономической безопасности у организации-посредника, указанных в арбитражном деле № А32-29429/2024 событий удалось бы избежать.

Также, как и любой подобной технологии, интернет-банкингу свойственно наличие технических ошибок. Например, в рамках арбитражного дела № А40-46373/23, сотрудниками банковской организации при установке и обновлении конкретных значений курсов конвертации в компьютерной программе банка была допущена ошибка в результате которой отображаемые у клиентов банка курсы валюты, доступные для конвертации в рамках различных валютных пар, значительно отличались от рыночного курса, что создало предпосылки для необоснованного обогащения клиентов банка за счет банка в результате проведения массовых операций конвертации валюты, используя уязвимость в работе алгоритма промежуточной конвертации. Один из клиентов банка решил воспользоваться данной ошибкой и менее чем за 25 минут, совершил подряд 18 операций конвертации валюты. При этом клиент, для обеспечения доходности совершаемых операций последовательно переводил денежные средства из RUB в GBP, из GBP в EUR, из EUR - вновь в RUB, т.е. клиент многократно, используя уязвимость алгоритма промежуточной конвертации валюты, переводил денежные средства в различные виды валют и в конечном счете вновь привел валюту, в тот вид, в котором данные денежные средства находились у него до осуществления всех операций. Спустя небольшой промежуток времени этим же клиентом менее чем за три часа, было совершено подряд еще 123 операции конвертации валюты по аналогичному алгоритму [11]. Указанными действиями данный клиент неосновательно обогатился на сумму свыше 30 млн. руб. Данный пример отлично демонстрирует как рядовая техническая ошибка, наличие которой не выявила служба безопасности банка, может повлиять на финансовое состояние организации.

Как усматривается из вышерассмотренных кейсов, банковские организации и их клиенты в условиях развития интернет-банкинга могут столкнуться с множеством угроз, возникновение большинства которых связана с недостаточным уровнем информационной и экономической безопасности обеих сторон.

Для предотвращения подобных угроз, большинству организаций достаточно соблюдать базовые принципы реализации экономической и информационной безопасности, которых было бы достаточно для снижения уровня рисков до приемлемого уровня. К подобным решениям можно отнести использование различных форм стратегического планирования, OSINT и SWOT-анализа, по результатам которых организация подготавливает комплекс мероприятий, реализуемый в различных сценариях. Самый простой формой прогнозирования можно считать матрицу рисков, поскольку она достаточно легко строится и не требует наличия специальных знаний у ее конечных пользователей. Пример подобной матрицы представлен в Таблице 2.

Более крупным организациям, при организации своих систем безопасности, рекомендуется использовать материалы судебной практики для построения вероятностных моделей угроз, с которыми организация может столкнуться. Подобный подход позволяет прогнозировать риски и обеспечивать оптимальный уровень безопасности организации без излишних финансовых вложений.

Наиболее важно, по мнению автора, осознавать уровень угроз и последствий от их реализации. Крайне распространённой ошибкой со стороны руководящих органов организаций, является недофинансирование или наоборот перефинансирование проектов по первоначальному построению своих систем безопасности. На фоне этого, могут возникать ситуации, когда у типового малого бизнеса реализована система безопасности на уровне крупного бизнеса, хотя

при этом годовой оборот денежных средств находится на довольно низком уровне. Не стоит забывать, что чрезмерные траты также имеют влияние на финансовую стабильность и устойчивость бизнеса.

Таблица 2

**Матрица рисков, возникающих при использовании интернет-банкинга
и различных систем ДБО**

Риски от использования интернет-банкинга		Степень значимости			
		Низкий	Средний	Высокий	Значительный
Вероятность возникновения	≤ 85%	Долгое заключение договора на ДБО	Человеческий фактор	Операционные задержки	Высокая комиссия
	≤ 60%	Плановые работы банка	Блокировка важных транзакций	Высокая стоимость банковских услуг	Технические сбои
	≤ 35%	Потеря ЭЦП	Блокировка доступа к счетам	Кража денежных средств	Утечка данных
	≤ 10%	Отказ от заключения договора на ДБО	Саботаж деятельности	Временное прекращение функционирования банковских систем	Полное прекращение функционирования банковских систем

Источник: составлено автором

Заключение

Проведенное исследование позволило провести оценку взаимозависимости экономической и информационной безопасности в условиях развития интернет-банкинга. Результаты исследования демонстрируют, что в условиях развития интернет-банкинга экономическая и информационная безопасность являются созависимыми, вследствие чего недостаточный уровень развития одного вида безопасности отрицательно сказывается на ином виде безопасности и потенциально способен дестабилизировать всю систему. Проанализированные статистические данные, публикуемые Банком России и практические кейсы из судебной практики, свидетельствуют об актуальности проведения изысканий по данной тематике, а также свидетельствуют о необходимости дальнейшей проработки механизмов обеспечения безопасности, как банковских, так и небанковских организаций. Приведённые по итогам исследования рекомендации и полученные результаты могут являться полезным вкладом в будущие исследования в области экономической безопасности.

Литература

1. Указ Президента РФ от 02.07.2021 № 400 «О стратегии национальной безопасности Российской Федерации». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/cb0c5bc1eaf4bd94d8e78f233af494e8e9dcde2b/ (дата обращения: 14.03.2025).
2. Указ Президента РФ от 13.05.2017 № 208 «О стратегии экономической безопасности Российской Федерации на период до 2030 года». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 14.03.2025).
3. Указ президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс]. URL: <https://base.garant.ru/71556224/> (дата обращения: 14.03.2025).
4. Письмо Банка России от 31.03.2008 № 36-Т Банка России от 31.03.2008 № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_76122/60da956c4a691b755fc16b077928347b44122614/ (дата обращения: 14.03.2025).
5. Письмо Банка России от 26.10.2010 № 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского

обслуживания». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_106206/695f8d141294d0f58cf62d3141a10628f22b53e1/ (дата обращения: 14.03.2025).

6. СБП: Основные показатели. [Электронный ресурс]. URL: https://www.cbr.ru/analytics/nps/sbp/4_2025/ (дата обращения: 14.03.2025).

7. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций. [Электронный ресурс]. URL: https://www.cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения: 14.03.2025).

8. Количество жалоб на банки в России выросло на 14,7% в 2025 год // Ведомости. [Электронный ресурс]. URL: <https://www.vedomosti.ru/finance/news/2026/02/06/1174647-kolichestvo-zhalob> (дата обращения: 14.03.2025).

9. Арбитражное дело А65-4246/2016 // Картотека арбитражных дел. [Электронный ресурс]. URL: <https://kad.arbitr.ru/Card/b8feecb-fbbe-4206-bab4-b2749984f5cc> (дата обращения: 14.03.2025).

10. Арбитражное дело А32-29429/2024 // Картотека арбитражных дел. [Электронный ресурс]. URL: <https://kad.arbitr.ru/Card/b64203a8-f45c-4ac4-be00-fce601a78d8b> (дата обращения: 14.03.2025).

11. Арбитражное дело А40-46373/2023 // Картотека арбитражных дел. [Электронный ресурс]. URL: <https://kad.arbitr.ru/Kad/Card?number=%D0%9040-46373%2F2023> (дата обращения: 14.03.2025).