

ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ/PUBLIC LAW (STATE LAW) SCIENCES

DOI: https://doi.org/10.60797/IRJ.2026.168.72 EDN: FRELRV

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРУГРОЗЫ В БАНКОВСКОМ СЕКТОРЕ

Научная статья

Волкова Д.А.[1, *], Ревина С.Н.[2]
[2] ORCID : 0000-0001-9565-1356;
[1, 2] Самарский государственный экономический университет, Самара, Российская Федерация

* Корреспондирующий автор (diana.vo2016[at]yandex.ru)

Предложена: 21.03.2026; Принята: 30.04.2026; Опубликована: 17.06.2026

Аннотация

В статье исследуется институт ответственности за киберугрозы в банковском секторе Российской Федерации в условиях цифровой трансформации финансового рынка. На основе анализа эмпирических данных ФинЦЕРТ, научных трудов отечественных исследователей и нормативно-правовых актов Банка России рассматривается трансформация целевых установок злоумышленников, смещающих фокус с прямого хищения средств на деструктивные многостадийные операции. Особое внимание уделяется феномену латентного присутствия нарушителей в информационной инфраструктуре как ключевому параметру оценки защищенности организаций. В работе систематизированы требования ключевых положений Банка России, регламентирующих обеспечение информационной безопасности и операционной надежности. Проанализирована проблема атак на цепочки поставок и необходимость контроля за уровнем защищенности подрядных организаций. Обосновывается вывод о трехкомпонентной структуре института ответственности, включающей нормативный каркас регулятора, координирующую функцию ФинЦЕРТ и внутреннюю ответственность кредитных организаций за внедрение технологий защиты, управление персоналом и рисками поставщиков.

Ключевые слова: кибербезопасность, ответственность, ФинЦЕРТ, банковский сектор, Банк России, информационная безопасность, кибератаки, латентное присутствие, операционная надежность, нормативное регулирование.

LIABILITY FOR CYBERTHREATS IN THE BANKING SECTOR

Research article

Volkova D.A.[1, *], Revina S.N.[2]
[2] ORCID : 0000-0001-9565-1356;
[1, 2] Samara State University of Economics, Samara, Russian Federation

* Corresponding author (diana.vo2016[at]yandex.ru)

Suggested: 21.03.2026; Accepted: 30.04.2026; Published: 17.06.2026

Abstract

The article examines the concept of liability for cyberthreats in the banking sector of the Russian Federation in the context of the digital transformation of the financial market. Based on an analysis of FinCERT's empirical data, academic works by Russian researchers and the Bank of Russia's regulatory acts, the paper discusses the transformation of attackers' objectives, shifting the focus from direct theft of funds to destructive multi-stage operations. Particular attention is paid to the phenomenon of the dormant presence of attackers within information infrastructure as a key parameter for assessing the security of organisations. The paper systematises the requirements of key Bank of Russia regulations governing information security and operational reliability. It analyses the problem of attacks on supply chains and the need to monitor the security levels of contractors. The work substantiates the conclusion regarding a three-component structure of the accountability framework, comprising the regulator's regulatory framework, FinCERT's coordinating function, and the internal accountability of credit institutions for the implementation of security technologies, personnel management, and supplier risk management.

Keywords: cybersecurity, liability, FinCERT, banking sector, Bank of Russia, information security, cyberattacks, dormant presence, operational reliability, regulatory framework.

Введение

В эпоху стремительной цифровизации, пронизывающей все уровни социально-экономического взаимодействия, человечество столкнулось с парадоксальным последствием технологического прогресса, так беспрецедентное ускорение коммуникаций и упрощение бизнес-процессов обернулось пропорциональным ростом киберпреступности, поставившим под сомнение базовые гарантии безопасности.

В наибольшей степени эта диалектическая противоречивость проявилась в финансовой сфере, которая, будучи драйвером цифровой трансформации, превратилась в эпицентр киберугроз. Как аргументированно доказывают в своих исследованиях О.В. Лактюшина и Т.А. Горбачева, расширение цифрового ландшафта банковских услуг неизбежно продуцирует расширение атакуемой поверхности, делая кредитные организации первостепенной мишенью для злоумышленников [7, С. 27–40]. В данном контексте проблематика ответственности за киберугрозы обретает характер

сложносоставного, полиструктурного феномена, интегрирующего как прямую юридическую ответственность финансовых институтов за целостность данных и бесперебойность сервисов, так и регуляторно-надзорную функцию Банка России, формирующего нормативный фундамент и механизмы обеспечения соответствия обязательным требованиям.

Методы и принципы исследования

Обращаясь к эмпирическим данным, систематизированным в отчетах Центра взаимодействия и реагирования Департамента информационной безопасности (далее по тексту — ФинЦЕРТ), являющегося аналитическим ядром регулятора по противодействию кибератакам, невозможно не заметить не только количественную, но и качественную динамику угроз. Статистика регулятора за 2023 год демонстрирует 37-процентный рост атак на кредитные организации, причем эта восходящая траектория сохранила свою устойчивость и в 2024 году [9].

В контексте современной научной дискуссии о трансформации киберпреступности примечательным представляется вывод, сформулированный в аналитических материалах А.П. Буевич, согласно которому наблюдается фундаментальная перестройка целевых установок злоумышленников [5, С. 46–55]. Эволюция угроз выражается в последовательном смещении вектора противоправной деятельности от непосредственного завладения денежными средствами в сторону реализации деструктивных многостадийных сценариев, оказывающих системное воздействие на деятельность финансовой организации.

Содержательное наполнение данной тенденции раскрывается через совокупность взаимосвязанных угроз, а именно дестабилизацию операционных процессов, достигаемую путем компрометации конфиденциальной информации; психологическое воздействие на персонал, направленное на создание атмосферы неопределенности и паники; а также применение программ-блокировщиков, приводящее к временной или полной утрате контроля над информационными активами.

В сложившихся условиях принципиально важное значение для оценки действительного уровня защищенности кредитных организаций приобретает показатель продолжительности скрытого нахождения злоумышленников во внутренней инфраструктуре до момента реализации деструктивных действий. В научный оборот и практическую деятельность органов надзора данный параметр вошел под наименованием времени латентного присутствия (dwell time).

Как свидетельствуют данные ФинЦЕРТ, продолжительность такого скрытого пребывания может исчисляться несколькими месяцами, на протяжении которых осуществляется изучение архитектуры сети, сбор аутентификационных данных и подготовка условий для нанесения максимального ущерба. Указанное обстоятельство выдвигает на первый план проблему своевременного обнаружения признаков вторжения, поскольку к моменту выявления деструктивной активности злоумышленники, как правило, уже обладают устойчивым доступом к ключевым элементам информационной инфраструктуры и завершают подготовительную стадию атаки.

Необходимо подчеркнуть, что нормативно-правовой каркас, выстроенный Банком России, служит тем фундаментом, на котором базируется система ответственности финансовых организаций. Как резюмирует в своем исследовании А.П. Буевич, регулятором сформирован комплексный пакет документов, задающих эталонные стандарты защиты. Стержневым элементом этой системы выступает Положение Банка России от 17.08.2023 № 821-П, имплементирующее жесткие требования к информационной безопасности на всех этапах платежного цикла от идентификации клиентов до транзакционного обмена и архивирования данных [2].

В свою очередь неисполнение данных императивных требований инициирует каскад санкционных последствий, варьирующихся от административных штрафов до ограничения операционной деятельности, повышения страховых взносов в систему агентства страховых вкладов (АСВ) и, в экстремальных случаях, отзыва лицензии.

Существенной вехой в эволюции ответственности стало введение в действие в мае 2025 года Положения Банка России № 850-П «Об операционной надежности» [3]. Как подчеркивается А. Сергеевым в аналитических обзорах специализированного портала, новаторский характер данного документа заключается во внедрении количественно измеримых показателей допустимого времени простоя для критически значимых технологических процессов [8].

Для таких операций, как проведение платежей или кассовое обслуживание, законодательно фиксируются временные рамки восстановления, что трансформирует ответственность банка из формальной в содержательную. Так, организация обязана гарантировать непрерывность сервисов даже в условиях сложных целевых атак или деструктивных действий инсайдеров.

Стоит отметить, что Банк России помимо нормотворческой деятельности, направленной на пресечение угроз с правовой точки зрения, осуществляет превентивно-координирующую деятельность. Данная деятельность возложена и соответственно осуществляется ФинЦЕРТ, что отражено в статистических данных за 2024 год. В рамках анализа было выявлено, что в указанный временной период для участников финансового рынка было направлено более 360 бюллетеней с актуальными индикаторами компьютерных атак, а также 38 бюллетеней, которые отражали аналитическую информацию. Также в отчёте было отражено, что были проведены киберучения, в которых задействовали более 290 организаций финансовой сферы.

Анализ данных, отражённых в данном статистическом отчёте, также позволяет провести параллель между работой организаций по предупреждению данных угроз и игнорированием этих рекомендаций, которое впоследствии приводило к кибератакам.

Как подтверждение данного положения дел в отчёте были отражены случаи повторных атак, произошедшие в 2024 году. Так, несмотря на все предостережения о киберугрозах, уязвимость CVE-2022-27228 в системе 1С-Битрикс, которая была обнаружена ещё в 2022 году, несмотря на её устранение, была использована злоумышленниками впоследствии. Данным примером ФинЦЕРТ подчеркнул, что несмотря на устранение уязвимости, необходимо тщательно проверять все остальные системы, так как за время устранения кибератаки могут быть оставлены скрытые

элементы, которые позволяют совершить повторные атаки. Стоит отметить, что данный пример также свидетельствует о том, что в финансовых организациях недостаточный уровень ответственности по отношению к реальным киберугрозам, так как в данном случае пренебрежение установленным регламентам приводит к повторным атакам.

При анализе рассматриваемого отчета было выявлено, что наиболее популярным способом для получения первичного доступа к организации стала компрометация подрядных организаций. Так, в 2024 году было зафиксировано 17 инцидентов у ИТ-провайдеров, что поставило под удар более 70 финансовых компаний. Примечательно, что даже после получения 80 уведомлений о компрометации контрагентов, отдельные банки все же подверглись успешным целевым атакам, что отражает проблематику ответственности не только внутренней, но и экстерриториальной.

Обсуждение

Касаемо данной проблемы в научно-правовом обществе также сформировалась позиция. Так, в работе А.В. Зверева было указано, что банки обязаны не только следить за собственной безопасностью, но и внедрять проверяющие механизмы на уровень безопасности партнеров, с которыми они сотрудничают [6, С. 462–464]. С данным подходом нельзя не согласиться ввиду того, что внедрение бесперебойной проверки поступающих данных, а также строгая регламентация прав доступа позволят максимально обезопасить не только себя, но и контрагентов от формирования уязвимостей и дальнейших кибератак.

Данная проблема, к сожалению, в 2024 году заблокировала оптимальную работу у 300 небольших банков на всей территории Индии, когда группировка RansomEXX совершила атаку на C-Edge Technologies, которая была непосредственным поставщиком банковских систем [10]. Таким образом, данный пример является наглядным отражением того, почему так необходима защита от атак через цепочку поставок.

Показательно, что законодательная ветвь власти также движется по траектории ужесточения ответственности конечных бенефициаров и пособников киберпреступлений. Как детализируется в обзорах ФинЦЕРТ, с 1 января 2025 года вступили в силу поправки в Федеральный закон «О связи», ужесточающие идентификацию иностранных граждан при заключении договоров на связь [1]. Дополнительно, с 1 апреля 2025 года для граждан РФ вводится лимит на регистрацию сим-карт. Данные меры, по замыслу законодателя, направлены на деанонимизацию злоумышленников, использующих мобильные прокси и подменные номера, что является критически значимым для противодействия методам социальной инженерии.

Вместе с тем, как справедливо отмечают в своих исследованиях Е. Н. Беспалов и М. Ю. Мишина, абсолютизация технических средств защиты представляется методологически ошибочной [4, С. 46-51]. Вторая, не менее значимая составляющая — это культура кибербезопасности и персональная ответственность сотрудников. Эмпирические исследования демонстрируют, что до 30% работников могут стать жертвой фишинговой атаки при отсутствии систематического обучения. Ответственность за минимизацию этого человеческого фактора ложится на руководство, обязанное интегрировать программы повышения цифровой грамотности в корпоративные KPI. Регулятор активно стимулирует этот процесс, внедряя практику обязательных киберучений, стоит отметить, что только в 2024 году в них приняло участие более 290 организаций, и тестирований на проникновение.

Заключение

Резюмируя вышеизложенное, можно с достаточной степенью обоснованности констатировать, что институт ответственности за киберугрозы в российском банковском секторе представляет собой динамично эволюционирующую, многосубъектную систему, структурная организация которой базируется на трех фундаментальных элементах. Во-первых, это жесткий нормативный каркас, выстроенный Банком России, подкрепленный неотвратимостью санкционного воздействия. Во-вторых, это координирующая и превентивная функция ФинЦЕРТ, формирующего единое информационное поле для противодействия угрозам. В-третьих, это внутренняя ответственность самих кредитных организаций, которые, как справедливо заключает в своей работе А.П. Буевич, призваны не только имплементировать передовые технологии защиты, но и формировать культуру безопасности, управлять рисками поставщиков и минимизировать уязвимости персонала.

Именно синергия этих трех компонентов, по единодушному мнению, исследовательского сообщества, выступает необходимым и достаточным условием обеспечения устойчивости финансовой системы и сохранения доверия к ней в эпоху перманентного киберпротивостояния.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Российская Федерация. О связи: Федеральный закон от 07 июля 2003 г.№ 126-ФЗ: [в редакции от 20 февраля 2026 г.] : Федеральный закон №126-ФЗ 2003.

2. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при

осуществлении переводов денежных средств : Положение Банка России от 17 августа 2023 г. № 821-П. — URL: https://www.consultant.ru/document/cons_doc_LAW_363973/ (дата обращения: 10.03.2026).

3. Об обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг : Положение Банка России от 13 января 2025 г. № 850-П. — Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.03.2026).

4. Беспалов Е.Н. Киберугрозы в цифровом банковском секторе и механизмы их предотвращения / Е.Н. Беспалов, М.Ю. Мишина. // Тенденции и перспективы развития банковской системы в современных экономических условиях. Т. 1: материалы VI всероссийской научно-практической конференции с международным участием (26 декабря 2024 года); — Брянск: РИСО БГУ, 2025. — С. 46–51.

5. Буевич А.П. Киберугрозы как современный вызов безопасности банковского сектора в России / А.П. Буевич // Национальная безопасность / nota bene. — 2025. — № 4. — С. 46–55.

6. Зверев А.В. Цифровизация как метод конкурентной борьбы в банковском секторе / А.В. Зверев, О.А. Денисенко // Таможенное администрирование и экономическая безопасность в цифровой экономике. — 2019. — С. 462–464.

7. Лактюшина О.В. Киберугрозы в банковской сфере и направления их снижения в Российской Федерации / О.В. Лактюшина, Т.А. Горбачева // Вестник Московского университета имени С.Ю. Витте. Серия 1: Экономика и управление. — 2025. — С. 27–40.

8. Сергеев А. Как российские банки защищают данные клиентов от киберугроз / А. Сергеев. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-Russian-banks-protect-data?ysclid=mmoi7msfas890349430#part32 (дата обращения: 12.04.2026)

9. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году // Центральный банк Российской Федерации. — URL: https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (дата обращения: 12.04.2026)

10. Cyberthreats to the financial sector: forecast for 2025–2026. — URL: https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-the-financial-sector--forecast-for-2025-2026/#Navigation-1 (accessed: 12.04.2026)

Список литературы на английском языке / References in English

1. Russian Federation. O svyazi: Federal'ny'j zakon ot 07 iyulya 2003 g.№ 126-FZ: [v redakcii ot 20 fevralya 2026 g.] [On Communications: Federal Law No. 126-FZ dated July 7, 2003: [as amended on February 20, 2026]] : Federal Law №126-ФЗ 2003. [in Russian]

2. O trebovanijah k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv i o porjadke osushhestvlenija Bankom Rossii kontrolja za sobljudeniem trebovanij k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv [On requirements for ensuring information protection in the implementation of money transfers and on the procedure for the Bank of Russia to exercise control over compliance with requirements for ensuring information protection in the implementation of money transfers] : Regulation of the Bank of Russia No. 821-P of August 17, 2023. — URL: https://www.consultant.ru/document/cons_doc_LAW_363973/ (accessed: 10.03.2026). [in Russian]

3. Ob objazatel'nyh dlja kreditnyh organizacij, inostrannyh bankov, osushhestvljajushhih dejatel'nost' na territorii Rossijskoj Federacii cherez svoi filialy, trebovanijah k operacionnoj nadezhnosti pri osushhestvlenii bankovskoj dejatel'nosti v celjah obespechenija nepreryvnosti okazanija bankovskih uslug [On mandatory requirements for credit institutions and foreign banks operating on the territory of the Russian Federation through their branches for operational reliability in the implementation of banking activities to ensure continuity of banking services] : Regulation of the Bank of Russia No. 850-P of January 13, 2025. — Access from the reference-legal system «Konsul'tantPljus» (accessed: 10.03.2026). [in Russian]

4. Bespalov E.N. Kiberugrozy' v cifrovom bankovskom sektore i mexanizmy' ix predotvrashheniya [Cyber threats in the digital banking sector and their prevention mechanisms] / E.N. Bespalov, M.Yu. Mishina. // Trends and Prospects for the Development of the Banking System in Modern Economic Conditions. Vol. 1: Proceedings of the 6th All-Russian Scientific and Practical Conference with International Participation (December 26, 2024); — Bryansk: RISO BGU, 2025. — P. 46–51. [in Russian]

5. Buevich A.P. Kiberugrozy kak sovremennyj vyzov bezopasnosti bankovskogo sektora v Rossii [Cyber threats as a modern challenge to the security of the banking sector in Russia] / A.P. Buevich // Nacional'naja bezopasnost' / nota bene [National Security / nota bene]. — 2025. — № 4. — P. 46–55. [in Russian]

6. Zverev A.V. Cifrovizacija kak metod konkurentnoj bor'by v bankovskom sektore [Digitalization as a method of competition in the banking sector] / A.V. Zverev, O.A. Denisenko // Tamozhennoe administrirovanie i jekonomicheskaja bezopasnost' v cifrovoj jekonomike [Customs administration and economic security in the digital economy]. — 2019. — P. 462–464. [in Russian]

7. Laktjushina O.V. Kiberugrozy v bankovskoj sfere i napravlenija ih snizhenija v Rossijskoj Federacii [Cyber threats in the banking sector and directions for their reduction in the Russian Federation] / O.V. Laktjushina, T.A. Gorbacheva // Vestnik Moskovskogo universiteta imeni S.Ju. Vitte. Serija 1: Jekonomika i upravlenie [Bulletin of Moscow Witte University. Series 1: Economics and Management]. — 2025. — P. 27–40. [in Russian]

8. Sergeev A. Kak rossijskie banki zashhishhajut dannye klientov ot kiberugroz [How Russian banks protect customer data from cyber threats] / A. Sergeev. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-Russian-banks-protect-data?ysclid=mmoi7msfas890349430#part32 (accessed: 12.04.2026) [in Russian]

9. Obzor osnovnyh tipov komp'juternyh atak v finansovoj sfere v 2024 godu [Overview of the main types of computer attacks in the financial sector in 2024] // Central'nyj bank Rossijskoj Federacii [Central Bank of the Russian Federation]. — URL: https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (accessed: 12.04.2026) [in Russian]

10. Cyberthreats to the financial sector: forecast for 2025–2026. — URL: https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-the-financial-sector--forecast-for-2025-2026/#Navigation-1 (accessed: 12.04.2026)