Национальная безопасность / nota bene
Правильная ссылка на статью:
Буевич А.П. Киберугрозы как современный вызов безопасности банковского сектора в России // Национальная безопасность / nota bene. 2025. № 4. DOI: 10.7256/2454-0668.2025.4.74921 EDN: RAPRMK URL: https://nbpublish.com/library_read_article.php?id=74921

Киберугрозы как современный вызов безопасности банковского сектора в России

Буевич Анжелика Петровна

ORCID: 0000-0001-8936-9135

кандидат экономических наук

доцент; кафедра экономической теории; Финансовый университет при Правительстве РФ

125167, Москва, пр-кт Ленинградский, д. 49/2

buanpeet@mail.ru

Статья из рубрики "Научно-техническое обеспечение национальной безопасности"

DOI:

10.7256/2454-0668.2025.4.74921

EDN:

RAPRMK

Дата направления статьи в редакцию:

20-06-2025

Дата публикации:

25-08-2025

Аннотация: С развитием цифровых технологий и повсеместной цифровизацией финансовых услуг наблюдается экспоненциальный рост количества и сложности киберугроз, которые представляют серьёзный системный вызов для различных сфер экономики, но особенно – для банковской отрасли как ключевого элемента финансовой инфраструктуры государства. По данным Банка России, в 2023 году количество кибератак на кредитные организации увеличилось на 37% по сравнению с предыдущим годом, при этом 68% атак были направлены на клиентские данные и платежные системы, а средний размер ущерба от успешной атаки составил около 15 млн рублей. Именно поэтому увеличение уровня кибербезопасности сегодня является не просто приоритетной задачей, а стратегической необходимостью для обеспечения

экономической стабильности финансового сектора и национальной безопасности страны в целом. Цель исследования заключается в комплексной оценке существующих мер противодействия киберугрозам в российском банковском секторе, анализе их эффективности и выработке рекомендаций по совершенствованию защитных механизмов. В работе использованы методы сравнительного анализа, экспертные оценки и изучение реальных кейсов кибератак за период 2020-2024 гг. В ходе проведения исследования была детально проанализирована ключевая роль Банка России как мегарегулятора финансового рынка в решении возникающих проблем. При этом было выявлено, что крупные кредитные организации также занимают особое место в противодействии угрозам, внедряя в свои системы различные инструменты предотвращения кибератак. Однако небольшие финансовые организации по-прежнему остаются под угрозой. Это, в совокупности с активным развитием схем мошенничества, обусловливает необходимость дальнейшего совершенствования стратегии борьбы с кибератаками. Исследование основано на анализе регуляторной практики Банка России, данных FinCERT и опроса 50 экспертов банковского сектора. Результаты могут быть использованы для совершенствования подходов к управлению киберрисками на всех уровнях финансовой системы России.

Ключевые слова:

кибербезопасность, цифровые технологии, финансовый сектор, кредитные организации, киберугрозы, банковская безопасность, кибератаки, Банк России, финансовая кибербезопасность, Финтех-риски

Введение

С развитием цифровых технологий растёт и число киберугроз, которые представляют серьёзный вызов для различных сфер, особенно для банковской отрасли. Кибератаки становятся всё более изощрёнными, наносят значительный финансовый ущерб, подрывают доверие клиентов и замедляют внедрение новых технологий. Для успешной цифровой трансформации банковского сектора важно не только развивать инновации, но и защищать финансовые активы и данные от утечек и несанкционированного доступа. Именно поэтому увеличение уровня кибербезопасности сегодня является одной из приоритетных задач для обеспечения экономической безопасности финансового сектора и всей страны.

Вопросами изучения развития финансового сектора занимаются многие исследователи, в частности Гранкина Я. А., Баймедетов С. Д.[3], Зайнулабидов М.Х., Исаев О.В., Толстых О.В.[4], Лактюшина О.В., Горбачева Т.А.[5] и т.д. Тем не менее, несмотря на обилие исследований в данной сфере, важным остаётся вопрос комплексного анализа существующих мер противодействия киберугрозам в России, выявления роли разных институтов в реализации данных мер и их эффективности.

Цель исследования заключается в оценке существующих мер противодействия киберугрозам в России и выявлении их эффективности.

Новизна исследования состоит в консолидации существующей информации касательно существующих механизмов противодействия киберугрозам с целью выявления роли различных институтов в решении возникшей проблемы, а также эффективности реализации мер на территории России.

При проведении исследования был осуществлен анализ, оценка и сопоставление статистической и аналитической информации, связанной с данной проблемой, а также нормативно-правовой базы РФ.

Основная часть

Пандемия COVID-19 ускорила переход многих процессов в цифровую среду. Бизнес, образование, государственные услуги и даже личное общение массово переместились в онлайн. Это дало новые возможности — от удалённой работы до онлайн-покупок и цифровых сервисов. Но одновременно с этим открылось и больше уязвимостей, которыми начали активно пользоваться киберпреступники.

Например, в условиях удалённой работы компании стали использовать больше облачных сервисов, видео платформ и систем удалённого доступа. Эти инструменты упростили жизнь, но также создали новые точки входа для хакеров [4]. Начались атаки на корпоративные сети, взломы учетных записей, утечки данных и фишинговые кампании, которые значительно осложнили работу многих организаций.

Для банков такие угрозы особенно опасны. Утечка клиентских данных, взлом платёжных систем или сбой в работе цифровой инфраструктуры могут привести не только к финансовым потерям, но и к утрате доверия со стороны клиентов. Это делает вопрос кибербезопасности ключевым для успешной работы банков в цифровую эпоху [5].

Сегодня банки активно инвестируют в защиту своих систем: внедряют искусственный интеллект для обнаружения угроз, усиливают шифрование данных, проводят киберучения и тестируют свои системы на устойчивость к атакам. Одновременно регуляторы, такие как Банк России, разрабатывают рекомендации и нормативные акты, чтобы повысить уровень безопасности в финансовом секторе.

Кибербезопасность теперь — это не просто защита от угроз, а основа, на которой строится современная экономика любой страны [14]. Только эффективно управляя киберрисками, банки и другие организации смогут безопасно внедрять новые технологии и ускорять цифровую трансформацию, делая её безопасной для клиентов и бизнеса.

Резкий рост числа кибератак привёл к повышенному вниманию со стороны государства и бизнеса к вопросам информационной безопасности [3]. Банки стали выделять всё большую часть своих расходов на обеспечение киберзащиты, что вызвало рост спроса на инновационные технологии в этой сфере и поставило новые задачи перед регуляторами банковской системы.

Согласно данным Банка России, количество жалоб клиентов операторов денежных переводов, включая банки, на несанкционированное использование их электронных платежных средств продолжает увеличиваться с каждым кварталом. Это подчёркивает необходимость усиления мер по защите финансовых систем от киберугроз.

Все, кто связан с банковской системой, активно работают над развитием технологий кибербезопасности.

Банк России разрабатывает нормативные акты, устанавливающие требования к обеспечению информационной безопасности. Одним из ключевых документов в этой области является Положение от 17 августа 2023 года № 821-П «О требованиях к обеспечению информационной безопасности при осуществлении переводов денежных средств и порядке осуществления Банком России контроля за соблюдением указанных

требований» [2]. Данное положение является важной основой и включает в себя:

· Идентификация и авторизация клиента. Банки должны защищать данные клиентов в процессе идентификации, чтобы минимизировать риск мошенничества.

· Передача сообщений. Все транзакционные операции и связанные с ними данные должны передаваться по защищенным каналам связи, чтобы предотвратить перехват данных мошенниками.

· Выполнение транзакций. Денежные переводы должны иметь надежную защиту для предотвращения несанкционированного изменения данных транзакции.

· Хранение информации о переводах. Данные о завершенных транзакциях должны надежно храниться для предотвращения утечек или несанкционированного доступа. Кроме того, регламент требует от финансовых организаций регулярно тестировать и совершенствовать свои системы информационной безопасности. В частности, они должны ежегодно проводить следующее:

· Тестирование на уязвимости. Выявление слабых мест в системах безопасности и оперативное их устранение.

· Анализ уровня безопасности. Оценка эффективности существующих мер и разработка новых подходов к защите информации.

· Внешние независимые оценки. Привлечение внешних аудиторов, уполномоченных подтверждать, что меры информационной безопасности учреждения соответствуют требованиям регламента Банка России.

Согласно положению Банка России от 16 декабря 2003 года № 242-П «О внутреннем контроле в кредитных организациях и банковских группах», кредитные организации обязаны включать в планы действий на случай непредвиденных обстоятельств меры по обеспечению информационной безопасности для обеспечения непрерывности деятельности или ее восстановления в случае возникновения нестандартных или чрезвычайных ситуаций [1]. Кроме того, они должны соблюдать различные стандарты, например Стандарт № 822-СТ «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Основные организационно-технические меры» [13].

В случае несоблюдения требований информационной безопасности кредитные организации могут столкнуться с мерами со стороны регуляторов. Среди возможных последствий: повышение страховых взносов в АСВ, ограничение на оказание некоторых услуг, наложение штрафов или даже лишение лицензии на ведение банковской деятельности.

Однако деятельность Банка России в этой области не ограничивается лишь санкциями. Регулятор также проводит превентивный надзор, формируя стратегию развития информационной безопасности в финансовом секторе. Кроме того, он разрабатывает безопасные технологии и рекомендации, направленные на повышение защиты данных в банковской сфере.

Согласно документу Банка России «Основные направления развития технологий Suptech и Regtech на период 2021–2023 годов» [9], регулятор поставил перед собой несколько ключевых задач в области информационной безопасности. Эти задачи направлены на

защиту финансовой системы и создание более устойчивой и надёжной инфраструктуры в условиях стремительной цифровизации.

Для достижения этих целей Банк России работает над созданием безопасной и современной финансовой инфраструктуры. Среди примеров успешных инициатив:

· «Маркетплейс» - платформа, обеспечивающая удобный и прозрачный доступ к финансовым услугам;

· «Цифровой профиль» - инструмент, упрощающий идентификацию клиентов и обеспечивающий надёжную защиту их данных;

· Системы для регистрации сделок;

· Технологии распределённых реестров;

· Система быстрых платежей;

· Облачные платёжные платформы.

Банк России также активно работает над практическими мерами для повышения устойчивости всей системы. Например:

· Совершенствование аудита. Идея данной инициативы заключалась в том, чтобы аккредитованные аудиторы проводили независимую проверку надёжности инфраструктуры и приложений компаний, основываясь на национальных стандартах. Кроме того, планировалось разработать концепцию добровольной сертификации, чтобы убедиться, что финансовые организации соблюдают требования по информационной безопасности. Эти меры направлены на повышение доверия к системе и её устойчивости перед возможными киберугрозами.

· Проведение киберучений. В рамках данной инициативы планируется разрабатывать специальные механизмы / процедуры для оценки уровня киберустойчивости банковского сектора. Другими словами, будут разработаны параметры стресс-тестирования киберрисков. Подобного рода процедуры помогут снизить риски финансовых потерь клиентами от кибератак, а также повысят эффективность мероприятий по противодействию киберугрозам.

Дополнительно, в рамках документа Банка России «Основные направления цифровизации финансового рынка на 2022–2024 годы» было предусмотрено внедрение инструментов и механизмов для борьбы с киберугрозами и мошенничеством [10]. Основные усилия были сосредоточены на реализации следующих задач:

1. Внедрение облачной усиленной квалифицированной электронной подписи (УКЭП);

2. Обеспечение поднадзорных организаций УКЭП;

3 . Создание доверенной среды для безопасного предоставления финансовых услуг удалённо;

4 . Уменьшение убытков от операций, проводимых через удалённые каналы обслуживания;

5. Внедрение института киберучений;

6. Улучшение информационного обмена через ФинЦЕРТ.

И, как можно заметить, данные направления в большинстве своём были успешно реализованы.

Таким образом, становится очевидно, что сегодня Банк России уделяет особое внимание разработке и совершенствованию нормативной базы для защиты информации, а также созданию стандартов и правил для повышения уровня безопасности.

Однако в то же время важно заметить, что финансовые организации также уделяют немалое внимание защите информации. Так, банки не только инвестируют в новые технологии, но и обеспечивают трансформацию своих внутренних процессов. Например, они внедряют системы на основе искусственного интеллекта, которые помогают быстрее обнаруживать угрозы и реагировать на них. Регулярно проводятся киберучения и стресс-тесты для подготовки систем к потенциальным атакам и минимизации последствий.

Более того, помимо технических решений, банки уделяют особое внимание и обучению сотрудников. Человеческие ошибки играют важную роль в защите данных, поэтому регулярное повышение квалификации сотрудников имеет решающее значение для предотвращения кибератак или минимизации ущерба, который они наносят.

Все эти меры направлены на то, чтобы клиенты могли доверять сохранности своих данных и средств. Таким образом, обеспечение кибербезопасности банковской системы становится основой её успешной цифровой трансформации, поскольку оно не только способствует укреплению доверия клиентов, но и помогает банкам уверенно развиваться в условиях стремительной цифровизации. В современном мире кибербезопасность — это уже не просто дополнительная мера, а ключевой элемент успешного функционирования любой финансовой организации.

Рассмотрим на примере АО «Тинькофф Банк», который в свою очередь является лидеров на рынке финансовых технологий, в том числе, благодаря специфики своей деятельности.

В 2017 году в кредитной организации была создана должность инспектора по информационной безопасности, а также нанят дополнительный эксперт по кибербезопасности [11]. Это было сделано для усиления усилий банковской группы АО «Тинькофф Банк» в период с 2019 по 2020 годы по предупреждению и предотвращению новых угроз в сфере информационной безопасности.

В 2018 году, совместно с международной компанией Group-IB, специализирующейся на предотвращении кибератак, банк внедрил эшелонированную систему кибербезопасности. Она основана на использовании продуктов для выявления угроз нулевого дня и предотвращения целевых атак. Кроме того, была запущена совместная с операторами связи IT-платформа, которая позволяет выявлять мошеннические звонки. Эти данные интегрируются в системы информационной безопасности банка.

В 2019 году банк, в сотрудничестве с SafenSoft, внедрил первую в России само обновляющуюся систему защиты банкоматов. Эта система позволяет обновлять программное обеспечение в ответ на новые угрозы без остановки работы банкоматов и без участия инженеров, полностью в дистанционном режиме.

В 2021 году банк запустил масштабный проект — комплексную платформу безопасности «Тинькофф Защита», направленную на обеспечение максимального уровня защиты данных и операций (рис. 1) [12].

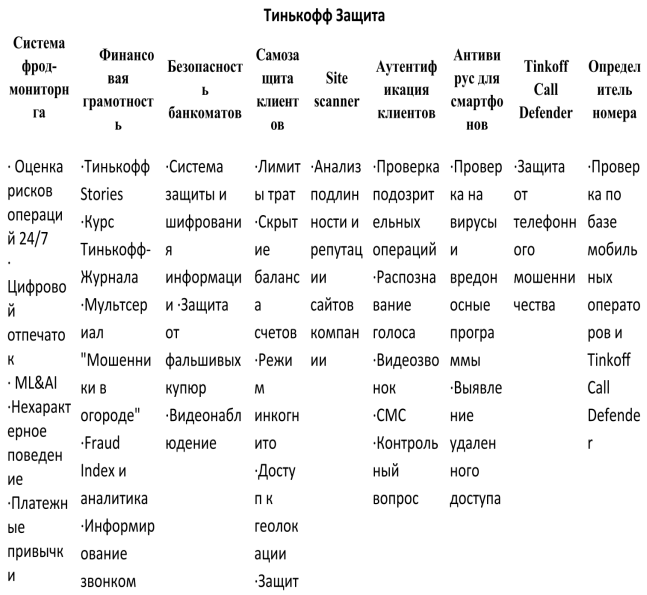

Рисунок 1. Платформа безопасности «Тинькофф Защита».

Как видно по данным рисунка, платформа включает в себя традиционные и новые технологии защиты средств клиентов, разработанные в экосистеме Тинькофф (в частности, Tinkoff Call Defender, selfie-аутентификация). Задачей платформы является обеспечение безопасности розничных, бизнес-клиентов и партнеров экосистемы в любых пользовательских сценариях (открытие счета, вход в приложение или интернет-банк, проведение транзакций и др), предотвращение атаки мошенников, минимизация клиентских потерь и повышение финансовой грамотности среди жителей России.

Однако, несмотря на такое разнообразие мер, в период с 2022 по 2024 гг. заметно возросло количество атак с использованием методов социальной инженерии: в 2023 году их число выросло на 20%, а в 2024 году — еще на 8,3% (таблица 1). В то же время наблюдается постепенное снижение распространенности фишинговых атак (на 20% в 2023 году и на 8,3% в 2024 году), атак с использованием вредоносного ПО (программного обеспечения) (на 25% в 2023 году и на 33,3% в 2024 году) и DDoS-атак (на 20% в 2023 году и на 10% в 2024 году) [6-8].

Таблица 1

Основные типы компьютерных атак

Тип атаки (ед.) / Период	III кв. 2022 года	III кв. 2023 года	III кв. 2024 года	Прирост 2023 к 2022 (%)	Прирост 2024 к 2023 (%)
Использование методов социальной инженерии	15 000	18 000	19 500	+20%	+8.3%
Фишинговые атаки	1 500	1 200	1 100	-20%	-8,3%
Атаки с использованием ВПО	200	150	100	-25%	-33,3%
Атаки типа					

Атаки типа «отказ в обслуживании» (DDoS)	250	200	180	-20%	-10%

Источник: составлено автором на основе данных из открытых источников.

Именно такое положение вещей свидетельствует о несовершенстве существующей системы предотвращения кибератак и необходимости поиска новых путей её модернизации.

Выводы

В заключение следует отметить, что стремительный рост технологий стал ключевым фактором развития финансового сектора как в России, так и в других странах. Таким образом, перед в таких изменяющихся условиях, перед банковским сектором стоят такие важные задачи, как защита данных клиентов и обеспечение информационной безопасности.

Банк России играет важнейшую роль в решение указанных выше задач. Он разрабатывает нормативные акты и стандарты, направленные на повышение безопасности, внедряет передовые технологии и задает стратегическое направление будущего развития банковского сектора. Все это, способствует поддержанию стабильности и надежности для всех участников финансового рынка.

Крупные кредитные организации используют инновационные технологии для защиты данных, что значительно снижает финансовые риски от кибератак. Для небольших финансовых учреждений выполнение всех требований информационной безопасности остается серьезной проблемой. Поэтому крайне важно подчеркнуть необходимость доступных и универсальных решений, которые могут быть реализованы финансовыми учреждениями всех размеров, гарантируя, что преимущества технологических достижений будут доступны всему банковскому сектору.

При этом также сохраняется необходимость в модернизации существующих мер предотвращения кибератак ввиду их активного распространения и постоянного появления новых способов кражи данных.

Библиография

1. Положение Банка России от 16 декабря 2003 года № 242-П "О внутреннем контроле в кредитных организациях и банковских группах" // Вестник Банка России. – 2004. – 4 февраля. – № 7. [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_46304/
2. Положение от 17 августа 2023 года № 821-П "О требованиях к обеспечению информационной безопасности при осуществлении переводов денежных средств и порядке осуществления Банком России контроля за соблюдением указанных требований" // Вестник Банка России. – 2023. – 21 декабря. – № 76. [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_464233/ (дата обращения: 21.06.2025).
3. Гранкина Я. А., Баймедетов С. Д. Кибербезопасность в современном мире: актуальные угрозы и методы защиты // Вестник науки. – 2024. – № 11 (80). – С. 864-870. EDN: RUZZZK
4. Зайнулабидов М. Х., Исаев О. В., Толстых О. В. Киберпреступления в кредитно-финансовой сфере // Закон и право. – 2024. – № 8. – С. 68-73. DOI: 10.24412/2073-

3313-2024-8-68-73 EDN: MVSUQU
5. Лактюшина О. В., Горбачева Т. А. Киберугрозы в банковской сфере и направления их снижения в Российской Федерации // Вестник Московского университета имени С. Ю. Витте. Серия 1: Экономика и управление. – 2025. – № 1 (52). – С. 27-39. DOI: 10.21777/2587-554X-2025-1-27-40 EDN: HRTNXQ
6. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2022 года // ЦБ РФ. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/ib/review_3q_2022/ (дата обращения 21.06.2025).
7. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2023 года // ЦБ РФ. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/ib/review_3q_2023/ (дата обращения 21.06.2025).
8. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2024 года // ЦБ РФ. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/ib/review_3q_2024/ (дата обращения 21.06.2025).
9. Основные направления развития технологий Suptech и Regtech на период 2021-2023 годов // ЦБ РФ. – 2021. [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/content/document/file/120709/suptech_regtech_2021-2023.pdf (дата обращения 21.06.2025).
10. Основные направления развития финансовых технологий // ЦБ РФ. [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/about_br/publ/onfintech/ (дата обращения: 21.06.2025).
11. Специалисты по информационной безопасности в ТБанке // ТБанк. [Электронный ресурс]. – Режим доступа: https://www.tbank.ru/career/it/security/ (дата обращения: 21.06.2025).
12. Тинькофф запустил "Тинькофф Защиту" – комплексную платформу безопасности экосистемы // ТБанк. – 2021. [Электронный ресурс]. – Режим доступа: https://www.tbank.ru/about/news/02062021-tinkoff-launched-tinkoff-defense-comprehensive-ecosystem-security-platform/ (дата обращения: 21.06.2025).
13. Утвержден новый национальный стандарт безопасности банковских и финансовых операций // ЦБ РФ. – 2017. [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/eng/press/event/?id=1274 (дата обращения 21.06.2025).
14. Чапаев Н. М. Современное состояние кибербезопасности в Российской Федерации // Журнал прикладных исследований. – 2024. – № S2. – С. 178-182. DOI: 10.47576/2949-1878.2024.91.13.025 EDN: RFWKOR

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в рецензируемой работе выступают вопросы обеспечения кибербезопасности банковского сектора в России.
Методология исследования базируется на проведении анализа, оценки и сопоставления статистической и аналитической информации, связанной с решаемой в работе проблемой, а также на изучении нормативно-правовой базы РФ в сфере обеспечения информационной безопасности банковского сектора.
Актуальность работы авторы справедливо связывают с ростом числа киберугроз, которые представляют серьёзный вызов для банковской отрасли, с тем, что кибератаки становятся всё более изощрёнными, наносят значительный финансовый ущерб, подрывают доверие клиентов и замедляют внедрение новых технологий.

Структурно в тексте выделены следующие разделы: Введение, Основная часть, Выводы и Библиография.

Заявленная авторами научная новизна исследования заключается «в консолидации существующей информации касательно существующих механизмов противодействия киберугрозам с целью выявления роли различных институтов в решении возникшей проблемы, а также эффективности реализации мер на территории России».

В статье отмечено, что в настоящее время банки активно инвестируют в защиту своих систем: внедряют искусственный интеллект для обнаружения угроз, усиливают шифрование данных, проводят киберучения и тестируют свои системы на устойчивость к атакам; Банк России разрабатывает рекомендации и нормативные акты для повышения уровня безопасности в финансовом секторе. Однако, растет количество жалоб на несанкционированное использование электронных платежных средств, что подчёркивает необходимость усиления мер по защите финансовых систем от киберугроз. В публикации приведены примеры успешных инициатив ЦБ РФ по созданию безопасной и современной финансовой инфраструктуры, а также практические меры для повышения устойчивости всей банковской системы. В работе детально рассмотрен масштабный проект одного из коммерческих банков – комплексная платформа безопасности «Тинькофф Защита», направленная на обеспечение максимального уровня защиты данных и операций, проведен анализ основных типов компьютерных атак в этом банке.

Библиографический список включает 14 источников – научные публикации отечественных и зарубежных авторов на русском и иностранных языках по рассматриваемой теме, а также интернет-ресурсы. На источники, приведенные в разделе «Библиография» по тексту приводятся адресные отсылки, подтверждающие наличие апелляции к оппонентам.

Из недостатков публикации стоит отметить, что авторами не соблюдены принятые редакцией Правила оформления списка литературы в части количества и категорий источников: «… не менее 20 источников…, не менее трети зарубежных источников; не менее половины работ, изданных в последние 3 года. … В списке литературы не указываются: нормативно-правовая документация; … Интернет-источники, включая информацию с сайтов, а также статьи на сайтах и в блогах…Все вышеперечисленные источники упоминаются в тексте статьи в скобках, наряду с прочими комментариями и примечаниями авторов».

Рецензируемый материал соответствует направлению журнала «Национальная безопасность / nota bene», отражает результаты проведенного авторами исследования, может вызвать интерес у читателей, материал рекомендуется к опубликованию после доработки оформления списка литературы.