https://doi.org/10.25559/SITITO.022.202601.28-39
УДК 004.9

Оригинальная статья

Кибербезопасность как составляющая национальной безопасности: теоретические и прикладные аспекты

Е. А. Богданов, А. Н. Когтева, Р. С. Танчук*
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва, Российская Федерация
Адрес: 125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2
* rstanchuk@fa.ru

Аннотация

Введение. В современных условиях кибербезопасность признается важнейшим фактором обеспечения национальной безопасности государства. Широкомасштабное внедрение цифровых технологий сопровождается ростом киберугроз, способных нанести ущерб государственной безопасности, экономике и правам граждан. В Российской Федерации кибербезопасность традиционно рассматривается в контексте информационной безопасности, являясь ее неотъемлемой частью. Стратегия национальной безопасности Российской Федерации 2021 г. и другие основополагающие документы закрепляют защиту информационного пространства и устойчивость критической информационной инфраструктуры (далее – КИИ) среди стратегических приоритетов государства. В то же время стремительное развитие киберпреступности и кибератак выявляет недостатки действующего правового регулирования и практики, требуя научного осмысления и обновления подходов.

Материалы и методы. Эмпирическая база включает анализ стратегических и нормативных актов Российской Федерации (Конституция; Доктрина информационной безопасности; Стратегия национальной безопасности; федеральные законы «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной инфраструктуры Российской Федерации», «О персональных данных» и подзаконные акты), официальные методические документы регуляторов (ФСТЭК, ФСБ, Роскомнадзор), разъяснения высших судов по цифровым доказательствам, а также открытые государственные статистические массивы и отчеты отраслевых центров реагирования. Для сопоставления использованы зарубежные регуляторные модели (на уровне стратегий и рамочных актов) и международные инициативы (ООН, региональные форматы). Применены формально-юридический, сравнительно-правовой и системно-структурный методы; метод правовой политики и риск-ориентированного регулирования; анализ норм и правоприменительной практики (2019-2025 гг.); элементы *case-study* по инцидентам в КИИ. Верификация выводов осуществлялась через перекрестное сопоставление нормативных требований, практики надзора и доступных статистических рядов.

Результаты исследования. Получена интегральная модель правового обеспечения кибербезопасности как подсистемы национальной безопасности, включающая четыре блока.

1) Доктринально-понятийный: предлагается нормативно закрепить дефиниции «кибербезопасность», «киберустойчивость», «кибератака», провести унификацию терминологии через целевые поправки в федеральные законы «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной инфраструктуры Российской Федерации», а также утвердить отдельную Стратегию кибербезопасности Российской Федерации с таксономией рисков и уровнями реагирования.

2) Институциональный: обосновано создание национального координатора (межведомственного органа) с мандатом на управление инцидентами, сетью отраслевых CSIRT и режимом «единого окна» для уведомлений; вводится обязанность значимых операторов сообщать о существенных инцидентах в регулятор в течение установленного срока с защитой добросовестного раскрытия.

3) Регуляторный: предложен рамочный закон о кибербезопасности, который устанавливает минимальные базовые меры, профили по секторам КИИ, риск-градуированное надзорное воздействие и механизмы поощрения независимых аудитов и баг-баунти.
4) Уголовный, в т.ч. уголовно-процессуальный, и международный: уточняются правила обращения с цифровыми доказательствами, вводится состав киберсаботажа в отношении КИИ, расширяются процессуальные возможности трансграничного получения е-доказательств; предусмотрена имплементация международных инструментов и приоритизация кооперации в дружественных региональных форматах.
Отдельно предложен блок по технологическому суверенитету: поэтапные преференции закупок, требования *secure-by-design* и жизненного цикла, метрики MTTD/MTTR и аудит готовности.
Обсуждение и заключение. Предложенная архитектура устраняет ключевые дефекты нынешнего режима: понятийную неопределенность, фрагментацию требований и слабую координацию инцидентов. Риско-ориентированная модель снижает регуляторные издержки за счет пропорциональности мер и предсказуемости надзора, а *safe harbor* и публично-частное партнерство повышают качество раскрытия уязвимостей. В то же время необходимы предохранители прав: судебный контроль за доступом к шифрованным данным, процессуальные гарантии при работе с е-доказательствами, прозрачность отчетности регуляторов и независимый аудит. Практическая реализация должна быть поэтапной (пилоты в секторах КИИ, затем масштабирование), с четкими метриками (MTTD/MTTR, доля инцидентов с восстановлением в целевом SLA, охват CSIRT), пересмотром каждые 2-3 года и синхронизацией с программами импортонезависимости. В результате повышается киберустойчивость государства и снижается системный риск для безопасности, экономики и прав граждан; Российская Федерация получает согласованный правовой инструментариум, совместимый с международной кооперацией и целями технологического суверенитета.

Ключевые слова: кибербезопасность, национальная безопасность, информационная безопасность, информационное право, киберпреступность, критическая информационная инфраструктура

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Богданов Е. А., Когтева А. Н., Танчук Р. С. Кибербезопасность как составляющая национальной безопасности: теоретические и прикладные аспекты // Современные информационные технологии и ИТ-образование. 2026. Т. 22, № 1. С. 28-39. https://doi.org/10.25559/SITITO.022.202601.28-39

Original article

Cybersecurity as a Component of National Security: Theoretical and Applied Aspects

E. A. Bogdanov, A. N. Kogteva, R. S. Tanchuk*
Financial University under the Government of the Russian Federation, Moscow, Russian Federation
Address: 49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation
* rstanchuk@fa.ru

Abstract

Introduction. In modern conditions, cybersecurity is recognized as the most important factor in ensuring the national security of the state. The large-scale introduction of digital technologies is accompanied by an increase in cyber threats that can damage state security, the economy and the rights of citizens. In the Russian Federation, cybersecurity is traditionally considered in the context of information security, being an integral part of it. The National Security Strategy of the Russian Federation 2021 and other fundamental documents consolidate the protection of the information space and the sustainability of critical information infrastructure (hereinafter referred to as CII) among the strategic priorities of the state. At the same time, the rapid development of cybercrime and cyber attacks reveals the shortcomings of current legal regulation and practice, requiring scientific reflection and updating approaches.

Materials and Methods. The empirical base includes an analysis of strategic and regulatory acts of the Russian Federation (Constitution; Information Security Doctrine; National Security Strategy; Federal Laws "On Information, Information Technologies and Information Protection", "On the Security of Critical Information Infrastructure of the Russian Federation", "About personal data" and by-laws), official methodological documents of regulators (FSTEC, FSB, Roskomnadzor), clarifications of the supreme courts on digital evidence, as well as open government statistical arrays and reports from industry response centers. Foreign regulatory models (at the level of strategies and framework acts) and international initiatives (UN, regional formats) were used for comparison. Formal-legal, comparative-legal and system-structural methods are applied; the method of legal policy and risk-oriented regulation; analysis of norms and law enforcement practice (2019-2025); elements of a case study on incidents in the CII. The conclusions were verified through a cross-comparison of regulatory requirements, surveillance practices, and available statistical series.

Results. An integrated model of legal support for cybersecurity as a subsystem of national security, comprising four blocks, has been obtained.

1) Doctrinal and conceptual: it is proposed to establish the definitions of "cybersecurity", "cyber resilience", "cyberattack", to unify terminology through targeted amendments to federal laws "On Information, Information Technologies and Information Protection", "On the security of critical information infrastructure of the Russian Federation", as well as to approve a separate Cybersecurity Strategy of the Russian Federation with a taxonomy of risks and response levels.

2) Institutional: the creation of a national coordinator (interdepartmental body) with a mandate for incident management, a network of industry-specific CSIRT and a single window for notifications is justified; the obligation of significant operators to report significant incidents to the regulator within a specified period with the protection of fair disclosure (safe harbor) is introduced.

3) Regulatory: a framework law on cybersecurity has been proposed, which establishes minimum baseline controls, profiles by CI sector, risk-graded supervisory impact, and mechanisms for encouraging independent audits and bug bounties.

4) Criminal, including criminal procedure, and international: the rules for handling digital evidence are being clarified, the composition of cybersabage in relation to CII is being introduced, the procedural possibilities for cross-border e-evidence are being expanded; the implementation of international instruments and the prioritization of cooperation in friendly regional formats are provided.

A separate block on technological sovereignty is proposed: phased procurement preferences, secure-by-design and lifecycle requirements, MTTD/MTTR metrics, and readiness audit.
Discussion and Conclusion. The proposed architecture addresses core deficiencies of the current regime—conceptual uncertainty, regulatory fragmentation, and weak incident coordination. A risk-based model reduces compliance costs through proportionality and supervisory predictability, while safe-harbor rules and public-private partnership improve vulnerability disclosure quality. Rights safeguards remain essential: judicial oversight for access to encrypted data, due-process protections for e-evidence, regulator transparency, and independent audits. Implementation should proceed in phases (pilots in CII sectors followed by scale-up), guided by clear metrics (MTTD/MTTR, share of incidents restored within target SLAs, CSIRT coverage), periodic review every 2-3 years, and synchronization with import-independence programs. The result is stronger national cyber-resilience and reduced systemic risk to security, the economy, and individual rights, providing Russia with a coherent legal toolkit compatible with international cooperation and technological-sovereignty objectives.

Keywords: cybersecurity, national security, information security, information law, cybercrime, critical information infrastructure

Conflict of interests: The authors declare no conflict of interest.

For citation: Bogdanov E.A., Kogteva A.N., Tanchuk R.S. Cybersecurity as a Component of National Security: Theoretical and Applied Aspects. *Modern Information Technologies and IT-Education.* 2026;22(1):28-39. https://doi.org/10.25559/SITITO.022.202601.28-39

Введение

Кибербезопасность доктринально рассматривается как один из ключевых факторов национальной безопасности: устойчивость цифрового государства, непрерывность КИИ и защита прав граждан в онлайн-среде зависят от качества правового регулирования и эффективности институциональной координации [1, 2]. Российская правовая модель исторически развивалась вокруг более широкого концепта информационной безопасности, что обеспечило стратегические рамки, но не нивелировало необходимость формализации кибербезопасности как самостоятельного правового института со своим понятийным аппаратом, инструментами реагирования и проверяемыми показателями результативности[1] [3].

Стремительная цифровизация государственного управления, экономики и социальной сферы породила сложные трансграничные киберугрозы, тогда как правовой ответ остаётся фрагментарным и концептуально неопределённым. В российском праве не закреплены легальные определения ключевых категорий кибербезопасности, отсутствует самостоятельная национальная стратегия и уполномоченный координатор с полномочиями межведомственного управления инцидентами, а регуляторные требования к операторам КИИ неоднородны, что затрудняет соблюдение и надзор.

Практики обмена данными об инцидентах между государством и бизнесом носит точечный характер и не обеспечена режимом «безопасной гавани» для добросовестного раскрытия, правоприменение сталкивается с пробелами в обращении с цифровыми доказательствами и в трансграничном получении электронных данных, а ведомственная статистика инцидентов и преступлений остаётся несопоставимой. Зависимость отдельных сегментов КИИ от зарубежных технологий усиливает системный риск, осложняя управление уязвимостями и обеспечение непрерывности.

В результате складывается ситуация, когда отсутствие согласованной правовой архитектуры снижает устойчивость государства к кибервоздействиям и повышает издержки для экономики и граждан. Для преодоления этого разрыва требуется модель, способная объединить доктрину, нормы и организационные аспекты в единую, измеримую и предсказуемую систему, совместимую с международной кооперацией и целями технологического суверенитета.

Цель исследования: проанализировать теоретические и прикладные аспекты обеспечения кибербезопасности в Российской Федерации, выявить актуальные проблемы правового обеспечения кибербезопасности и предложить пути их разрешения.

Материалы и методы

Понятие кибербезопасности в российской доктрине и законодательстве сформировалось относительно недавно и до сих пор окончательно не институционализировано. В отличие от зарубежных стран, где еще в начале 2000-х гг. были приняты национальные стратегии кибербезопасности, в Российской Федерации долгое время превалировало понятие «информационная безопасность», охватывающее как техническую защиту информации, так и защиту от угроз в информационной сфере (идеологические воздействия и пр.).

Термин «кибербезопасность» отсутствовал в российских законах вплоть до второй половины 2010-х годов и вызывал сопротивление регуляторов, опасавшихся, что его официальное признание потребует радикального пересмотра нормативной базы и разработки новых стандартов [4, С. 61]. Лишь с 2016-2017 гг. понятие стало употребляться на корпоративном и ведомственном уровнях, однако законодательно до сих пор не закреплено четкое определение кибербезопасности [5-9].

Согласно экспертным оценкам, российские регуляторы исторически рассматривали кибербезопасность как часть широкой системы информационной безопасности, что повлияло на правовой статус и регулирование данной сферы. Тем не менее, изменение характера угроз и международные тенденции вынуждают переосмыслить место кибербезопасности в системе национальной безопасности. Президентом РФ в 2021 г. утверждены Основы государственной политики в области международной информационной безопасности[2], акцентирующие защиту национальных интересов в цифровой сфере. Это свидетельствует о возросшей роли кибербезопасности в стратегическом планировании безопасности государства.

Таким образом, на теоретическом уровне происходит постепенный переход от узкого понимания кибербезопасности как технической задачи к ее признанию в качестве комплексного правового института, необходимого для суверенитета и устойчивого развития страны в цифровую эпоху [10-13].

Правовой фундамент обеспечения кибербезопасности в Российской Федерации состоит из совокупности нормативных актов разного уровня. Базовыми являются стратегические документы: Доктрина информационной безопасности РФ[3] и Стратегия национальной безопасности РФ[4], которые закрепляют приоритеты противодействия киберугрозам и защиты информационного суверенитета.

Доктрины действуют на основе федеральных законов, определяющих обязанности субъектов в цифровой сфере. К ключевым актам относятся: федеральный закон «О безопасности критической информационной инфраструктуры РФ»[5], устанавливающий требования по защите значимых объектов КИИ; поправки 2019 г. в закон «Об информации, информационных

[1] Дубень А. К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации: дис. … канд. юрид. наук. М., 2023. С. 4. EDN: QABIHE

[2] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента РФ от 12.04.2021 № 213 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_381999/ (дата обращения: 11.02.2026).

[3] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения: 11.02.2026).

[4] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400 [Электронный ресурс]. С. 246. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 11.02.2026).

[5] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26.07.2017, № 187-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 11.02.2026).

технологиях и о защите информации»[6] (т.н. закон о «суверенном Рунете»), давшие государству механизмы централизованного управления российским сегментом интернета (так называемый «пакет Яровой»)[7], обязавший организаторов связи хранить трафик и передавать ключи шифрования спецслужбам; закон о локализации персональных данных[8] (внесены изменения в федеральный закон «О персональных данных»)[9] и последующее ужесточение ответственности ИТ-компаний за невыполнение требований локализации и модерации контента (федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[10] усилил санкции).

Кроме того, приняты подзаконные акты, регламентирующие функционирование государственной системы обнаружения и предотвращения кибератак (ГосСОПКА) и создание Центра реагирования на компьютерные инциденты. Формируется институциональная структура: функции по обеспечению кибербезопасности распределены между ФСБ (техническая защита и контрразведка), ФСТЭК (защита информационных систем), МВД (расследование киберпреступлений), Роскомнадзором (контроль за соблюдением законов об информации и персональных данных) и профильными подразделениями других органов.

Несмотря на наличие значительного массива нормативных актов, в научной литературе отмечается фрагментарность и недостаточная системность правового регулирования [14, С. 260-261]. Не принят единый закон о кибербезопасности или полноценная стратегия кибербезопасности, которая бы охватила все аспекты – от профилактики инцидентов до реагирования и восстановления.

Терминологический аппарат также остается несогласованным: законодательно не определены ключевые понятия вроде «кибератака», «киберустойчивость», отсутствует разграничение между кибербезопасностью и информационной безопасностью [4, С. 65]. Все это затрудняет правоприменение и межведомственную координацию.

Таким образом, основной проблемой на нормативном уровне является необходимость унификации и обновления законодательства с учетом современных реалий. Требуется закрепить понятие кибербезопасности и внести изменения в профильные законы, устранив коллизии и пробелы. Прежде всего, целесообразно на законодательном уровне отразить обязанности органов власти по обеспечению устойчивости критических систем, порядок обмена данными об инцидентах и основания для введения режимов кибербезопасности в кризисных ситуациях.

Актуальность предложенного обосновывается тем, что последние годы характеризуются взрывным ростом киберпреступности и усложнением профильных угроз. Это непосредственно отражается на национальной безопасности. Статистические данные свидетельствуют, что за пять лет число регистрируемых киберпреступлений в Российской Федерации увеличилось в 2,3 раза – с ~294 тысяч случаев в 2019 г. до ~677 тысяч в 2024 г. При этом доля киберпреступлений достигла 35% от всех зарегистрированных преступлений по итогам 2023 г. (против 26,5% годом ранее), то есть каждый третий преступный посягатель сегодня совершается с использованием информационно-коммуникационных технологий[11]. Наиболее массовыми остаются преступления против собственности – хищения средств путем онлайн-мошенничества, краж с банковских счетов и пр. – однако стремительно растет число иных, ранее редких посягательств.

В 2023 г. зафиксирована качественно новая тенденция: значительное увеличение количества кибератак деструктивного характера, нацеленных на выведение из строя информационных систем, а не только на получение выгоды или распространение информации. По данным профильных органов, в 2023 г. было отражено свыше 65 тысяч кибератак на объекты критической информационной инфраструктуры (государственные информационные системы, сети в секторах здравоохранения, транспорта, связи, энергетики, финансов и др.)[12]. Эти цифры многократно превышают показатели предыдущих лет и связаны, в частности, с обострением геополитической обстановки: фактически киберпространство стало ареной международного противоборства, что подтвердили события 2022-2023 гг.

Кроме целенаправленных атак на инфраструктуру, серьезную угрозу представляет утечка и незаконная торговля персональными данными граждан. В 2023 г. в открытом доступе оказа-

[6] О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : федер. закон от 01.05.2019, № 90-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_323815/ (дата обращения: 11.02.2026).

[7] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федер. закон от 06.07.2016, № 374-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_201078/ (дата обращения: 11.02.2026); О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федер. закон от 06.07.2016, № 375-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_201087/ (дата обращения: 11.02.2026).

[8] О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях : федер. закон от 21.07.2014, № 242-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_165838/ (дата обращения: 11.02.2026).

[9] О персональных данных : федер. закон от 27.07.2006, № 152-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 11.02.2026).

[10] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : федер. закон от 30.12.2020, № 511-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_372707/ (дата обращения: 11.02.2026).

[11] Основные статистические показатели состояния судимости в России за 2003-2024 годы [Электронный ресурс] // Судебный департамент при Верховном Суде Российской Федерации, 2026. URL: https://cdep.ru/index.php?id=79&item=2074 (дата обращения: 11.02.2026).

[12] Козин Н. Количество киберпреступлений в России выросло в 2,3 раза за пять лет [Электронный ресурс] // Парламентская газета. 16.04.2024. URL: https://www.pnp.ru/social/kolichestvo-kiberprestupleniy-v-rossii-vyroslo-v-23-raza-za-pyat-let.html (дата обращения: 11.02.2026).

лось свыше 510 млн записей о персональных данных россиян вследствие ряда крупных утечек (для сравнения, в 2022 г. – около 150 крупных утечек)[13]. Утечки затрагивали в том числе данные из государственных информационных систем и коммерческих сервисов, что говорит о недостаточной защищенности систем и о неисполнении организациями требований закона о персональных данных.

Таким образом, новые вызовы включают: кибершпионаж и диверсии против критически важных объектов, массовые нарушения конфиденциальности информации, распространение вредоносных программ (в т.ч. вымогателей), атаки на цепочки поставок программного обеспечения.

Рост угроз выявил ряд проблем правоприменения. Во-первых, правоохранительная система испытывает объективные сложности в раскрытии и расследовании киберпреступлений, многие из которых совершаются анонимно и транснационально[14] [15-17]. Согласно официальным данным, лишь около четверти возбужденных уголовных дел о киберпреступлениях доводится до суда[15]. Низкая раскрываемость означает и крайне низкий уровень возмещения ущерба потерпевшим – возвращается порядка 7,5% похищенных средств[16]. Основные препятствия – недостаток квалифицированных кадров и технической оснащенности у органов следствия на местах, юрисдикционные трудности (многие атаки исходят из-за рубежа), сложности в собирании доказательственной базы [18]. Несмотря на требования «пакета Яровой» об обязательном хранении сервисами связи данных о передаваемых сообщениях, на практике эти массивы данных не всегда доступны либо недостаточно полны для идентификации злоумышленников. При этом, объем и формат сохраняемых операторами и интернет-платформами данных не в полной мере соответствуют потребностям следствия.

Во-вторых, имеет место коллизия между правом на тайну связи/частную жизнь и потребностями оперативно-розыскных мероприятий: правоприменители указывают на необходимость расширения доступа к зашифрованным сообщениям, однако баланс с конституционными правами пока не найден в законе [19, С. 68].

В-третьих, организационная разобщенность – несмотря на создание отраслевых центров реагирования (CERT) и межведомственных комиссий, отсутствует единый координирующий орган по кибербезопасности на национальном уровне, что замедляет реагирование на крупные инциденты.

Сфера кибербезопасности по своей природе трансгранична, поэтому для ее обеспечения необходимо международное сотрудничество. Российская Федерация традиционно выступает сторонником разработки универсальных норм и правил поведения государств в информационном пространстве. Начиная с 1998 г., российская дипломатия продвигает идею международной конвенции по кибербезопасности (в терминологии – «обеспечение международной информационной безопасности»). В 2021-2023 гг. Российская Федерация активизировала усилия на площадке ООН: в рамках Открытой рабочей группы ООН (OEWG) в июне 2023 г. был внесен очередной проект конвенции об обеспечении международной информационной безопасности[17]. Хотя этот документ не был поддержан большинством стран и не попал в итоговый отчет OEWG, его появление подтверждает намерение Российской Федерации продвигать собственную повестку в киберпространстве.

Российские проекты часто содержат положения, отражающие национальные интересы (например, идею государственного суверенитета в сегментах интернета и недопустимость использования кибертехнологий для вмешательства во внутренние дела)[18]. Параллельно Российская Федерация добилась успеха на другом треке – в декабре 2024 г. Генеральная Ассамблея ООН приняла согласованный текст Международной конвенции о противодействии киберпреступности, сопредседателем разработки которого выступала Российская Федерация[19]. Этот новый глобальный договор отражает в значительной мере подходы, близкие для российской стороны, делая упор на суверенные права государств и сотрудничество в пресечении преступлений в сфере ИКТ.

В условиях санкционного давления и сокращения двустороннего взаимодействия с западными странами, Российская Федерация усиливает координацию в рамках СНГ, ОДКБ, ШОС. Заключены соглашения СНГ о сотрудничестве в борьбе с киберпреступностью (2018), действуют двусторонние договоры с рядом государств о взаимной помощи в расследованиях.

Тем не менее, разногласия на уровне международного права сохраняются: отсутствует консенсус по применению международного гуманитарного права к киберконфликтам (Российская Федерация недавно поставила под сомнение автоматическое применение норм МГП в киберпространстве), а также по вопросам атрибуции кибератак и меры самообороны в ответ на них[20].

Развитие международно-правовых механизмов идет медленно, поэтому в ближайшей перспективе важную роль будет играть региональное сотрудничество и обмен информацией

---

[13] Там же.

[14] Сустина Т. И. Правовое обеспечение информационной безопасности несовершеннолетних в условиях цифровой трансформации общества : дис… канд. юрид. наук. М.: ИГП РАН, 2023. С. 5.

[15] Козин Н. Количество киберпреступлений в России выросло в 2,3 раза за пять лет [Электронный ресурс] // Парламентская газета. 16.04.2024. URL: https://www.pnp.ru/social/kolichestvo-kiberprestupleniy-v-rossii-vyroslo-v-23-raza-za-pyat-let.html (дата обращения: 11.02.2026).

[16] Там же.

[17] Convention on Cybercrime (Budapest Convention) [Электронный ресурс] // Council of Europe. 23.11.2001. European Treaty Series – No. 185. URL: https://rm.coe.int/1680081561 (дата обращения: 11.02.2026).

[18] Kajander A. Russia's Latest Attempt at a New UN Convention on Cyberspace // NATO CCDCOE Law Brief. 2023. No. 8. P. 1-5 [Электронный ресурс]. URL: https://ccdcoe.org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf (дата обращения: 11.02.2026).

[19] Яникеева И. О. Фактор международной информационной безопасности в двусторонних отношениях России и США в XXI веке: дис… канд. полит. наук. М.: РУДН, 2023. 269 с. EDN: RYKTIM

[20] Kajander A. Russia's Latest Attempt at a New UN Convention on Cyberspace // NATO CCDCOE Law Brief. 2023. No. 8. P. 1-5 [Электронный ресурс]. URL: https://ccdcoe.org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf (дата обращения: 11.02.2026).

между компетентными органами дружественных стран. Кроме того, кибербезопасность становится неотъемлемой частью двусторонних отношений – например, в формате Российская Федерация – Китайская Народная Республика закреплено сотрудничество по вопросам «информационной безопасности», включая технологическую независимость.

Таким образом, для эффективного обеспечения национальной кибербезопасности Российской Федерации необходимо одновременно совершенствовать внутреннее законодательство и активно участвовать в формировании новых международных режимов, учитывающих национальные интересы.

Проведенный анализ позволяет выделить ряд первоочередных мер для укрепления кибербезопасности как компонента национальной безопасности.

1) **Закрепление понятий и стратегии.** Требуется на законодательном уровне дать официальное определение термину «кибербезопасность» и смежным категориям. Это позволит устранить разночтения и согласовать терминологию в нормативных актах.

Целесообразна разработка и принятие отдельной Стратегии кибербезопасности Российской Федерации, согласованной с действующей Стратегией национальной безопасности, а также конкретизация положений Доктрины информационной безопасности. Такая стратегия должна четко определить цели, объекты защиты, угрозы и принципы государственного реагирования в киберпространстве, а также распределить ответственность между органами власти.

2) **Комплексный закон о кибербезопасности**. Представляется целесообразным принять единый рамочный закон, устанавливающий основы обеспечения кибербезопасности. В нем можно объединить нормы, сейчас разбросанные по разным актам: об обязанности субъектов КИИ внедрять средства защиты, о порядках обмена информацией об инцидентах между госорганами и частным сектором, о режимах реагирования на кибератаки на национальном уровне, о стимулировании импортозамещения критичных технологий и др. Такой закон мог бы также определить статус уполномоченного органа в сфере кибербезопасности.

3) **Совершенствование уголовного законодательства.** Необходимо дальнейшее обновление УК РФ и УПК РФ с учетом специфики киберпреступлений. В декабре 2022 г. Пленум Верховного Суда РФ издал постановление[21], где разъяснил особенности квалификации киберпреступлений (например, разграничил уголовную ответственность за неправомерный доступ и за атаки типа DDoS). Однако, возможно, потребуются новые составы преступлений, учитывающие современные посягательства: кибершпионаж, несанкционированное вмешательство в функционирование критических систем (саботаж), создание и распространение вредоносных кодов и др. Следует пересмотреть санкции за киберпреступления с высокой общественной опасностью (атаки на объекты жизнеобеспечения, военные системы) – вплоть до ужесточения ответственности.

4) **Укрепление механизмов расследования и международной кооперации.** Для повышения раскрываемости киберпреступлений необходимо наделить правоохранительные органы современными инструментами. Рекомендуется расширить полномочия следственных органов по получению цифровых доказательств, в том числе путем более тесного взаимодействия с частными ИТ-компаниями. Можно рассмотреть вопрос об увеличении сроков хранения данных операторами связи или о создании государственной системы логирования критических событий в киберпространстве. Важно ускорить имплементацию новой Конвенции ООН против киберпреступности и заключение двусторонних соглашений об экстрадиции киберпреступников, обмене информацией и совместных расследованиях. Учитывая геополитические ограничения, акцент следует сделать на сотрудничестве в рамках СНГ, ШОС, БРИКС.

5) **Организационно-правовые меры.** Предлагается создать единый координационный центр (межведомственный орган) по кибербезопасности при Совете Безопасности Российской Федерации, который бы отвечал за реализацию государственной политики, мониторинг угроз и координацию действий всех субъектов (силовых структур, регуляторов, частных компаний). Необходимо продолжить развитие системы ГосСОПКА, охватив ею максимальное число объектов КИИ, и внедрить централизованную систему оповещения о киберинцидентах [14]. Также следует совершенствовать механизмы публично-частного партнерства: стимулировать обмен информацией о кибератаках между бизнесом и государством, вводить требования к частным предприятиям по минимальным стандартам киберзащиты. В образовательной сфере нужна подготовка кадров – расширение специализаций по кибербезопасности в вузах, обучение судей и следователей особенностям киберпреступлений, проведение регулярных учений и тренингов (как на национальном уровне, так и совместно с партнерами по ОДКБ/СНГ) [20, 21].

6) **Обеспечение технологического суверенитета.** Как показали последние события, наличие критической зависимости от зарубежных ИКТ-продуктов создает уязвимости для национальной безопасности. Поэтому важным направлением является поддержка отечественной индустрии кибербезопасности, импортозамещение в сегменте программного обеспечения и оборудования для ключевых систем [22], [23,] [24, С. 650]. Законодательные меры (например, требование 2025 г. о переходе значимых объектов КИИ на российское ПО) уже принимаются, но их реализация требует контроля и стимулирования инноваций. Правовые условия для трансфера технологий, налоговые льготы для разработчиков защитных решений – все это должно стать частью политики кибербезопасности.

Реализация перечисленных мер позволит повысить уровень готовности государства к отражению кибератак и минимизировать ущерб от них. Как отмечается в научных исследованиях, эффективность национальной кибербезопасности зависит не только от технологических факторов, но и от политико-правовой среды: в государствах с проактивной и согласованной

[21] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022, № 37 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 11.02.2026).

киберполитикой наблюдается меньшая уязвимость к киберугрозам [25, С. 1183]. В этом смысле предложенные изменения в российском законодательстве и управлении послужат укреплению общей системы национальной безопасности.

Результаты исследования

Кибербезопасность в настоящее время выступает неотъемлемой составляющей национальной безопасности, влияя на все ключевые сферы – оборону, экономику, общественный порядок. Проведенный анализ показал, что в Российской Федерации формируется собственная модель обеспечения кибербезопасности, базирующаяся на концепции цифрового суверенитета и интеграции кибербезопасности в широкое понятие информационной безопасности.

С одной стороны, достигнут заметный прогресс: создана правовая основа защиты критической информационной инфраструктуры, внедряются национальные технологии киберзащиты, Российская Федерация активно продвигает на международной арене инициативы по регулированию поведения государств в киберпространстве.

С другой стороны, исследование выявило ряд острых проблем. К ним относятся: отсутствие единообразия в терминологии и комплексной стратегии кибербезопасности; фрагментарность нормативной базы и пробелы, не позволяющие в полной мере пресекать новые виды киберпосягательств; недостаточная эффективность правоохранительной практики, выражающаяся в низкой раскрываемости киберпреступлений и трудностях доказывания; организационные сложности координации и дефицит кадровых ресурсов. Рост кибератак в последние годы, в том числе на фоне обострения международной обстановки, подтвердил необходимость срочного решения этих проблем.

В работе предложены конкретные направления совершенствования законодательства и правоприменения, обладающие научной новизной и практической значимостью. В их числе – законодательное закрепление понятия кибербезопасности и принятие Стратегии кибербезопасности; разработка рамочного закона, консолидирующего основы обеспечения безопасности в киберпространстве; обновление уголовного законодательства с учетом новых угроз; укрепление механизмов расследования с упором на международное сотрудничество и реализацию новой глобальной конвенции о киберпреступности; создание единого координационного органа по кибербезопасности и развитие системы обмена информацией об инцидентах; меры по поддержке отечественных технологий и обеспечению цифрового суверенитета. Реализация этих мер позволит сформировать целостную систему правового и организационного обеспечения кибербезопасности, адекватную вызовам современной цифровой эпохи.

Обсуждение и заключение

Кибербезопасность как компонент национальной безопасности требует постоянного развития правовых доктрин и механизмов. Балансируя между защитой от киберугроз и соблюдением прав граждан, государство должно выработать гибкий и опережающий подход. От эффективности предпринимаемых шагов во многом зависит способность Российской Федерации противостоять киберинцидентам, обеспечивая устойчивое развитие и безопасность в информационном обществе. Дальнейшие исследования в данной области могут быть направлены на мониторинг реализации предлагаемых мер и оценку их влияния на уровень защищенности страны в киберпространстве.

Список использованных источников

[1] Sokolova M., Chislova O. Cybersecurity in Russia // International Cybersecurity Law Review. 2021. Vol. 2, issue 2. P. 245-251. https://doi.org/10.1365/s43439-021-00032-9
[2] Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 383-390. https://doi.org/10.25559/SITITO.18.202202.383-390
[3] Троян Н. А. Правовое обеспечение цифрового суверенитета России: актуальные проблемы и перспективные направления // Право и государство: теория и практика. 2024. № 6(234). С. 169-172. https://doi.org/10.47643/1815-1337_2024_6_169
[4] Добродеев А. Ю. Кибербезопасность в Российской Федерации: модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2021. № 4(44). С. 61-72. https://doi.org/10.21681/2311-3456-2021-4-61-72
[5] Язов Ю. К. Об определении понятия «кибербезопасность» и связанных с ним терминов // Вопросы кибербезопасности. 2025. № 1(65). С. 2-6. https://doi.org/10.21681/2311-3456-2025-1-2-6
[6] Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1(47). С. 2-9. https://doi.org/10.21681/2311-3456-2022-1-2-9
[7] Möller D. P. F. Introduction to Cybersecurity // Cybersecurity in Digital Transformation. SpringerBriefs on Cyber Security Systems and Networks. Cham: Springer, 2020. P. 11-27. https://doi.org/10.1007/978-3-030-60570-4_2
[8] Starodubtsev Y. I., Balenko E. G., Vershennik E. V., Fedorov V. H. Cyberspace: Terminology, Properties, Problems of Operation // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). Vladivostok, Russia: IEEE Press, 2020. P. 1-3. https://doi.org/10.1109/FarEastCon50210.2020.9271282
[9] Буряков В. М. Цифровая эпоха как императив смены старой парадигмы информационной безопасности России // Защита информации. Инсайд. 2024. № 2(116). С. 4-11. EDN: UUBLNC
[10] Баландин А. Ю. Особенности правового регулирования кибербезопасности в эпоху глобального противостояния // Правовая информатика. 2025. № 1. С. 50-56. https://doi.org/10.24412/1994-1404-2025-1-50-56
[11] Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Развитие доктрины российского информационного права в условиях перехода к экономике данных // Государство и право. 2023. № 9. С. 158-171. https://doi.org/10.31857/S102694520027660-7

[12] Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3(31). С. 18-23. https://doi.org/10.21681/2311-3456-2019-3-18-23

[13] Прокопьев И. В. Анализ действующей правовой системы Российской Федерации в сфере киберправа и кибербезопасности // Вестник Академии права и управления. 2025. № 5(86). С. 86-93. https://doi.org/10.47629/2074-9201_2025_5_86_93

[14] Серебренникова А. В. Правовые основы кибербезопасности в Российской Федерации // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 260-265. https://doi.org/10.33693/2072-3164-2021-14-4-260-265

[15] Каменец А. В. Проблемы расследования преступлений в сфере информационной безопасности // Закон и право. 2025. № 1. С. 70-73. https://doi.org/10.24412/2073-3313-2025-1-70-73

[16] Поздышев Р. С. Вопросы квалификации преступлений в сфере компьютерной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1(61). С. 105-112. https://doi.org/10.36511/2078-5356-2023-1-105-112

[17] Кайгородова О. С. Нормативно-правовое обеспечение кибербезопасности: защищены ли мы? // Правопорядок: история, теория, практика. 2023. № 4(39). С. 155-161. https://doi.org/10.47475/2311-696X-2023-39-4-155-161

[18] Shcherbovich A. Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia // CyberBRICS ; ed. by L. Belli. Cham: Springer, 2021. P. 67-131. https://doi.org/10.1007/978-3-030-56405-6_3

[19] Лепешкина О. И. Киберпреступность как угроза национальной безопасности России // Теоретическая и прикладная юриспруденция. 2022. № 2(12). С. 65-69. https://doi.org/10.22394/2686-7834-2022-2-65-69

[20] Северин В. А. Комплексный подход подготовки кадров для обеспечения кибербезопасности: вызовы и проблемы // Лоббирование в законодательстве. 2023. Т. 2, № 2. С. 16-20. https://doi.org/10.33693/2782-7372-2023-22-16-20

[21] Царегородцев А. В., Малюк А. А., Волков С.Д. Современные вызовы системе подготовки кадров в области информационной безопасности // Информационное общество. 2025. № 2. С. 119-130. https://doi.org/10.52605/16059921_2025_02_119

[22] Смыслова О. Ю., Леонов М. А. Импортозамещение программного обеспечения в Российской Федерации: анализ законодательства, рыночной динамики и конкурентоспособности отечественных решений в условиях санкционного давления // Экономика, предпринимательство и право. 2025. Т. 15, № 6. С. 3933-3952. https://doi.org/10.18334/epp.15.6.123328

[23] Березнев С. В., Кульпина Е. Е. Импортозамещение как ключевой фактор укрепления суверенитета и экономической безопасности современной России // Научные труды Вольного экономического общества России. 2022. Т. 237, № 5. С. 58-80. https://doi.org/10.38197/2072-2060-2022-237-5-58-80

[24] Kolodii R. Unpacking Russia's Cyber-Incident Response // Security Studies. 2024. Vol. 33, issue 4. P. 640-669. https://doi.org/10.1080/09636412.2024.2391757

[25] Kleiner J. How political regimes affect national cybersecurity: the polity flux effect // Democratization. 2025. Vol. 32, issue 5. P. 1181-1212. https://doi.org/10.1080/13510347.2025.2451951

Поступила 14.01.2026; одобрена после рецензирования 04.03.2026; принята к публикации 02.04.2026.

Об авторах:

Богданов Евгений Александрович, заведующий кафедрой информационной безопасности Факультета информационных технологий и анализа больших данных, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2), PhD (Doctor of Philosophy), **ORCID: https://orcid.org/0009-0007-2973-6248,** eabogdanov@fa.ru

Когтева Анна Николаевна, доцент кафедры информационной безопасности Факультета информационных технологий и анализа больших данных, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2), кандидат экономических наук, **ORCID: https://orcid.org/0000-0001-8109-9900,** annelya1@yandex.ru

Танчук Роман Сергеевич, заместитель декана по связям с российскими и международными партнерами Факультета информационных технологий и анализа больших данных, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2), кандидат экономических наук, доцент, **ORCID: https://orcid.org/0000-0003-3998-1080,** rstanchuk@fa.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Sokolova M., Chislova O. Cybersecurity in Russia. *International Cybersecurity Law Review.* 2021;2(2):245-251. https://doi.org/10.1365/s43439-021-00032-9

[2] Lebed S.V. Innovative Technologies in Cybersecurity. *Modern Information Technologies and IT-Education*. 2022; 18(2):383-390. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.18.202202.383-390

[3] Troyan N.A. Legal Support of Russia's Digital Sovereignty: Current Problems and Promising Directions. *Law and State: The Theory and Practice.* 2024;(6):169-172. (In Russ., abstract in Eng.) https://doi.org/10.47643/1815-1337_2024_6_169

[4] Dobrodeev A.Yu. Cybersecurity in Russian Federation. A Trendy Term or the Priority Technologic Area of Enhancing National and International Security of the XXI Century. *Cybersecurity issues.* 2021;(4):61-72. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2021-4-61-72
[5] Yazov Yu.K. Cybersecurity Terms and Definitions. *Cybersecurity issues.* 2025;(1):2-6. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2025-1-2-6
[6] Markov A.S. Cybersecurity and Information Security as Nomenclature Bifurcation Scientific Specialties. *Cybersecurity issues.* 2022;(1):2-9. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2022-1-2-9
[7] Möller D.P.F. Introduction to Cybersecurity. In: Cybersecurity in Digital Transformation. *SpringerBriefs on Cyber Security Systems and Networks.* Cham: Springer; 2020. p. 11-27. https://doi.org/10.1007/978-3-030-60570-4_2
[8] Starodubtsev Y.I., Balenko E.G., Vershennik E.V., Fedorov V.H. Cyberspace: Terminology, Properties, Problems of Operation. In: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). Vladivostok, Russia: IEEE Press; 2020. p. 1-3. https://doi.org/10.1109/FarEastCon50210.2020.9271282
[9] Buryakov V.M. The Digital Age as an Imperative to Change the Current Paradigm of Russian Information Security. *Zaŝita informacii. Inside.* 2024;(2):4-11. (In Russ., abstract in Eng.) EDN: UUBLNC
[10] Balandin A.Yu. Specific Features of Legal Regulation of Cybersecurity in the Times of Global Confrontation. *Legal information.* 2025;(1):50-56. (In Russ., abstract in Eng.) https://doi.org/10.24412/1994-1404-2025-1-50-56
[11] Polyakova T.A., Minbaleev A.V., Krotkova N.V. Development of the Doctrine of Russian Information Law in the Context of the Transition to a Data Economy. *State and Law.* 2023;(9):158-171. (In Russ., abstract in Eng.) https://doi.org/10.31857/S102694520027660-7
[12] Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Modern trends of cyber-threats and transformation of the concept of cybersecurity in the conditions of digitalization of the system of law. *Cybersecurity issues.* 2019;(3):18-23. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2019-3-18-23
[13] Prokopiev I.V. Analysis of the current legal system of the Russian Federation in the field of cyber law and cybersecurity. *Bulletin of the Academy of Law and Management*. 2025;(5):86-93. (In Russ., abstract in Eng.) https://doi.org/10.47629/2074-9201_2025_5_86_93
[14] Serebrennikova A.V. The Legal Framework for Cybersecurity in the Russian Federation. *Gaps in Russian Legislation.* 2021;14(4):260-265. (In Russ., abstract in Eng.) https://doi.org/10.33693/2072-3164-2021-14-4-260-265
[15] Kamenets A.V. Problems of investigation of crimes in the sphere of information security. *Law and legislation*. 2025;(1):70-73. (In Russ., abstract in Eng.) https://doi.org/10.24412/2073-3313-2025-1-70-73
[16] Pozdyshev R.S. Issues of qualification of crimes in the sphere of computer information. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.* 2023;(1):105-112. (In Russ., abstract in Eng.) https://doi.org/10.36511/2078-5356-2023-1-105-112
[17] Kaigorodova O.S. Regulatory and legal support of cybersecurity: are we protected? *Pravoporyadok: istoriya, teoriya, praktika* = Legal and Order: History, Theory, Practice. 2023;(4):155-161. (In Russ., abstract in Eng.) https://doi.org/10.47475/2311-696X-2023-39-4-155-161
[18] Shcherbovich A. Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia. In: Belli L. (ed.) CyberBRICS. Cham: Springer; 2021. p. 67-131. https://doi.org/10.1007/978-3-030-56405-6_3
[19] Lepeshkina O.I. Cybercrime as Threat of National Security of Russia. *Theoretical and Applied Law.* 2022;(2):65-69. (In Russ., abstract in Eng.) https://doi.org/10.22394/2686-7834-2022-2-65-69
[20] Severin V.A. Integrated Approach of Personnel Training for Cybersecurity: Challenges and Problems. Lobbying *in the Legislative Process.* 2023;2(2):16-20. (In Russ., abstract in Eng.) https://doi.org/10.33693/2782-7372-2023-2-2-16-20
[21] Tsaregorodtsev A.V., Malyuk A.A., Volkov S.D. Modern Challenges to the Personnel Training System in the Field of Information Security. *Information Society.* 2025;(2):119-130. (In Russ., abstract in Eng.) https://doi.org/10.52605/16059921_2025_02_119
[22] Smyslova O.Y., Leonov M.A. Software import substitution in the Russian Federation: analysis of legislation, market dynamics and competitiveness of domestic solutions under sanctions pressure. *Journal of Economics, Entrepreneurship and Law.* 2025;15(6):3933-3952. (In Russ., abstract in Eng.) https://doi.org/10.18334/epp.15.6.123328
[23] Bereznev S.V., Kul'pina E.E. Import substitution as a key factorin strengthening the sovereigntyand economic security of modern Russia. *The Proceedings of the Free Economic Society of Russia.* 2022;237(5):58-80. In Russ., abstract in Eng.) https://doi.org/10.38197/2072-2060-2022-237-5-58-80
[24] Kolodii R. Unpacking Russia's Cyber-Incident Response. *Security Studies.* 2024;33(4):640-669. https://doi.org/10.1080/09636412.2024.2391757
[25] Kleiner J. How political regimes affect national cybersecurity: the polity flux effect. *Democratization.* 2025;32(5):1181-1212. https://doi.org/10.1080/13510347.2025.2451951

Submitted 14.01.2026; approved after reviewing 04.03.2026; accepted for publication 02.04.2026.

About the authors:
Evgenii A. Bogdanov, Head of the Department of Information Security at the Faculty of Information Technologies and Big Data Analysis, Financial University under the Government of the Russian Federation (49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation), PhD (Doctor of Philosophy), **ORCID: https://orcid.org/0009-0007-2973-6248,** eabogdanov@fa.ru

Anna N. Kogteva, Associate Professor of the Department of Information Security at the Faculty of Information Technologies and Big Data Analysis, Financial University under the Government of the Russian Federation (49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation), Cand. Sci. (Econ.), **ORCID: https://orcid.org/0000-0001-8109-9900,** annelya1@yandex.ru
Roman S. Tanchuk, Deputy Dean for Relations with Russian and International Partners, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation (49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation), Cand. Sci. (Econ.), Associate Professor, **ORCID: https://orcid.org/0000-0003-3998-1080,** rstanchuk@fa.ru

All authors have read and approved the final manuscript.