Дата поступления рукописи в редакцию: 13.05.2026 г.
Дата принятия рукописи в печать: 19.06.2026 г.
DOI: 10.24412/2224-9133-2026-5-298-302

ЗАРИФОВА Вероника Баходуровна,
Финансовый университет при Правительстве Российской Федерации Россия, Москва, магистр,
e-mail: nika.zarifova@yandex.ru

СЕЛЮКОВА Арина Андреевна,
Финансовый университет при Правительстве Российской Федерации Россия, Москва, магистр,
e-mail: seluykovaa@gmail.com

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НАЦИИ: МЕЖДУНАРОДНЫЕ НОРМЫ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТВЕТСТВЕННОСТИ ЗА КИБЕРПРЕСТУПЛЕНИЯ

Аннотация. *В статье представлен комплексный анализ информационной безопасности как элемента национальной безопасности в условиях цифровизации. На основе актуальных статистических данных охарактеризована динамика киберпреступности в Российской Федерации за, выделены новейшие угрозы — использование технологий искусственного интеллекта (дипфейки, синтез голоса) и эволюция программ-вымогателей. Рассмотрены нормы российского уголовного и административного законодательства о защите критической информационной инфраструктуры. Проведён сравнительный анализ механизмов уголовной ответственности за киберпреступления против личности и компьютерных систем в России, США, Японии, Германии, Италии и Республике Корея. Изучены международные стандарты и инициативы: Будапештская конвенция (2001), Конвенция ООН против киберпреступности (2024). Сформулированы рекомендации по построению экосистемы упреждающей киберзащиты, интегрирующей право, технологии и международное сотрудничество.*

Ключевые слова: *информационная безопасность, киберпреступления, критическая информационная инфраструктура, искусственный интеллект, Будапештская конвенция, Конвенция ООН против киберпреступности, ШОС, СНГ, БРИКС, уголовная ответственность, цифровой суверенитет.*

ZARIFOVA Veronika Bahodurovna,
Financial University under the Government of the Russian Federation Russia,
Moscow Master's degree

SELYUKOVA Arina Andreevna,
Financial University under the Government of the Russian Federation Russia,
Moscow Master's degree

INFORMATION SECURITY OF THE NATION: INTERNATIONAL NORMS AND COMPARATIVE ANALYSIS OF RESPONSIBILITY FOR CYBERCRIMES

Annotation. *The article presents a comprehensive analysis of information security as an element of national security in the context of digitalization. Based on current statistical data, the article describes the dynamics of cybercrime in the Russian Federation and highlights the latest threats, such as the use of artificial intelligence technologies (deepfakes, voice synthesis) and the evolution of ransomware. The article also examines the provisions of Russian criminal and administrative legislation regarding the protection of critical information infrastructure. Additionally, the article provides a comparative analysis of the mechanisms of criminal liability for cybercrimes against individuals and computer systems in Russia, the United States, Japan,*

Germany, Italy, and the Republic of Korea. International standards and initiatives have been studied: The Budapest Convention (2001), the UN Convention against Cybercrime (2024). Recommendations have been formulated for building an ecosystem of proactive cyber defense that integrates law, technology, and international cooperation.

Key words: *information security, cybercrimes, critical information infrastructure, artificial intelligence, Budapest Convention, UN Convention against Cybercrime, SCO, CIS, BRICS, criminal liability, digital sovereignty*.

На протяжении последних лет наблюдался устойчивый рост преступлений, совершаемых с использованием цифровых технологий. Так, в 2017 г. было зарегистрировано 90 597 таких преступлений, в 2018 г. — 174 674 (+92,8 %), в 2019 г. — 294 409 (+68,5 %), в 2020 г. — 510 396 (+73,4 %), в 2021 г. — 517 722 (+1,5 %), в 2022 г. — 522 065 (+0,8 %), в 2023 г. — 676 951 (+29,7 %), в 2024 г. — 775 тыс. . Однако в 2025 году ситуация принципиально изменилась: впервые за многие годы зафиксировано снижение числа киберпреступлений — до 663 тыс., что на 12% меньше, чем годом ранее. Сократилось и число жертв кибермошенников — на 5,5%, до 534,5 тыс. человек. При этом сумма зарегистрированного материального ущерба также снизилась с 205 млрд. до 189,5 млрд. рублей. Эксперты МВД связывают это с комплексом принятых государством мер: если в январе 2025 года ведомство еженедельно фиксировало свыше 9 тыс. киберпреступлений, то в декабре показатель опустился ниже 6 тыс.[1]. Данная динамика свидетельствует о первых ощутимых результатах государственной политики, однако прогнозы указывают на высокую степень киберугрозы. Мировой экономический ущерб может достичь 10,5 трлн долларов США, что превращает ее в одну из наиболее значимых угроз [2].

Информационные технологии стремительно развиваются, проникая во все сферы жизни. Они формируют глобальное информационное пространство, которое открывает новые возможности для экономического роста и социального прогресса. Однако вместе с этим возникают и новые угрозы. Информационная среда стала неотъемлемой частью нашей реальности, но одновременно превратилась в площадку для противоправной деятельности. Её масштабы и общественная опасность растут. Эволюция правонарушений в сфере информации напрямую связана с научно-техническим прогрессом. Цифровая среда стала ареной для преступлений против личности и общественной безопасности. Такие как нарушение неприкосновенности частной жизни через незаконный сбор и распространение персональных данных, киберпреследование (сталкинг) и установку шпионского программного обеспечения. Серьезной угрозой является распространение противоправного материалов: от экстремистской направленности и детской порнографии до клеветы и оскорблений в публичном пространстве. Особую и новейшую группу преступлений против личности формируют деяния, совершаемые с использованием технологий искусственного интеллекта (ИИ). Речь идет о создании дипфейков для компрометации или шантажа, а также о синтезе голоса для введения в заблуждение. К числу иных киберпреступлений относятся деяния против безопасности компьютерных данных и систем (неправомерный доступ, создание вредоносного ПО), а также имущественные киберпреступления (компьютерное мошенничество, кибервымогательство.

Многоуровневая природа киберпреступлений подчеркивает необходимость комплексного правового регулирования на национальном и международном уровнях. К числу наиболее значимых глобальных инициатив относится Будапештская конвенция о преступности в сфере компьютерной информации (2001 г.). Она остается наиболее ратифицированным международным договором, специально посвященным борьбе с преступлениями в сфере компьютерной информации. Ее основное значение заключается в унификации составов преступлений и создании общих процессуальных механизмов. Однако Будапештская конвенция подвергается критике за свою «экстерриториальность» (особенно в контексте ст. 32, допускающей трансграничный доступ к данным без уведомления государства) и отражение преимущественно западных правовых подходов, что, по мнению ряда исследователей, подрывает суверенитет национальных государств. Данная критика стимулировала инициативу России и группы единомышленников в рамках ООН по разработке Всеобъемлющей международной конвенции по противодействию использованию ИКТ в преступных целях. Итогом стало принятие Конвенции ООН против киберпреступности (резолюция ГА ООН 79/243 от 24 декабря 2024 г.). В отличие от Будапештской конвенции, новый документ применяет широкий подход, охватывая не только киберзависимые, но и кибепосредованные преступления. Конвенция фокусируется на определении юрисдикции, защите прав человека при осуществлении мер киберследствия (ст. 6), а также на механизмах оказания правовой помощи развивающимся

странам. Фрагментация глобального правового ландшафта подчеркивает растущую роль региональных альянсов, ориентированных на цифровой суверенитет. В 2025 году в рамках СНГ Таджикистан предложил создать Межгосударственный киберотряд, а в рамках БРИКС обсуждается целесообразность учреждения Рабочей группы по кибербезопасности и защите электронных доказательств. Сравнительный анализ уголовной ответственности за киберпреступления против личности Борьба с киберпреступлениями против личности требует гармонизации национальных законодательств, однако существующие правовые системы демонстрируют значительные различия в подходах. Российская Федерация основывает свою систему на Главе 28 УК РФ «Преступления в сфере компьютерной информации» (ст. 272– 274.5), а также на смежных нормах. Незаконный сбор и распространение персональных данных подпадают под действие ст. 137 и ст. 138 УК РФ. С 2024 года ужесточена ответственность за распространение дипфейков, если деяние совершено с использованием ИИ. Статья 274.1 УК РФ устанавливает специальную ответственность за неправомерное воздействие на критическую информационную инфраструктуру (до 10 лет лишения свободы). Административная ответственность предусмотрена главой 13 КоАП РФ [3].

Соединенные Штаты Америки применяют универсальную концепцию «защищенного комв пьютера» (Computer Fraud and Abuse Act, 18 U.S.C. § 1030). Для преступлений против личности используются: 18 U.S.C. § 2261A (киберпреследование), 18 U.S.C. § 1028 (мошенничество с идентификационными данными), 18 U.S.C. § 1028A (отягченная кража личности). Характерной чертой американского подхода является обязательное дополнительное наказание за кражу личности [4].

Япония регулирует ответственность Законом о запрете несанкционированного компьютерного доступа и Уголовным кодексом. Закон о защите персональной информации (APPI) предусматривает уголовную ответственность за нарушение приказов Комиссии. В 2011 году в УК Японии введены ст. 168-2 и 168-3, криминализирующие создание и распространение компьютерных вирусов. Особенностью японского подхода является уголовное преследование даже за загрузку пиратского контента при осознании незаконности.

Германия основывается на УК ФРГ (Strafgesetzbuch). § 202a StGB (Выведывание данных) охватывает несанкционированный доступ, § 202b StGB (Перехват данных) устанавливает ответственность за перехват. Для преступлений против личности применяются § 238 StGB (киберпреследование), § 185–187 StGB (оскорбление и клевета). Германия имплементировала GDPR и Директиву NIS2 [5; 6].

Италия регулирует ответственность Уголовным кодексом, в который внесены изменения Законом № 547/1993. Ст. 615-ter устанавливает ответственность за несанкционированный доступ. Преступления против личности регулируются ст. 612-bis и 595 УК Италии. В 2025 году принят Закон об искусственном интеллекте. Особенностью итальянского подхода является наличие квалифицированного состава для случаев совершения преступления с использованием статуса оператора системы [7].

Республика Корея имеет одно из наиболее строгих законодательств в рассматриваемой сфере. Основные акты: УК, Закон о сетях (Network Act) и Закон о защите персональных данных (PIPA). Ст. 48 Сетевого закона запрещает вторжение в сеть без законного права доступа. PIPA предусматривает значительные оборотные штрафы для организаций. Уголовная ответственность за клевету — одна из самых строгих: правдивые сведения также могут быть наказуемы, если они порочат честь (ст. 307 УК Кореи) [8].

Общие тенденции и выводы. Проведенный сравнительный анализ показывает, что российское законодательство является одним из наиболее детализированных, с акцентом на уголовно-правовые меры и защиту государственного суверенитета в цифровом пространстве. В то же время в России отсутствует специализированный состав «кража личности» с обязательным дополнительным наказанием (в отличие от США), а также состав киберпреследования (в отличие от США, Германии, Италии и Японии).

США и страны Европейского союза делают акцент на универсальные нормы и административные санкции. Япония и Республика Корея занимают промежуточную позицию, сочетая строгие уголовные наказания с активным государственным регулированием. Общими тенденциями являются: ужесточение ответственности за посягательства на критическую информационную инфраструктуру; расширение круга субъектов ответственности (включая производителей ПО и руководителей компаний); внедрение превентивных обязанностей по оценке рисков; гармонизация законодательства в рамках региональных объединений. Таким образом, национальные законодательства движутся по пути создания более жестких, детализированных и превентивных правовых режимов, сочетающих уголовно-правовые санкции с административно-регуляторными мерами.

Стратегические направления построения экосистемы упреждающей киберзащиты. Проведенный анализ демонстрирует, что современная

киберпреступность эволюционировала в качественно новое явление, где особую опасность представляют преступления против личности с использованием технологий ИИ. Необходима новая парадигма национальной кибербезопасности, основанная на интеграции права, технологий, образования и международного сотрудничества.

1. Систематизация информационного законодательства.

Назревшая разрозненность норм об информации, персональных данных, связи, цифровых платформах, идентификации, электронном документообороте и искусственном интеллекте требует подготовки единого Цифрового кодекса. Одновременно необходимо законодательно определить понятие информационного правонарушения и закрепить в уголовном законе чёткие критерии, разграничивающие, выступает ли информация объектом, средством или обстановкой совершения деяния. Это устранит коллизии и обеспечит единообразие правоприменения.

2. Противодействие дипфейкам и обороту ИИ-контента.

Вместо расширительных и потенциально опасных формулировок об «автоматизированной обработке» данных следует ввести специальный состав незаконного создания и распространения синтезированных изображений, аудио- и видеозаписей, имитирующих личность без её согласия. Гражданско-правовую защиту чести и достоинства необходимо прямо распространить на случаи использования дипфейков. Маркировку ИИ-контента целесообразно внедрять поэтапно: сначала — как право, а не обязанность, с разработкой технических рекомендаций; затем, по мере накопления технологических решений и с учётом международного опыта, — как административно обеспечиваемое требование.

3. Усиление уголовно-правовой защиты и унификация ответственности.

Использование информационно-телекоммуникационных сетей и программно-аппаратных средств должно быть закреплено в качестве общего отягчающего обстоятельства, что усилит превентивный эффект без точечной правки десятков статей. Кроме того, особенная часть уголовного закона нуждается в восполнении пробелов: требуется ввести составы «кража личности» и «киберпреследование», что позволит отказаться от квалификации таких деяний по разрозненным нормам и обеспечит более надёжную защиту граждан.

4. Дифференциация административной ответственности операторов цифровой среды. Необходимо установить повышенные штрафы для организаторов распространения информации, владельцев социальных сетей, провайдеров хостинга и поисковых систем за неисполнение специфических публично-правовых обязанностей — от непредоставления сведений о пользователях до отказа удалять противоправный контент. Прогрессивная шкала санкций за систематические нарушения, вплоть до административного приостановления деятельности, должна стать реальным стимулом к оперативной модерации. Параллельно важно создать внесудебный механизм, обязывающий владельцев сайтов удалять явно недостоверные и порочащие сведения по требованию гражданина в сжатые сроки.
5. Гражданско-правовые и потребительские механизмы защиты.

Гражданский кодекс следует дополнить институтом штрафных убытков за умышленные информационные деликты, включая нарушение исключительных прав и заведомое распространение ложных порочащих сведений, что создаст серьёзный сдерживающий эффект. Одновременно в законодательстве о защите прав потребителей необходимо закрепить обязанности маркетплейсов по верификации продавцов и контролю достоверности информации о товарах, а также их субсидиарную ответственность за ущерб, причинённый потребителям недостоверными сведениями.

6. Профилактика, кадровое и технологическое обеспечение.

Упреждающая модель кибербезопасности невозможна без массового повышения цифровой грамотности. Предлагается создать единую государственную платформу кибергигиены с адаптивными сценариями обучения, ввести обязательную сертификацию компетенций для специалистов, работающих с персональными данными и объектами критической информационной инфраструктуры, а также запустить программу психологической и правовой помощи жертвам киберпреследований и дипфейков. Технологический контур должен включать национальную платформу предиктивной аналитики киберугроз и специализированные следственные подразделения по преступлениям с использованием искусственного интеллекта.

7. Международное партнёрство. Приоритетом является скорейшая ратификация Конвенции ООН против киберпреступности с оговорками, обеспечивающими национальные интересы, и продвижение гибридной модели участия негосударственных организаций в её работе — с правом экспертного голоса, но без права решающего голоса. На региональном уровне необходимо поддержать инициативу создания Межгосударственного киберотряда СНГ, разработать соглашение

о совместном реагировании на инциденты, а в формате БРИКС — учредить постоянно действующую рабочую группу по кибербезопасности и защите электронных доказательств, поручив ей подготовку модельных норм о трансграничном доступе к компьютерной информации.

Список литературы:

[1] Дремлюга Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 6 (73). С. 111–117.

[2] Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М.: Юрлитинформ, 2021. 248 с.

[3] Головненков П.В. Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB): науч.-практ. комментарий и перевод текста закона. Potsdam: Universitätsverlag Potsdam, 2021. 489 с.

[4] Русскевич Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учебное пособие. М.: Проспект, 2025. 208 с.

[5] Мартиросян А.Ж. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий: автореф. дис. ... канд. юрид. наук. М.: Дипломатическая академия МИД России, 2024. 28 с.

[6] Позднякова Е.А. Авторское право: учебник и практикум для вузов. 5-е изд., перераб. и доп. М.: Издательство Юрайт, 2026. 259 с.

References:

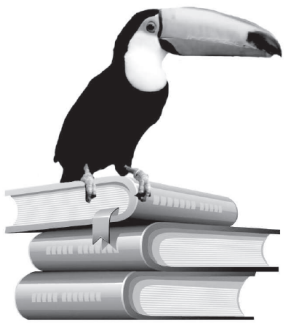
[1] Dremlyuga R.I. Computer Information as an Object of Infringement in Unauthorized Access: A Comparative Analysis of US and Russian Legislation // Journal of Foreign Legislation and Comparative Law. 2018. No. 6 (73). Pp. 111–117.

[2] Zhizhina M.V., Zavyalova D.V. Investigation of Computer Crimes in the Russian Federation and Foreign Countries: A Monograph. Moscow: Yurlitinform, 2021. 248 p.

[3] Golovnenkov P.V. Criminal Code of the Federal Republic of Germany – Strafgesetzbuch (StGB): Scientific and Practical Commentary and Translation of the Law Text. Potsdam: Universitätsverlag Potsdam, 2021. 489 p.

[4] Ruskevich E.A. Computer Crimes: Qualification Algorithms and Trends: A Study Guide. Moscow: Prospekt, 2025. 208 p.

[5] Martirosyan A.Zh. International Legal Regulation of Ensuring Security in the Field of Information and Communication Technologies: Abstract of Dissertation ... Candidate of Law. Sciences. Moscow: Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, 2024. 28 p.



Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников, учебных и методических пособий, монографий, научных статей.

Профессионально.

В максимально короткие сроки.

Размещаем в РИНЦ, E-Library.

www.law-books.ru