Дата поступления рукописи в редакцию: 20.03.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-511-514

НЕСТЕРЕНКО Андрей Владимирович,
заместитель начальника кафедры
организации правоохранительной деятельности
Северо-Кавказского института повышения квалификации
(филиал) Краснодарского университета МВД России,
подполковник полиции,
e-mail: mail@law-books.ru

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. *В статье проводится комплексный анализ современных вызовов в сфере противодействия киберпреступности в условиях ускоряющейся цифровизации общественных отношений. Рассматриваются детерминанты и специфика киберпреступности, актуальные тенденции, включая использование технологий искусственного интеллекта, а также проблемы уголовно-правового и криминологического характера. На основе изучения отечественного и зарубежного опыта, в частности законодательства Китайской Народной Республики, формулируются предложения по совершенствованию механизма противодействия данным видам преступлений. Особое внимание уделяется вопросам международного сотрудничества, необходимости усиления профилактической работы и развития цифровой грамотности населения.*

Ключевые слова: *киберпреступность, цифровая эпоха, уголовно-правовое противодействие, искусственный интеллект, международное сотрудничество, кибербезопасность, законодательство.*

NESTERENKO Andrey Vladimirovich,
Deputy Head of the Department of Law Enforcement Organization
North Caucasus Institute of Advanced Training (branch)
Krasnodar University of the Ministry of Internal Affairs of Russia,
Police Lieutenant Colonel

ACTUAL ISSUES OF COUNTERING CYBERCRIME IN THE CONTEXT OF DIGITAL TRANSFORMATION

Annotation. *The article provides a comprehensive analysis of current challenges in the field of countering cybercrime in the context of accelerating digitalization of social relations. It examines the determinants and specifics of cybercrime, current trends, including the use of artificial intelligence technologies, as well as criminal and criminological issues. Based on the study of domestic and foreign experience, particularly the legislation of the People's Republic of China, the article formulates proposals for improving the mechanism of countering these types of crimes. Special attention is given to international cooperation, the need to strengthen preventive measures, and the development of digital literacy among the population.*

Key words: *cybercrime, digital era, criminal law counteraction, artificial intelligence, international cooperation, cybersecurity, legislation*.

Стремительное развитие информационно-телекоммуникационных технологий, пронизывающих все сферы современного общества, породило принципиально новую криминальную угрозу — киберпреступность. Динамичный и трансграничный характер этого явления создает серьезные вызовы для национальных правоохранительных систем и международной безопасности в целом. Как верно отмечается в научной литературе, высокие технологии, проникая во все сферы жизнедеятельности человека, в корне меняют ее, что, бесспорно, касается и преступности [1, с. 105]. Реалии современного мира требуют постоянного совершенствования мер противодействия, основанного на глубоком научном осмыслении природы и механизмов кибер-

преступности. Актуальность темы обусловлена значительным ростом количества преступлений, совершаемых с использованием IT-технологий, их возрастающей разрушительной силой для экономики и критической инфраструктуры, а также появлением новых видов киберугроз, таких как атаки с применением генеративного искусственного интеллекта. Ущерб от таких преступлений исчисляется миллиардами рублей, что подтверждается, например, данными по Краснодарскому краю, где только в 2024 году ущерб превысил 7 млрд рублей [3].

Единое понимание киберпреступления в отечественной и международной правовой доктрине до сих пор не сформировано, что создает значительные трудности как для законодателя, так и для правоприменителя. В научном сообществе используются различные термины: «компьютерная преступность», «киберпреступность», «цифровая преступность» и др., которые характеризуются широтой подхода и сложностями в определении конкретных признаков [6, с. 22]. В российском уголовном законодательстве отсутствует легальное определение киберпреступления. Уголовная ответственность за преступления, непосредственно связанные с вмешательством в работу компьютерной информации, установлена в главе 28 УК РФ. Однако, по сути, к киберпреступлениям следует относить и те традиционные составы, которые все чаще совершаются с использованием информационно-телекоммуникационных сетей (мошенничество, вымогательство и др.), где соответствующий признак включается в качестве квалифицирующего. Интересен опыт китайских коллег, где в правовой доктрине под киберпреступлением предлагается понимать «любые преступления, совершаемые с помощью компьютерной системы или сети, в ее рамках или против нее». Верховный народный суд КНР, Верховная народная прокуратура КНР и Министерство промышленности и информатизации КНР закрепили в своих мнениях трехуровневую классификацию дел о киберпреступлениях, относя к ним преступления против безопасности компьютерных информационных систем, преступления, связанные с невыполнением обязательств по управлению кибербезопасностью, а также иные преступления, совершаемые в основном через информационные сети [4]. Представляется, что данный комплексный подход к классификации является более прогрессивным и отвечает реалиям цифровой эпохи, так как охватывает не только прямые атаки на компьютерные системы, но и всю палитру противоправной деятельности в киберпространстве.

Ландшафт киберпреступности непрерывно эволюционирует, адаптируясь к технологическим новшествам и меняющимся условиям. Среди наиболее актуальных тенденций можно выделить использование технологий искусственного интеллекта (AI) и генеративных моделей. ИИ предоставил злоумышленникам принципиально новые возможности. Так, с помощью генеративных моделей стало возможным создание глубоких подделок (дипфейк) — видео- и аудиоконтента, который практически невозможно отличить от реального для неподготовленного пользователя [7, с. 52; 8, с. 3]. Это позволяет мошенникам имперсонировать руководителей, родственников, представителей власти, существенно повышая эффективность социальной инженерии. Подделать можно все: аккаунты, письма, QR-коды, голоса и лица знакомых. Наблюдается также рост масштабов и изощренности социальной инженерии. Если ранее фишинговые рассылки были достаточно примитивными, то сегодня атакующий, незаконно завладев персональной информацией, может знать имена начальника, коллег, родственников, последние события в компании и многое другое, что делает его атаки высокотаргетированными и персонализированными. Криминализация криптовалют и децентрализованных финансов (DeFi) также остается серьезной проблемой: несмотря на запретительные меры в ряде стран, включая Китай, злоумышленники находят обходные пути с использованием иностранных платформ для отмывания преступных доходов. Анонимность и быстрота транзакций в блокчейне делают его идеальным инструментом для киберпреступников. Утечки данных как системная угроза — утечка конфиденциальных данных, включая персональные данные и медицинскую тайну, стала одной из самых распространенных и разрушительных угроз для бизнеса и общества, последствия таких утечек варьируются от репутационных потерь до шантажа и прямого финансового ущерба. Наконец, трансграничный характер киберпреступности по своей природе не знает национальных границ: преступники могут действовать из одной юрисдикции, а их жертвы находиться в другой, что создает непреодолимые препятствия для правоохранительных органов и требует тесного международного сотрудничества [5].

Система противодействия киберпреступности в России сталкивается с рядом системных проблем, которые снижают ее эффективность. Прежде всего, это пробелы и архаичность законодательства. Уголовный кодекс РФ не успевает за скоростью технологических изменений. Составы преступлений, сформулированные в главе 28 УК РФ, зачастую не покрывают новые способы совершения преступлений с использованием AI, больших данных и интернета вещей (IoT). В отличие от Китая, где киберзаконодательство представляет собой систему законов, адми-

нистративных правил и ведомственных инструкций, создающую надежные институциональные гарантии [4], в России наблюдается фрагментарность правового регулирования. Острейшей проблемой остаются сложности квалификации и доказывания: сложность сбора и фиксации цифровых доказательств, их процессуального закрепления является одной из ключевых проблем. Электронные доказательства легко могут быть уничтожены, изменены или перенесены в другую юрисдикцию. Отсутствие единых методик расследования и недостаточная оснащенность экспертных учреждений специальным программно-аппаратным комплексом также тормозят раскрываемость. Несмотря на признание важности сотрудничества на высшем уровне [5], на практике межведомственное и международное взаимодействие затруднено из-за различий в национальных законодательствах, бюрократических барьеров и политических разногласий. Кроме того, наблюдается острый кадровый дефицит — острейшая нехватка высококвалифицированных кадров в правоохранительных органах, способных эффективно расследовать сложные киберинциденты, остается системной проблемой. В этой связи положительным представляется опыт создания киберполигонов для эффективной подготовки специалистов по кибербезопасности для банковской сферы, о котором сообщалось на круглом столе в НИУ ВШЭ [2].

Следует рассмотреть возможность стимулирования добровольного сообщения об инцидентах, например, путем введения уголовно-правового иммунитета для компаний, своевременно сообщающих о хакерских атаках и утечках данных, что будет способствовать сбору более полной информации о киберугрозах. Важнейшим направлением является усиление профилактической и просветительской работы. Как верно отмечает А.В. Серебренникова, вектор внимания должен быть направлен не на ограничение использования онлайн-пространств, а на эффективную цифровую социализацию молодого поколения, формирование у него качеств ответственных и компетентных пользователей [1, с. 110]. Необходима серьезная просветительская работа, подобная той, что обсуждалась на круглом столе «Цифровая гигиена», направленная на все слои населения [3]. Государство должно инициировать и финансировать масштабные кампании по повышению цифровой грамотности. Учитывая трансграничный характер угрозы, необходимо активизировать работу по развитию международного сотрудничества в направлении гармонизации законодательства — сближения национальных законодательств в сфере кибербезопасности на основе таких международных документов, как Конвенция Совета Европы о киберпреступности (Будапештская конвенция), и выработке новых универсальных договоров, а также создания оперативных каналов связи для упрощения процедур взаимодействия правоохранительных органов разных стран. Не менее важно укрепление публично-частного партнерства: бизнес, обладающий передовыми технологиями и экспертизой, должен стать полноправным партнером государства в этой борьбе. Создание на базе ведущих российских IT-компаний центров мониторинга и реагирования на кибератаки позволит объединить ресурсы для более эффективного противодействия. Наконец, необходима адаптация положительного зарубежного опыта. Опыт Китая демонстрирует эффективность комплексного подхода, включающего не только уголовно-правовые запреты, но и мощную профилактическую составляющую. В КНР снимаются и постоянно демонстрируются фильмы, видеоролики, транслируются передачи, издаются журналы о борьбе с мошенничеством, в подготовке которых участвуют работники органов прокуратуры [4]. Создание в Верховной народной прокуратуре КНР специальной руководящей группы по борьбе с киберпреступностью также является позитивной практикой, которую можно изучить и адаптировать.

В качестве первоочередных шагов предлагается закрепить в УК РФ комплексное определение киберпреступления и криминализировать новые способы их совершения с использованием AI; активно развивать систему подготовки и переподготовки профильных кадров для правоохранительных органов, в том числе на базе киберполигонов; инициировать масштабную государственную программу по повышению цифровой грамотности населения, делая акцент на «цифровой гигиене»; интенсифицировать международное сотрудничество, в первую очередь с стратегическими партнерами, такими как Китай, в области гармонизации законодательства и создания оперативных каналов взаимодействия. Только комплексный и проактивный подход, объединяющий усилия государства, бизнеса и общества, позволит эффективно противостоять вызовам киберпреступности и обеспечить безопасное развитие цифрового общества.

Список литературы:

[1] Серебренникова А.В. Противодействие киберпреступности: актуальные вопросы // Вестник ВНИИ МВД России. 2023. Т. 16. № 1. С. 104-112.

[2] Круглый стол по кибербезопасности // Факультет компьютерных наук НИУ ВШЭ. [Электронный ресурс]. URL: https://cs.hse.ru/table_cybersecurity (дата обращения: 03.03.2026).

[3] Круглый стол «Цифровая гигиена: Как защититься от кибермошенников» // Коммерсантъ. 2025. [Электронный ресурс]. URL: https://events.kommersant.ru/krd/events/czifrovaya-gigiena-k… (дата обращения: 03.03.2026).

[4] Уголовно-правовое противодействие киберпреступности в России и Китае: сравнительно-правовой аспект // Legascom. [Электронный ресурс]. URL: https://legascom.ru/notes/8056-ugolovno-pravovoe-protivodejs… (дата обращения: 03.03.2026).

[5] Круглый стол по киберправу, киберпреступности и кибербезопасности // Международный союз электросвязи (МСЭ). 2023. [Электронный ресурс]. URL: https://www.itu.int/net4/wsis/forum/2023/ru/Agenda/Session/5… (дата обращения: 03.03.2026).

[6] Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. 158 с.

[7] Ларан А. А. Теоретико-правовые подходы к пониманию искусственного интеллекта: понятие, виды и существенные признаки искусственного интеллекта // Студенческий. – 2021. – № 36-3(164). – С. 50-55.

[8] Никольская К., Наумов В. Искусственный интеллект в праве // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. – Владивосток, 2020.

References:

[1] Serebrennikova A.V. Countering cybercrime: topical issues//Bulletin of the All-Russian Research Institute of the Ministry of Internal Affairs of Russia. 2023. T. 16. № 1. S. 104-112.

[2] Round table on cybersecurity//Faculty of Computer Science, National Research University Higher School of Economics. [Electronic resource]. URL: https://cs.hse.ru/table_cybersecurity (access date: 03.03.2026).

[3] Round table “Digital hygiene: How to protect yourself from cyber fraudsters “//Kommersant. 2025. [Electronic resource]. URL: https://events.kommersant.ru/krd/events/czifrovaya-gigiena-k… (accessed on: 03.03.2026).

[4] Criminal law counteraction to cybercrime in Russia and China: comparative legal aspect//Legascom. [Electronic resource]. URL: https://legascom.ru/notes/8056-ugolovno-pravovoe-protivodejs… (accessed on: 03.03.2026).

[5] Round table on cyber law, cybercrime and cybersecurity//International Telecommunication Union (ITU). 2023. [Electronic resource]. URL: https://www.itu.int/net4/wsis/forum/2023/ru/Agenda/Session/5… (accessed on: 03.03.2026).

[6] Efremova M.A. Criminal law protection of information security: monograph. M., 2018. 158 pp.

[7] Laran A. A. Legal approaches to the understanding of artificial intelligence: the concept, types and essential features of artificial intelligence//Student. – 2021. – № 36-3(164). - S. 50-55.

[8] Nikolskaya K., Naumov V. Artificial Intelligence in Law//2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. - Vladivostok, 2020.

