

ИНФОРМАЦИОННОЕ ПРАВО

2025 # 1(83)



ТЕМЫ НОМЕРА:

Киберпреступность:
правовые новеллы

ИИ против мошенничества
в финансовой сфере

Информационная среда
высокотехнологичных компаний

Цифровые технологии
в трансграничных
строительных проектах

Правовая классификация
беспилотных транспортных
средств

ISSN 1999-480X



9 771999 480005 >

Новеллы национального законодательства и международного права в сфере противодействия киберпреступности

Ивлиев Г.П., Карцхия А.А.*

Аннотация. Целью исследования является правовой анализ актуальных правовых вопросов состояния и особенностей противодействия киберпреступности в сфере информационно-коммуникационных и цифровых технологий в российском и международном праве. **Методы исследования** заключаются в сравнительно-правовом анализе национального законодательства и международного права в сфере информационно-коммуникационных технологий и практики его применения, а также формально-логическом исследовании понятийного аппарата, содержания и структуры предмета исследования. **Результаты исследования** позволяют выявить особенности современной киберпреступности, виды и состав современных киберпреступлений, включая правонарушения, совершенные с использованием компьютерной техники, программного обеспечения, технических средств в реальном мире и в цифровом киберпространстве. **Обсуждение.** Авторы пришли к выводу, что стремительное развитие цифровых и информационных технологий, создание институтов киберэкономики повлекли формирование нового вида преступлений вне рамок традиционного понимания преступности в сфере информационных технологий и средств связи, что обусловлено цифровой революцией в современном обществе.

Ключевые слова: информационные технологии, цифровая модернизация, цифровые технологии, Интернет, киберэкономика, киберпреступность, преступления в сфере ИКТ, безопасность, противодействие киберпреступности.

Abstract. The purpose of the research is a legal analysis of current legal issues of the state and features of countering cybercrime in the field of information, communication and digital technologies in Russian and international law. **The research methods** consist in a comparative legal analysis of national legislation and international law in the field of information and communication technologies and the practice of its application, as well as a formal and logical study of the conceptual framework, content and structure of the research subject. **The results** of the study make it possible to identify the features of modern cybercrime, the types and composition of modern cybercrimes, including offenses committed using computer technology, software, and technical means in the real world and in digital cyberspace. **Discussion.** The authors concluded that the rapid development of digital and information technologies, the creation of institutions of cyber economics has led to the formation of a new type of crime beyond the traditional understanding of crime in the field of information technology and communications, due to the digital revolution in modern society."

Keywords: information technology, digital modernization, digital technologies, Internet, cybereconomics, cybercrime, crimes in the field of ICT, security, countering cybercrime.

Введение. Современное общество, как отмечается в Концепции внешней политики Российской Федерации¹, переживает эпоху революционных перемен, которая прежде всего связана со структурной перестройкой мировой экономики,

обусловленной переходом на новую технологическую основу посредством внедрения технологий искусственного интеллекта, новейших информационно-коммуникационных, энергетических, биологических технологий и нанотехнологий.

Цифровая эпоха показывает экспоненциальный рост экономики, который стимулируется цифровыми, информационными технологиями и, прежде всего, углублением взаимосвязанности глобального

¹ Указ Президента РФ от 31 марта 2023 г. № 229 «Об утверждении Концепции внешней политики Российской Федерации» // Собрание законодательства РФ. 2023. 03 апреля. № 14. Ст. 2406.

* **Ивлиев Григорий Петрович**, Президент Евразийского патентного ведомства, научный руководитель Федерального института промышленной собственности, кандидат юридических наук, заслуженный юрист Российской Федерации. E-mail: ivliev@eapo.org

Карцхия Александр Амиранович, профессор кафедры публичного и международно-правового обеспечения национальной безопасности РГУ нефти и газа (НИУ) имени И.М. Губкина, доктор юридических наук, доцент. E-mail: arhz50@mail.ru

Рецензент: Лопатин Владимир Николаевич, главный редактор журнала «Информационное право», научный руководитель РНИИИС, эксперт РАН, доктор юридических наук, профессор, Заслуженный деятель науки Российской Федерации.

Novelties of National Legislation and International Law in the Field of Countering Cybercrime

G.P. Ivliev, President of the Eurasian Patent Office, Research advisor of the Federal Institute of industrial property, Candidate of Law, Honored Lawyer of the Russian Federation.

A.A. Kartskhiya, Professor of the Department of Public and International Legal Support of National Security at Gubkin Russian State University of Oil and Gas (NIU), Doctor of Law, Associate Professor.

Reviewer: V.N. Lopatin, Editor-in-Chief of the journal «Information Law», Scientific Director of the Republican Research Institute of Intellectual Property, expert of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Scientist of the Russian Federation.

ландшафта между такими передовыми технологиями, как блокчейн, искусственный интеллект (далее – ИИ) и нейросети, Интернет вещей (IoT) и др. Активное и расширяющееся использование криптовалют, смарт-контрактов и децентрализованных организаций предоставляет существенные преимущества в конкуренции с глобальными корпорациями благодаря трансграничности, скорости операций, масштабируемости и доступу к лучшим ресурсам в самых выгодных регионах мира.

С точки зрения киберэкономики (*cyber economy*) как концепта новой экономической теории [1], в настоящее время происходит смена одной системной парадигмы на другую, главенствующими функциями которой становятся: (1) децентрализованные социально-экономические системы (киберэко-системы), функционирующие независимо от государств и правительств; (2) виртуальные агенты (цифровые сущности), которые могут создавать собственные валюты, продукты и услуги в виртуальных экономических мирах; (3) финансовые транзакции на основе технологии децентрализованных реестров (блокчейн) без участия финансовых регуляторов, центральных банков и традиционных финансовых институтов; (4) децентрализованные глобальные рынки, объединяющие производителей и потребителей без посредничества банковской системы и надзорных органов.

Киберэкономику можно рассматривать как цифровую систему управления экономикой (некий аналог ранее разработанной в СССР общегосударственной системы сбора и обработки информации (ОГАС) для учета, планирования и управления народным хозяйством) [2], способную прогнозировать и просчитывать перспективные модели и управленческие решения с помощью современных IT-технологий и данных в целях превращения хаотичных процессов в более управляемую систему, способную предугадывать проблемы, находить решения, распределять ресурсы, предотвращать угрозы и нивелировать риски.

Как результат цифровой модернизации современной экономики в рамках технологической революции Индустрии 4.0, киберэкономика формирует в различных отраслях новые цифровые бизнес-модели; горизонтальную и вертикальную интеграцию и интегрированные цепочки создания стоимости, интеллектуальные услуги и сервисы, цифровые рабочие места, цифровые продажи и маркетинг, а также новые экосистемы и сети создания ценностей. Все это с применением технологией обработки и анализа больших данных, промышленного Интернета вещей, кибербезопасности, облачных технологий, аддитивного (дополнительного) производства и расширенной (виртуальной) реальности. Киберэкономика представляет собой новую систему хозяйствования [3, 4]. В то же время киберэкономика рассматривается как эффективная экономическая государственная система противодействия гибридной войне, обеспечения национальной безопасности [5]. Более того, уже давно обосновано, что цифровая экономика закономерно приведет к экономической киберсистеме [6] – киберэкономике.

Вместе с тем развитие киберэкономики способствовало появлению нового аспекта кибербезопасности – экономики кибербезопасности [7], объединяющей в научном смысле основные

результаты и инструменты таких дисциплин, как социология, психология, юриспруденция, политология и информатика.

Состояние киберпреступности. На фоне стремительного изменения экономической модели хозяйствования складываются новые негативные тенденции. Хотя новые технологии обладают огромным потенциалом для революционного изменения новой экономики (киберэкономики), они одновременно создают новые угрозы и уязвимости в сфере кибербезопасности, новые риски в отношении публичного и частного характера. Вместе с тем огромное число ложной информации и контента, создаваемых нейросетями (*deep fake*) в Интернете, расширение практики использования даркнет (*dark net*) в преступных целях формируют новые угрозы в сфере кибербезопасности.

Новый подход к киберпреступности сформулирован в утвержденной Правительством РФ в декабре 2024 года Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий² (далее – ИКТ). Современное информационное общество характеризуется широким распространением и доступностью мобильных устройств, а также беспроводных технологий и сетей связи. Информационно-коммуникационные технологии стали частью современных управленческих систем практически во всех сферах жизни российского общества. Развитие инструментов финансового рынка, платежных систем, а также в целом цифровизация экономических процессов дали толчок к появлению специфических способов расчетов – электронных средств платежа и их использованию юридическими и физическими лицами для безналичных расчетов. Вместе с тем преступные посягательства в информационно-коммуникационной сфере с каждым годом занимают все более заметное место в структуре всех зарегистрированных преступлений в стране: за последние пять лет количество таких преступлений возросло более чем в два раза, а каждое третье преступление совершено в информационно-коммуникационной сфере либо с использованием ИКТ. В структуре преступлений данной категории в последний год преобладали кражи и мошенничества (70%), незаконное производство, сбыт или пересылки наркотических средств и психотропных веществ (12%), экономическую направленность имеют 3,4% преступлений, экстремистскую направленность и террористический характер – 0,2%. В сфере ИКТ особую активность проявляют организованные преступные группы, которые используют вредоносное программное обеспечение, фишинговые сайты, специальную технику, электронные платформы и кол-центры для совершения массовых мошеннических звонков. Существенное негативное влияние на криминальную обстановку в IT-сфере оказывает сложная международная ситуация, в том числе связанная с деятельностью спецслужб недружественных государств и неонацистских формирований, курируемых иностранными спецслужбами. Основная масса

² Распоряжение Правительства РФ от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // Собрание законодательства РФ. 2025. 13 января. № 2. С. 76.



преступлений совершается специализирующимися на мошенничествах транснациональными организованными преступными группами, связанными с организацией хищения персональных данных граждан Российской Федерации и работой действующих с территорий недружественных государств колл-центров, с использованием которых похищаются средства граждан. Все большее распространение получает использование цифровой валюты при совершении преступлений, особенно при отмывании преступных доходов.

По оценкам экспертов российских компаний в сфере кибербезопасности³, самой атакуемой киберпреступниками отраслью России в 2024 году стал госсектор – на него было направлено 15% всех атак хакерских группировок, а всего зафиксировано порядка 150 тысяч попыток хакерских атак на госсектор, что на 20% больше, чем в 2023 г. Подавляющее большинство атак на российский госсектор совершается с целью шпионажа и хактивизма, что обусловлено, в том числе, геополитическими причинами. Как правило, атаки на российский госсектор происходят из стран Азии и Восточной Европы.

В отчете Европола за 2024 год⁴ также отмечается, что ландшафт киберпреступлений по-прежнему разнообразен. Наиболее угрожающими проявлениями киберпреступности в Европейском союзе в 2023 году оставались атаки программ-вымогателей, сексуальная эксплуатация детей (CSE), онлайн-мошенничество, торговля краденными данными по принципу *crime-as-a-service*, а сеть даркнет (*dark web*) продолжает оставаться ключевым фактором, способствующим киберпреступности.

По опубликованным данным Следственного комитета России и МВД России⁵, рост преступлений с использованием ИКТ в 2024 г. составил 40% от общего числа зарегистрированных в России преступлений. Всего в 2024 г. в России зарегистрировано 765,4 тыс. киберпреступлений (рост на 13,1%), и тенденция ежегодного роста числа преступлений сохраняется. Общий ущерб от преступлений в ИКТ-сфере за 9 месяцев 2024 года составил 150 млрд рублей. Отмечается особая активность организованных групп, применяющих вредоносное ПО, фишинговые сайты, специальную технику, электронные платформы и колл-центры с подменными номерами. В Интернете продолжают создаваться финансовые пирамиды, а ИКТ-сфера активно используется в совершении наркопреступлений, преступлений экстремистской и террористической направленности.

Противодействие киберпреступности является одной из форм обеспечения национальной безопасности России. В последние годы определился ряд устойчивых трендов существующих киберугроз [8].

Киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации

в информационной сфере. Предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием ИКТ, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют, определены основными задачами достижения целей обеспечения государственной и общественной безопасности в соответствии со Стратегией национальной безопасности Российской Федерации⁶. При этом обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации и неприкосновенности частной жизни при использовании информационных технологий, отнесены к национальным интересам Российской Федерации в информационной сфере, согласно Доктрине информационной безопасности Российской Федерации.

Особенности киберпреступности. Эксперты отмечают особые характеристики киберпреступности: высокая латентность, специальная подготовка преступников, трансграничность, автоматизированность преступлений, нетрадиционность средств противодействия киберпреступности [9, 10]. Объективная реальность подтверждает тот факт, что новые технологии способствуют появлению новых видов преступлений, росту числу совершаемых преступлений.

Следует отметить, что на сегодняшний день не существует универсального определения киберпреступности. Киберпреступность можно рассматривать как традиционную преступную деятельность, девиантное поведение, правовую проблему, политическую проблему, преступление «белых воротничков», продукт социального конструирования или технологическую проблему. Эта концепция основана на признании того, что киберпреступность носит глобальный характер, совершается в обширной области киберпространства, отличается от многих других преступлений, в том числе методиками расследования, применением специальных криминалистических методов, получением и исследованием доказательственной базы, цифровых доказательств [11, 12].

Обычно выделяют следующие виды киберпреступлений: (1) мошенничество с использованием электронной почты и интернета; (2) кража цифровой личности (хищение и использование персональных данных); (3) кража данных платежных карт и другой финансовой информации; (4) хищение и перепродажа корпоративных данных; (5) кибершантаж (вымогательство денег под угрозой атаки); (6) атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа); (7) криптоджекинг (майнинг криптовалют с использованием чужих энергоресурсов); (8) кибершпионаж (получение несанкционированного доступа к государственным или корпоративным сведениям); (9) нарушение работы систем с целью компрометации сети; (10) нарушение авторских прав (цифровое пиратство); (11) незаконное проведение азартных игр; (12) онлайн-торговля запрещенными товарами, включая

⁶ Указ Президента РФ от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. 05 июля. № 27 (часть II). Ст. 5351.

наркотики; (13) домогательства, изготовление или хранение детской порнографии. Отдельно следует выделить особо тяжкие преступления – кибертерроризм и экстремизм.

При этом киберпространство представляет собой сложную среду, формирующуюся в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключенных к ним сетей, не существующих в какой-либо физической форме [12]. Киберпреступность носит трансграничный характер, а Интернет все чаще становится сферой террористических и экстремистских деяний, вовлечения и вербовки молодежи в преступную деятельность, областью целенаправленных кибератак на государственные и коммерческие структуры в преступных целях, включая посягательства на критически важную инфраструктуру, а также дестабилизацию международной информационной безопасности. Современная действительность доказывает, что киберпреступность при определенных условиях перформатируется в информационную войну, и в борьбе с киберпреступностью нельзя ограничиваться сферой компьютерных преступлений, совершаемых с помощью ИКТ. Сфера киберпреступлений предполагает использование всех доступных ИКТ в преступных целях, включая не только компьютеры, но и современные телефоны, факсы, спутниковую связь и другие IT-технологии.

Многие исследователи отмечают [13, 14] такие особенности киберпреступности, как ее глобальный и трансграничный характер, неосязаемость (невидимость), специфику цифровой (электронной) среды совершения преступления, нетипичный характер правонарушения, многоаспектность и междисциплинарность (сочетание технических, правовых, социо-культурных аспектов).

Некоторые исследователи определяют киберпреступность как совокупность преступлений, которые совершаются не только с помощью компьютера или иных средств доступа к киберпространству, но и непосредственно в киберпространстве. Компьютерные, электронные, мультимедийные устройства являются не частью киберпространства, а лишь «ключами» к нему, «порталами» входа [15, 16]. Другие авторы рассматривают киберпреступность как исторически изменчивое, латентное социальное и уголовно-правовое негативное явление, представляющее собой систему преступлений, совершенных дистанционно в информационном пространстве с использованием средств ИКТ, делая акцент на способе и месте совершения преступления [17].

Под киберпреступлением, по мнению ряда авторов, следует понимать преступления, посягающие на безопасность личности, общества, государства, информационного виртуального пространства, совершенные с использованием информационных, технических и кибертехнологий. А использование Интернета и необходимых технических средств следует считать способом совершения киберпреступления [11, с. 344].

Уголовный кодекс РФ (глава 28) содержит виды преступлений, связанных с использованием современных компьютерных технологий, которые формируют особую группу преступлений – преступления в сфере компьютерной информации, которые включают: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание,

использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ИТС) (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1), а также нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации ИТС Интернет и сети связи общего пользования (ст. 274.2). Новая статья 272.1. УК РФ установила ответственность за незаконное использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения. Специальная уголовная ответственность установлена за незаконное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ), что представляет собой нарушение установленных законом и подзаконными актами правил, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием ИКТ, определено общее понятие противоправных деяний, совершенных с использованием ИКТ, к которым отнесены общественно опасные деяния, за которые предусмотрена уголовная либо административная ответственность, совершенные с использованием (применением) ИКТ или в сфере компьютерной информации, в том числе с использованием (применением) электронных или IT-сетей, включая сеть «Интернет», информационной инфраструктуры, компьютерной техники, программных средств, онлайн-сервисов, средств коммуникации (в том числе средств мобильной связи, сервисов обмена мгновенными сообщениями, IP-телефонии), электронных средств платежа, операций с цифровой валютой и цифровыми финансовыми активами. Противоправные деяния с учетом их особенностей классифицируются в Концепции по трем основным типам:

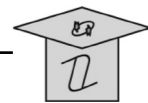
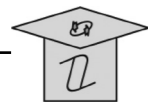
- правонарушения и преступления в сфере компьютерной информации;
- правонарушения и преступления, квалифицирующим признаком которых является их совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»;
- правонарушения и преступления, при совершении которых применение ИКТ является альтернативным способом.

Такая классификация подтверждает тройственный характер современной киберпреступности: как сферы совершения преступлений (сфера компьютерной информации, киберпространство), как специальный способ совершения киберпреступлений (с

³ THREAT ZONE2025. Исследование российского ландшафта киберугроз // BI.Zone. 2025. URL: <https://bi.zone/expertise/research/threat-zone-2025/> (дата обращения: 12.01.2025).

⁴ Internet Organised Crime Threat Assessment (IOCTA) 2024, Europol (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg. URL: https://ec.europa.eu/eusurvey/runner/eus_strategic_reports (дата обращения: 12.01.2025).

⁵ URL: <https://cnews.ru/link/n623042> (дата обращения: 10.12.2024).



использованием электронных или информационно-телекоммуникационных сетей) и как разновидность способа традиционного совершения преступлений.

Международное право также пополнилось новым документом – принятой в декабре 2024 года Генеральной Ассамблеей, разработанной по инициативе России и ее активном участии, всеобъемлющей Конвенции ООН против киберпреступности⁷ в целях повышения эффективности предупреждения и борьбы с киберпреступностью, укрепления международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, включая отмывание денег, коррупцию, террористические акты, торговлю людьми, незаконный ввоз мигрантов, незаконное изготовление и оборот огнестрельного оружия, его составных частей, компонентов и боеприпасов к нему, незаконный оборот наркотиков и незаконный оборот культурных ценностей. Конвенция ООН предусматривает унификацию правовой базы, регулирующей киберпреступления, формулирует ключевые понятия, такие как «информационно-коммуникационная система», «электронные данные» и др. Но, что не менее важно, Конвенция ООН содержит квалификацию (криминализацию) группы преступлений в сфере ИКТ, которую должны учитывать национальные законодательства государств-участниц, а именно:

- незаконный доступ к информационно-коммуникационной системе;
- незаконный перехват непубличных электронных сообщений;
- незаконное воздействие на информационно-коммуникационную систему;
- неправомерное использование устройств (программного обеспечения, электронной подписи и др.);
- подлог с использованием информационно-коммуникационной системы;
- хищение или мошенничество с использованием информационно-коммуникационной системы;
- преступления, связанные с размещением в Интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатацией;
- домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка;
- распространение интимных изображений без согласия;
- отмывание доходов от преступлений.

В 2024 году, по данным компаний, занимающихся кибербезопасностью, экономика киберпреступности стала третьей по величине экономикой в мире по объему ВВП. Киберпреступность стала одной из сложных проблем, глобальным вызовом как международному сообществу, так и национальным правовым порядкам в силу стремительного развития информационных и коммуникационных

технологий. Киберпреступность стала ключевым элементом системы обеспечения кибербезопасности, на которую оказывают влияние такие факторы, как растущая геополитическая напряженность, быстрое внедрение новых технологий, что приводит к появлению новых уязвимостей, росту числа киберпреступлений, а также отсутствию унификации нормативных требований в сфере кибербезопасности в международном масштабе. Эти проблемы усугубляются растущим дефицитом квалифицированных кадров, что крайне затрудняет эффективное управление киберрисками⁸.

Ввиду трансграничного характера и технической сложности совершаемых киберпреступлений, их расширяющегося разнообразия, которое следует за неукротимым развитием современных технологий, требуются унификация подхода к квалификации киберпреступлений и расширение международного сотрудничества в сфере противодействия киберпреступности, выработка согласованного правового механизма борьбы с ней.

Список источников

1. Filippov V.M. The Cyber Economy: Opportunities and Challenges for Artificial Intelligence in the Digital Workplace / V.M. Filippov A.A. Chursin, Ju.V. Ragulina, E.G. Popkova. Springer, 2020. 337 p.
2. Глушков В.М. Что такое ОГАС? / В.М. Глушков, В.Я. Валах. Москва: Наука, 1981. 160 с. URL: https://archive.org/details/chto_takoe_OGAS/page/5/mode/2up?q=кибернетика+экономика (дата обращения: 12.01.2025).
3. Степанов Д.А. Киберэкономика как результат цифровой модернизации современной экономики: эпоха технологий индустрии 4.0 / Д.А. Степанов // Экономика и социум: современные модели развития. 2020. Т. 10. № 3. С. 271–288.
4. Тонкогонов А.В. Киберэкономика – феномен XXI века / А.В. Тонкогонов // Закон и право. 2024. № 8. С. 94–97.
5. Бартош А. Кибернетическая экономика как фактор развития / А. Бартош // Независимая газета. 2023. 14 декабря. URL: https://nvo.ng.ru/concepts/2023-12-14/1_1266_factor.html (дата обращения: 12.01.2025).
6. Ведута Е. Цифровая экономика приведет к экономической киберсистеме // Международная жизнь. 2017. № 10. URL: <https://interaffairs.ru/jauthor/material/1926> (дата обращения: 12.01.2025).
7. Kianpour M. Systematically Understanding Cybersecurity Economics: A Survey / M. Kianpour, S. Kowalski, H. Overby // Sustainability. 2021. № 13(24). URL: <https://www.researchgate.net/publication/356987272> (дата обращения: 12.01.2025).
8. Карцхия А.А. Правовые аспекты современной кибербезопасности и противодействия киберпреступности / А.А. Карцхия, Г.И. Макаренко // Вопросы кибербезопасности. 2023. № 1(53). С. 28–44.
9. Nir H. A Global Regime for Cybersecurity and the Obstacles to Future Progress / H. Nir, M. Eviatar // Global Governance. 2024. № 30. P. 13–40. URL: <https://ssrn.com/abstract=4842370> (дата обращения: 10.12.2024).

⁸ Global Cybersecurity Outlook 2025, WEF January 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата обращения: 31.01.2025).

10. Ефремова И.А. Киберпространство как новая среда преступности / И.А. Ефремова, А.Б. Смушкин, А.Г. Донченко, П.А. Матушкин // Вестник Томского государственного университета. 2021. № 472. С. 248–256.

11. Никульченкова Е.В. Проблемы противодействия киберпреступности в России / Е.В. Никульченкова // Психопедагогика в правоохранительных органах. 2023. Т. 28. № 3(94). С. 345–352.

12. Handbook on the Language of Cybercrime. Comprehensive Study on Cybercrime / M.S. Boyd (eds.). 2020. URL: <https://www.researchgate.net/publication> (дата обращения: 20.12.2024).

13. Проблемы противодействия киберпреступности: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. 146 с.

14. The Palgrave Handbook of International Cybercrime and Cyberdeviance / T.J. Holt, A.M. Bossler (eds.). 2020. URL: https://doi.org/10.1007/978-3-319-78440-3_1 (дата обращения: 10.01.2025).

15. Международная информационная безопасность: подходы России / Отв. ред. А.В. Крутских, Е.С. Зиновьева. Москва, 2021. URL: <https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse> (дата обращения: 20.12.2024).

16. Стратегии кибербезопасности: аналитический отчет // Центр InfoWatch. 2022. URL: infowatch.ru/analytics (дата обращения: 10.01.2025).

17. Карабеков К.О. Понятие киберпреступности в Российской Федерации и Республике Казахстан / К.О. Карабеков // Известия Юго-Западного государственного университета. Серия «История и право». 2022. Т. 12. № 5. С. 99.

Referencis

1. Filippov V.M. The Cyber Economy: Opportunities and Challenges for Artificial Intelligence in the Digital Workplace / V.M. Filippov A.A. Chursin, Ju.V. Ragulina, E.G. Popkova. Springer, 2020. 337 p.
2. Glushkov V.M. Chto takoe OGAS? [What is OGAS?] / V.M. Glushkov, V.Ya. Valakh. Moscow: Nauka Publ., 1981. 160 s. URL: https://archive.org/details/chto_takoe_OGAS/page/5/mode/2up?q=Cybernetics+economics (date of request: 12.01.2025) (in Russian).
3. Stepanov D.A. Kiberekonomika kak rezul'tat cifrovoj modernizacii sovremennoj ekonomiki: epoha tekhnologij industrii 4.0 [Cybereconomics as a Result of Digital Modernization of the Modern Economy: The Era of Industry 4.0 Technologies] / D.A. Stepanov // Ekonomika i socium: sovremennye modeli razvitiya – Economics and Society: Modern Models of Development. 2020. Vol. 10. № 3. S. 271–288 (in Russian).
4. Tonkogonov A.V. Kiberekonomika – fenomen XXI veka [Cybereconomics – a Phenomenon of the 21st Century] / A.V. Tonkogonov // Zakon i pravo – Law and Right. 2024. № 8. S. 94–97 (in Russian).
5. Bartosh A. Kiberneticheskaya ekonomika kak faktor razvitiya [Cybernetic Economics as a Factor of Development] / A. Bartosh // Nezavisimaya Gazeta – Independent Newspaper. December 14, 2023. URL: https://nvo.ng.ru/concepts/2023-12-14/1_1266_factor.html (date of request: 12.01.2025) (in Russian).
6. Veduta E. Cifrovaya ekonomika privedet k ekonomicheskoj kibersisteme [The Digital Economy Will Lead to an Economic Cybersystem] / E. Veduta // Mezhdunarodnaya zhizn' – International Life. 2017. № 10. URL: <https://interaffairs.ru/jauthor/material/1926> (date of request: 12.01.2025) (in Russian).
7. Kianpour M. Systematically Understanding Cybersecurity Economics: A Survey / M. Kianpour, S. Kowalski, H. Overby // Sustainability. 2021. № 13(24). URL: <https://www.researchgate.net/publication/356987272> (date of request: 12.01.2025).
8. Kartskhiya A.A. Pravovye aspekty sovremennoj kiberbezopasnosti i protivodejstviya kiberprestupnosti [Legal Aspects of Modern Cybersecurity and Countering Cybercrime] / A.A. Kartskhiya, G.I. Makarenko // Voprosy kiberbezopasnosti – Cybersecurity Issues. 2023. № 1(53). S. 28–44 (in Russian).
9. Nir H. A Global Regime for Cybersecurity and the Obstacles to Future Progress / H. Nir, M. Eviatar // Global Governance. 2024. № 30. P. 13–40. URL: <https://ssrn.com/abstract=4842370> (date of request: 10.12.2024).
10. Efremova I.A. Kiberprostranstvo kak novaya sreda prestupnosti [Cyberspace as a New Crime Environment] / I.A. Efremova, A.B. Smushkin, A.G. Donchenko, P.A. Matushkin // Vestnik Tomskogo gosudarstvennogo universiteta – Bulletin of Tomsk State University. 2021. № 472. S. 248–256 (in Russian).
11. Nikulchenkova E.V. Problemy protivodejstviya kiberprestupnosti v Rossii [Problems of Countering Cybercrime in Russia] / E.V. Nikulchenkova // Psihopedagogika v pravoohranitel'nyh organah – Psychopedagogy in Law Enforcement Agencies. 2023. Vol. 28. № 3(94). S. 345–352 (in Russian).
12. Handbook on the Language of Cybercrime. Comprehensive Study on Cybercrime / M.S. Boyd (eds.). 2020. URL: <https://www.researchgate.net/publication> (date of request: 20.12.2024).
13. Problemy protivodejstviya kiberprestupnosti: materialy II Mezhdunarodnoj nauchno-prakticheskoy konferencii (Moskva, 26 aprelya 2024 goda) [Problems of Countering Cybercrime: Proceedings of the II International Scientific Conferencepractical Conference (Moscow, April 26, 2024)] / Under the general editorship of O.Yu. Antonov, E.B. Khatov. Moscow: Moscow Academy of the Investigative Committee named after A. Ya. Sukharev, 2024. 146 s. (in Russian).
14. The Palgrave Handbook of International Cybercrime and Cyberdeviance / T.J. Holt, A.M. Bossler (eds.). 2020. URL: https://doi.org/10.1007/978-3-319-78440-3_1 (date of request: 10.01.2025).
15. Mezhdunarodnaya informacionnaya bezopasnost': podhody Rossii [International Information Security: Russia's Approaches] / Ed. by A.V. Krutskikh, E.S. Zinoviev. Moscow, 2021. URL: <https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse> (date of request: 12.20.2024) (in Russian).
16. Стратегии кибербезопасности: аналитический отчет [Cybersecurity Strategies: An Analytical Report] // InfoWatch Center. 2022. URL: infowatch.ru/analytics (date of request: 10.01.2025).
17. Karabekov K.O. Ponyatie kiberprestupnosti v Rossijskoj Federacii i Respublike Kazahstan [The Concept of Cybercrime in the Russian Federation and the Republic of Kazakhstan] / K.O. Karabekov // Izvestiya YUgo-Zapadnogo gosudarstvennogo universiteta. Seriya «Istoriya i pravo» – Proceedings of the Southwestern State University. The Series «History and Law». 2022. Vol. 12. № 5. S. 99 (in Russian).

Will Lead to an Economic Cybersystem] / E. Veduta // Mezhdunarodnaya zhizn' – International Life. 2017. № 10. URL: <https://interaffairs.ru/jauthor/material/1926> (date of request: 12.01.2025) (in Russian).

7. Kianpour M. Systematically Understanding Cybersecurity Economics: A Survey / M. Kianpour, S. Kowalski, H. Overby // Sustainability. 2021. № 13(24). URL: <https://www.researchgate.net/publication/356987272> (date of request: 12.01.2025).

8. Kartskhiya A.A. Pravovye aspekty sovremennoj kiberbezopasnosti i protivodejstviya kiberprestupnosti [Legal Aspects of Modern Cybersecurity and Countering Cybercrime] / A.A. Kartskhiya, G.I. Makarenko // Voprosy kiberbezopasnosti – Cybersecurity Issues. 2023. № 1(53). S. 28–44 (in Russian).

9. Nir H. A Global Regime for Cybersecurity and the Obstacles to Future Progress / H. Nir, M. Eviatar // Global Governance. 2024. № 30. P. 13–40. URL: <https://ssrn.com/abstract=4842370> (date of request: 10.12.2024).

10. Efremova I.A. Kiberprostranstvo kak novaya sreda prestupnosti [Cyberspace as a New Crime Environment] / I.A. Efremova, A.B. Smushkin, A.G. Donchenko, P.A. Matushkin // Vestnik Tomskogo gosudarstvennogo universiteta – Bulletin of Tomsk State University. 2021. № 472. S. 248–256 (in Russian).

11. Nikulchenkova E.V. Problemy protivodejstviya kiberprestupnosti v Rossii [Problems of Countering Cybercrime in Russia] / E.V. Nikulchenkova // Psihopedagogika v pravoohranitel'nyh organah – Psychopedagogy in Law Enforcement Agencies. 2023. Vol. 28. № 3(94). S. 345–352 (in Russian).

12. Handbook on the Language of Cybercrime. Comprehensive Study on Cybercrime / M.S. Boyd (eds.). 2020. URL: <https://www.researchgate.net/publication> (date of request: 20.12.2024).

13. Problemy protivodejstviya kiberprestupnosti: materialy II Mezhdunarodnoj nauchno-prakticheskoy konferencii (Moskva, 26 aprelya 2024 goda) [Problems of Countering Cybercrime: Proceedings of the II International Scientific Conferencepractical Conference (Moscow, April 26, 2024)] / Under the general editorship of O.Yu. Antonov, E.B. Khatov. Moscow: Moscow Academy of the Investigative Committee named after A. Ya. Sukharev, 2024. 146 s. (in Russian).

14. The Palgrave Handbook of International Cybercrime and Cyberdeviance / T.J. Holt, A.M. Bossler (eds.). 2020. URL: https://doi.org/10.1007/978-3-319-78440-3_1 (date of request: 10.01.2025).

15. Mezhdunarodnaya informacionnaya bezopasnost': podhody Rossii [International Information Security: Russia's Approaches] / Ed. by A.V. Krutskikh, E.S. Zinoviev. Moscow, 2021. URL: <https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse> (date of request: 12.20.2024) (in Russian).

16. Стратегии кибербезопасности: аналитический отчет [Cybersecurity Strategies: An Analytical Report] // InfoWatch Center. 2022. URL: infowatch.ru/analytics (date of request: 10.01.2025).

17. Karabekov K.O. Ponyatie kiberprestupnosti v Rossijskoj Federacii i Respublike Kazahstan [The Concept of Cybercrime in the Russian Federation and the Republic of Kazakhstan] / K.O. Karabekov // Izvestiya YUgo-Zapadnogo gosudarstvennogo universiteta. Seriya «Istoriya i pravo» – Proceedings of the Southwestern State University. The Series «History and Law». 2022. Vol. 12. № 5. S. 99 (in Russian).

