Научная статья
УДК 343.985.7:[002:004](470)

Зарина Ирековна Харисова
Уфимский юридический институт МВД России, Уфа, Россия, zarinaid@mail.ru, ORCID 0000-0002-3902-3459

ГЕНЕЗИС ПРЕСТУПНОСТИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ЕЕ ДЕТЕРМИНАНТЫ

Аннотация. Статья посвящена исследованию генезиса преступности в сфере компьютерной информации как социально-правового явления и феномена правовой действительности с точки зрения системно-исторического подхода. Проведенный анализ позволил рассмотреть этапы развития и современное состояние компьютерной преступности, а также возможные направления ее трансформации с целью выявления наиболее перспективных методов предотвращения противоправных деяний, а также своевременного принятия законодательных, административных и иных предупреждающих мер. Сделан вывод, что появление новых форм преступности в сфере компьютерной информации будет обусловлено сложным взаимодействием технологических, социальных, экономических и политических факторов, а основным механизмом противодействия деструктивным формам в исследуемой сфере станут LegalTech-инструменты в виде программно-технических средств обеспечения юридической деятельности на базе стека индустрии Web 4.0, представленного технологиями искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных, Интернета вещей, а также виртуальной и дополненной реальности.

Ключевые слова: расследование преступлений, тенденции преступности, цифровая криминалистика, преступления в сфере компьютерной информации, киберпреступность, метапреступность, метавселенная, LegalTech, CrimeTech, DeepTech

Для **цитирования:** Харисова З. И. Генезис преступности в сфере компьютерной информации и ее детерминанты // Общество, право, государственность: ретроспектива и перспектива. 2025. № 1 (21). С. 57–65.

Original article

Zarina I. Kharisova
Ufa Law Institute Of The Ministry of Internal Affairs of Russia, Ufa, Russia, zarinaid@mail.ru, ORCID 0000-0002-3902-3459

GENESIS OF CYBERCRIME AND ITS DETERMINANTS

Abstract. The article is devoted to the study of the genesis of crime in the sphere of computer information as a socio-legal manifestation and a phenomenon of legal reality from the point of view of a systematic historical approach. The analysis made it possible to consider the stages of development and the current state of computer crime, as well as possible directions for its transformation in order to identify the most promising methods of preventing illegal acts, as well as the timely adaptation of legislative, administrative and other preventive measures. It is concluded that the emergence of new forms of cybercrime will be due to the complex interaction of technological, social, economic and political factors, and the main mechanism for counteracting destructive forms in the area under study will be LegalTech tools in the form of software and hardware to support legal activities based on Web 4.0 industry stack, represented by artificial intelligence technologies, distributed registry, ultra-high data transmission, the Internet of things, as well as virtual and augmented reality.

Keywords: crime investigation, crime trends, digital forensics, computer information crimes, cybercrime, metacrime, metaverse, LegalTech, CrimeTech, DeepTech

For citation: Kharisova Z. I. Genesis of cybercrime and its determinants // Society, law, statehood: retrospective and perspective. 2025. № 1 (21). P. 57–65. (In Russ.)

Введение

Современный этап общественного развития характеризуется переходом к информационному обществу. Развитие кибернетики, разработка и совершенствование технических устройств, внедрение информационно-телекоммуникационных технологий (далее – ИТТ) в большинство сфер жизнедеятельности человека привели к глобальной информатизации, обусловленной необходимостью обработки, хранения и анализа значительных объемов цифровых данных. ИТТ, являясь потенциальным инструментом содействия общественному прогрессу, одновременно создают широкие возможности для противоправной деятельности. Их использование преступниками способствует не только диверсификации преступных проявлений и эскалации их масштабов, но и деструктивному воздействию на общество, государство и его институты, а также коммерческие организации.

В контексте снижения потенциала использования ИТТ в целях совершения преступлений представляется необходимым исследование генезиса преступности в сфере компьютерной информации и ее основных детерминант. Использование системно-исторического подхода при анализе позволит рассмотреть не только этапы развития указанного вида преступности, но и современное состояние, а также возможные направления его трансформации с целью выявления наиболее перспективных (предикативных) методов предотвращения противоправных деяний, принятия предупреждающих мер, направленных на сокращение как существующих, так и потенциально возможных правонарушений.

Методы

В процессе исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), общенаучных (анализ, синтез, системный (системно-исторический) и системно-структурный подходы), частнонаучных (статистический, кибернетический, исторический), а также специальных методов (формально-юридический, сравнительно-правовой и предикативной аналитики). Применение указанных методов позволило провести обобщение и анализ эмпирического материала, определить перспективные направления дальнейших исследований в области предупреждения и расследования преступлений в сфере компьютерной информации.

Результаты

Преступления в сфере компьютерной информации (далее – преступления в СКИ) – это законодательное определение преступных деяний, предусмотренных главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ), объединяющей ст.ст. 272, 272.1, 273, 274, 274.1, 274.2. При этом имеется ряд схожих с ними форм девиантного поведения, именуемых как информационные компьютерные преступления и криминализированных в российском уголовном праве в соответствии с п. «г» ч. 3 ст. 158, ст. 159.3, 159.6, п. «в» ч. 3 и п. «в» ч. 5 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222.1, п. «в» ч. 3 и п. «в» ч. 5 ст. 222.2, п. «д» ч. 2 ст. 230, п. «г» ч. 2 ст. 242.2 УК РФ. Существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), рост их доли в общем числе преступлений, совершаемых с использованием ИТТ, крайне низкая раскрываемость указанного вида преступных деяний, а также рост утечек конфиденциальных данных, способный нанести существенный ущерб как отдельным гражданам государства, так и объектам критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ), оборонно-промышленного комплекса и смежных отраслей промышленности, говорят о том, что проводимое исследование является довольно актуальной задачей. Существенное негативное влияние на обстановку в указанной сфере оказыва-

ет сложившаяся международная ситуация, связанная с деятельностью транснациональных организованных преступных групп, нацеленных на хищение персональных данных граждан нашей страны, их неправомерное использование и распространение (ст. 272.1 УК РФ). Отдельная проблема заключается в противоправном применении ИТТ организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (далее – ПО) (ст. 273 УК РФ), фишинговые сайты и специальные технические средства. Кроме того, довольно часто нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и инфокоммуникационных сетей приводит к тяжким последствиям или создает угрозу их наступления (ст. 274 УК РФ). В связи с этим необходимо создание надежного барьера противодействия преступлениям именно в сфере компьютерной информации, а также выявление возможных направлений ее трансформации в будущем.

Современное право направлено на урегулирование вновь появляющихся форм отношений практически всех сфер деятельности человека, где объектами, субъектами, а порой и средствами все чаще выступают высокие технологии, что закономерно формирует новый вид права, именуемый высокотехнологичным и представляющий собой логистичный, наукоемкий и технологичный регулятор общественных отношений, который не только контролирует вновь возникающие отношения, связанные с высокими технологиями, но и активно использует их в правоприменении [1, с. 168]. Возникновение новых субъектов права, объектов регулирования и высокотехнологичных средств совершения преступлений в основном вынуждает законодателей принимать меры по разработке нормативных правовых актов, регулирующих новые правоотношения. Однако хорошей практикой является рассмотрение генезиса того или иного явления и его основных детерминант в целях выявления наиболее перспективных методов предотвращения нежелательных последствий в будущем, что возможно при проведении анализа с использованием системного подхода.

Наиболее распространенными разновидностями системного подхода в науке, которыми активно пользуются в естествознании, являются: системно-элементный (выявление элементов, входящих в исследуемую систему); системно-структурный (выявление взаимосвязей между составляющими систему элементами); системно-функциональный (выявление функций, выполняющихся системой); системно-коммуникационный (определение взаимосвязей между входящими в систему элементами и внешней средой) и системно-исторический (исследование генезиса системы и ее динамики как изучение пройденных этапов ее развития, современного состояния, а также возможных перспектив развития) [2, с. 70].

Под генезисом в науке понимается описание происхождения, возникновения, становления и развития различных природных, социальных и иных явлений [3, с. 20]. Генезис большинства явлений интересовал науку начиная с античных времен. Зачастую его рассмотрение получало научное обоснование в эволюционных теориях междисциплинарного и общенаучного характера. В современной науке объяснение генезиса любой природы связывается преимущественно с принципами глобального эволюционизма[1]. В связи с этим вполне целесообразно изучение генезиса преступности в СКИ как социально-правового явления и феномена правовой действительности с точки зрения системно-исторического подхода. Это позволит получить дополнительные сведения не только о природе юридических приемов создания, реализации и толкования норм права, но и сформулировать новые правовые концепции, конструкции и потенциально возможные формы преступности в будущем.

[1] Новейший философский словарь / сост. и гл. н. ред. Грицанов А. А. 3-е изд., испр. Мн. : Книжный Дом, 2003. С. 819.

Рассматривая основные составляющие ядра пятого индустриального технологического уклада (1980–2020 гг.), наибольшее внимание уделим таким областям науки, как электроника и прикладная информатика, регулирующим процесс изучения информационных технологий (далее – ИТ), телекоммуникаций, методов обеспечения информационной безопасности, защиты информации, функционирования различных технических устройств и т. п. Наступление шестого цикла Кондратьева [4, с. 5] как нового индустриального уклада связывают с развитием биотехнологий, генной инженерии и, безусловно, ИТТ, включая современный стек (от англ «stack» – набор инструментов или ИТ, используемых для реализации проекта) индустрии Web 4.0, представленный технологиями искусственного интеллекта, распределенного реестра (блокчейн), сверхвысокой передачи данных (5G), Интернета вещей (IoT), а также виртуальной (AR) и дополненной реальности (VR).

Основным преимуществом новой эпохи когнитивных технологий выступают глобализация, скорость связи и перемещения, постоянное повышение уровня комфорта жизни населения[1] с задействованием вышеперечисленных технологий. Вместе с тем уже на постоянной основе возникают проблемы, связанные с обеспечением безопасности эксплуатации ИТТ. В этой связи наряду с генезисом компьютерной преступности необходимо рассмотрение основных ее детерминант как комплекса социальных явлений, совместное действие которых порождает противоправные деяния.

Аналогично тому, как интенсивное развитие промышленности породило экологические проблемы планетарного масштаба, а достижения в области ядерной физики создали угрозу глобальной ядерной войны, на сегодняшний день можно констатировать, что информатизация является причиной таких негативных последствий, как возросший уровень преступных деяний, совершаемых с использованием ИТТ. Появление «информационного оружия» как следствие развития ИТ по степени опасности может превзойти ядерное оружие, поскольку даже запуск средств массового поражения в ряде случаев осуществляется командой в автоматизированной системе боевого управления.

Анализ криминогенной обстановки в Российской Федерации свидетельствует о том, что преступность в сфере компьютерной информации стала одним из ключевых деструктивных факторов общественного развития. Динамичный количественный рост преступности[2], сопровождающийся ее качественными изменениями, создает реальную угрозу социально-экономическому развитию, стабильности государственности и национальной безопасности. Криминализация использования ИТТ усугубляется активным вовлечением в нее организованных преступных групп, которые постоянно ищут новые способы совершения преступлений, используя передовые достижения науки и техники. По этой причине итогом пятилетней работы государств-членов ООН стало одобрение разработанной по инициативе Российской Федерации Конвенции против киберпреступности, являющейся первым универсальным договором, предусматривающим укрепление международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием ИТТ[3]. Проект

[1] История науки, техники и транспорта : учебник для вузов / В. В. Фортунатов [и др.] ; под общей редакцией В. В. Фортунатова. М. : Издательство Юрайт, 2024. С. 14.

[2] Комплексный анализ состояния преступности в Российской Федерации и ожидаемые тенденции ее развития : аналитический обзор / Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации / М. В. Гончарова, М. М. Бабаев, Р. В. Черкасов [и др.]. М. : ФГКУ «ВНИИ МВД России», 2024. С. 55.

[3] Конвенция Организации Объединенных Наций против киберпреступности: укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме от 27 ноября 2024 г. A/79/460 // Официальный сайт ООН. URL: https://documents.un.org/doc/undoc/gen/n24/372/06/pdf/n2437206.pdf (дата обращения: 26.01.2025).

резолюции принятого документа подчеркивает особую важность борьбы с указанным видом преступлений, поскольку они зачастую связаны с отмыванием денег, террористическими и экстремистскими актами, неправомерным использованием криптовалют, коррупцией, торговлей людьми, незаконным изготовлением и оборотом оружия, наркотических и психотропных веществ и пр., а статья 55 предусматривает проведение каждым отдельно взятым государством анализа тенденций, характеризующих совершаемые на их территории компьютерные преступления.

Рассматривая феномен преступности в СКИ с исторической точки зрения, выделим несколько ключевых факторов (условных этапов), которые способствовали ее широкому распространению и развитию. Одной из очевидных причин стало появление в 1940–1960-е гг. первых электронно-вычислительных машин, которые в большей степени эксплуатировались на предприятиях. Это стало отправной точкой развития таких примитивных деструктивных форм, как нарушение правил хранения и обработки информационных ресурсов и несанкционированный доступ к защищаемым данным [5, с. 11].

Последующее массовое распространение персональных компьютеров в 1970–1980-е гг. определило появление первых злоумышленников, взламывающих компьютерные системы и осуществляющих доступ к личным данным пользователей, и преимущественно движимых любопытством, желанием исследовать новые для них возможности использования ИТТ. Указанный этап характеризуется постепенным распространением компьютерных сетей, что обусловило распространение вирусного программного обеспечения ПО и зарождение первых сетевых атак [6, с. 12].

Глобализация сети Интернет в 1990–2000 гг. создала единое информационное пространство, доступное практически каждому пользователю, что обусловило появление таких актуальных даже на сегодняшний день видов преступлений, как фишинг, распространение вредоносного ПО в телекоммуникационных сетях, атаки на веб-ресурсы [7, с. 17], кража данных с электронных банковских счетов и пр.

Следующий этап связан с использованием мобильных средств связи, веб-сайтов и социальных сетей в 2000–2020 гг, Так, смартфоны с возможностью скоростной передачи данных стали неотъемлемой частью жизни общества, что привело к массовому их использованию и, как следствие, распространению преступлений в СКИ в геометрической прогрессии [8, с. 35].

Современный этап характеризуется развитием сложных и целевых кибератак, направленных на проникновение в конкретные системы и кражу конфиденциальной информации отдельно взятой личности. Также широко распространяется возможность использования искусственного интеллекта для автоматизации атак, синтетической генерации контента в целях установления с жертвой доверительных отношений и последующего совершения противоправных деяний или дезинформации общества. Кроме указанных явлений, широко распространяются различные цифровые фиатные активы, позволяющие анонимно осуществлять финансирование противоправной деятельности, атаки на IoT-устройства [9, с. 2].

Отдельного внимания заслуживает появление метавселенных, которые создают новые возможности совершения преступлений в СКИ, таких как мошенничество с цифровыми аватарами пользователей, виртуальное насилие, кража виртуальных активов и пр., а также взлом широко внедряемых в различные сферы биометрических систем распознавания и нейроинтерфейсов.

История развития криминалистики, как и любой другой науки, представляет собой систему фактов, позволяющих не только проследить закономерности становления научного знания, но и определить пути дальнейшего его совершенствования [10, с. 47]. Сегодня генезис ИТТ рассматривается как основополагающий институт современности. Предикативный анализ, обеспечиваемый уже типовыми технологическими

решениями, построенными на базе искусственного интеллекта, облачных технологий, распределенных баз данных и пр., уже сегодня становится частью общественного сознания [11, с. 38].

В будущем появление новых форм преступлений в СКИ будет обусловлено сложным взаимодействием технологических, социальных, экономических и политических факторов. Рассмотрим основные ее детерминанты. Так, среди технологических факторов стоит отметить возможности генеративного искусственного интеллекта для создания реалистичных фишинговых сообщений (дипфейков) и разнообразного синтетического контента, сложно поддающихся анализу и их выявлению. Кроме того, увеличивается частота роста использования нейросетей для разработки сложного и адаптивного вредоносного ПО, автоматизации процессов кибератак, управления трудно обнаруживаемыми ботнетами. При этом большинство имеющихся на сегодняшний день технологий и методов шифрования данных позволят обойти развивающиеся технологии квантовых вычислений, а увеличение количества IoT-устройств и API-интерфейсов в области прикладного программирования создаст множество дополнительных уязвимостей и точек воздействия для преступников. Среди технологических факторов все чаще выделяют появление еще сложно воспринимаемых в реальности, но распространяющихся в метапространстве, генерируемом с задействованием элементов дополненной реальности, преступных схем, связанных с виртуальными активами и цифровыми аватарами. Метавселенные порождают относительно новые виды преступных деяний (кража виртуальной собственности, идентификатора личности, виртуальный вандализм, кибербуллинг, виртуальные домогательства и насилие с использованием аватаров).

Постиндустриальная информационная среда обеспечивает широкие возможности для создания многочисленных и мощных баз данных, легкость распространения информации, простоту ее копирования, агрегирования и модификации, что способствует появлению новых информационных угроз для отдельно взятого человека [12, с. 90]. Соответственно, среди социальных факторов можно выделить увеличение зависимости общества от ИТТ, что делает его более уязвимым к атакам преступников, относительно низкий уровень грамотности населения в области ИТ, сложность восприятия принципов построения вновь возникающих технических средств и киберфизических систем, а также распространение деструктивных сведений в информационном пространстве и т. п.

Экономические факторы обусловлены увеличением объемов электронной торговли, развитием сервисов онлайн-банкинга и виртуальных финансовых инструментов, что создает новые платформы совершения преступлений в СКИ не только в «белом» Интернете, но и в даркнете.

Отдельного внимания заслуживают такие политические факторы, как использование кибератак в качестве инструмента для достижения стратегических целей. Так, например, осуществлять разведку и сбор информации все чаще приходится с задействованием широкого спектра ИТТ и технических средств, соответственно, усиление геополитической напряженности может приводить к росту кибершпионажа между государствами.

Нельзя оставить без внимания ряд организационных факторов, которые определяют недостаток квалифицированных специалистов в области ИТТ, цифровой криминалистики и обеспечения информационной безопасности, а также сложность расследования преступлений в СКИ, сбора и анализа цифровых доказательств, определения ответственности в информационном пространстве.

Все вышеперечисленные факторы создают сложную и довольно динамичную среду, в которой будут развиваться новые формы преступлений в СКИ в будущем. Одной из особенностей постнеклассической науки является интеграция гуманитарных, естественных и технических наук [13, с. 14], по этой причине предполагается, что для эффек-

тивной борьбы с преступностью в СКИ необходимы комплексные меры, включающие развитие ИТТ, усиление мер обеспечения информационной безопасности, повышение осведомленности населения и квалификации специалистов в области раскрытия и расследования рассматриваемого вида преступности, а также совершенствование правового регулирования отношений, возникающих в сфере информации, ИТ и защиты информации, налаживание международного сотрудничества. Однако базовым механизмом противодействия деструктивным формам в исследуемой области является разработка технических средств, широко освещаемых зарубежными источниками в доктринальной концепции «Юридические технологии» (описывающей систему знаний о юридико-технических средствах, приемах и способах применения, совершенствования и систематизации различных правовых инструментов) и именуемых LegalTech-инструментами (от англ. «legal technology» – технологичные решения в области информационно-технического обеспечения юридической деятельности) [14, с. 18]. Наряду с указанными средствами целесообразно развитие таких направлений системы «Юридических технологий», как CrimeTech (от англ. «crime technology» – современные решения на основе ИТТ, используемые в преступных целях) и DeepTech (от англ. «deep technology» – инновационные ИТТ, принятые на вооружение преступниками, но требующие значительных временных и экономических затрат для оказания противодействия им).

Таким образом, можно сделать вывод, что история становления преступности в СКИ является отражением развития ИТТ, причем каждый новый этап их развития позволял создавать новые возможности для совершения преступлений, что в свою очередь побуждало к разработке новых методов противодействия им. Анализ исторических факторов позволяет не только понять природу преступности в СКИ, но и ее тенденции с наиболее уязвимыми областями в целях разработки эффективных стратегий противодействия ей в будущем.

Заключение

Таким образом, основными причинами возникновения и широкого распространения преступности в СКИ являются повсеместный рост использования ИТТ и различных онлайн-сервисов, переход к цифровой экономике, развитие технических средств и технологий обезличивания в киберсреде и т. п. при сравнительно низком уровне цифровой грамотности населения и, как следствие, недостаточной защищенности личных данных пользователей. Существенной проблемой является использование интернет-пространства для политических и экономических манипуляций наравне с относительной легкостью анонимного совершения рассматриваемых преступлений и в большей части безнаказанности за совершенные деяния. Факторами, способствующими появлению новых форм преступности в СКИ, выступят: стабильное увеличение количества пользователей, применяющих ИТТ; широкое внедрение технологий искусственного интеллекта и квантовых вычислений в повседневную деятельность человека; развитие метавселенных, а также цифровых финансовых активов. Дальнейшая эволюция методов и способов совершения преступлений в СКИ будет обусловлена относительно легкой разработкой и внедрением ботнетов, в том числе на основе нейросетей для совершения кибератак, применением квантовых алгоритмов для взлома защищенных систем и методов социальной инженерии для манипуляции персональными данными граждан.

Проведенное исследование позволяет сделать вывод, что одним из перспективных направлений в системе юридических технологий является разработка программно-технических LegalTech-инструментов противодействия преступлениям в СКИ, которые должны учитывать не только текущие угрозы, но и новые, перспективные в плане появления, формы. Одной из основных задач, решаемых подобными системами, являются поиск, фиксация, анализ и интерпретация цифровых доказательств, а также автоматизация расследований и обеспечение целостности собранной информации, что позволя-

ет определить ключевым для ее реализации стек индустрии Web 4.0, представленным технологиями искусственного интеллекта, распределенного реестра, сверхвысокой передачи данных 5G, интернета вещей, а также виртуальной и дополненной реальности.

СПИСОК ИСТОЧНИКОВ

1. Пучков О. А. Право в зеркале высоких технологий: сравнительный анализ тенденций правового развития // Правовое государство: теория и практика. 2024. № 2. С. 163–172.

2. Отюцкий Г. П. Концепции современного естествознания. 2-е изд., перераб. и доп. М. : Издательство Юрайт, 2025. 447 с.

3. Петровская В. Н., Щепин В. И. Концепции современного естествознания: словарь терминов. Иркутск : Изд-во ИрГТУ, 2008. 104 с.

4. Sadovnichiy V. A., Akaev A. A., Davydova O. I. Modeling and Forecasting the Evolutionary Economic Development of the BRICS and G7 Countries in the First Half of the Twenty-First Century // Journal of Globalization Studies. 2024. Vol. 15. No. 2. P. 3–41.

5. Воробьева А. А., Пантюхин И. С. История развития программно- аппаратных средств защиты информации. СПб : Университет ИТМО, 2017. 62 с.

6. Tzavara V., Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review // Int. J. Inf. Secur. 2024. V. 23. P. 1–25.

7. Florido-Benitez L. The types of hackers and cyberattacks in the aviation industry // Transp. Secur. 2024. V. 17. P. 1–32.

8. Radoniewicz F. Cyberspace, cybercrime, cyberterrorism // Springer, Cham. 2024. V. 1. P. 33–51.

9. Lundberg E., Mozelius P. The potential effects of deepfakes on news media and entertainment // AI & Soc. 2024. V. 1. P. 1–12.

10. Эксархопуло А. А. Криминалистика: история и перспективы развития : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. М. : Издательство Юрайт, 2024. 167 с.

11. Сологубова Г. С. Составляющие цифровой трансформации : монография. М. : Издательство Юрайт, 2024. 147 с.

12. Малашенко А. В. Становление постиндустриальной цивилизации: от цифровизации до варварства : монография / А. В. Малашенко, Ю. А. Нисневич, А. В. Рябов. М. : Издательство Юрайт, 2024. 212 с.

13. Садохин А. П. Концепции современного естествознания. 2-е изд., перераб. и доп. М. : Юнити-Дана, 2006. 447 с.

14. Dariusz S., Mariusz Z. Legal Tech: Information technology tools in the administration of justice. Nomos Verlagsgesellschaft mbH & Co. KG. 2021. 665 p.

REFERENCES

1. Puchkov O. A. Law in the Mirror of High Technologies: A Comparative Analysis of Legal Development Trends // The Rule of Law: Theory and Practice. 2024. No. 2. P. 163–172. (In Russ.)

2. Otyutsky G. P. Concepts of Modern Natural Science. 2nd ed., revised and enlarged. M. : Yurait Publishing House, 2025. 447 p. (In Russ.)

3. Petrovskaya V. N., Shchepin, V. I. Concepts of Modern Natural Science: A Dictionary of Terms. Irkutsk : Irkutsk State Technical University Publishing House, 2008. 104 p.

4. Sadovnichiy V. A., Akaev A. A., Davydova O. I. Modeling and Forecasting the Evolutionary Economic Development of the BRICS and G7 Countries in the First Half of the Twenty-First Century // Journal of Globalization Studies. 2024. Vol. 15. No. 2. P. 3–41.

5. Vorobyova A. A., Pantyukhin I. S. History of the development of software and hardware for information security. St. Petersburg: ITMO University, 2017. 62 p. (In Russ.)

6. Tzavara V., Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review // Int. J. Inf. Secur. 2024. V. 23. P. 1–25.

7. Florido-Benitez L. The types of hackers and cyberattacks in the aviation industry // Transp. Secur. 2024. V. 17. P. 1–32.

8. Radoniewicz F. Cyberspace, cybercrime, cyberterrorism // Springer, Cham. 2024. V. 1. P. 33–51.

9. Lundberg E., Mozelius P. The potential effects of deepfakes on news media and entertainment // AI & Soc. 2024. V. 1. P. 1–12.

10. Eksarkhopulo A. A. Forensic science: history and development prospects: monograph / A. A. Eksarkhopulo, I. A. Makarenko, R. I. Zainullin. M. : Yurait Publishing House, 2024. 167 p. (In Russ.)

11. Sologubova G. S. Components of Digital Transformation: monograph. M. : Yurait Publishing House, 2024. 147 p. (In Russ.)

12. Malashenko A. V. Formation of Post-Industrial Civilization: from Digitalization to Barbarism : monograph / A. V. Malashenko, Yu. A. Nisnevich, A. V. Ryabov. M. : Yurait Publishing House, 2024. 212 p. (In Russ.)

13. Sadokhin A. P. Concepts of Modern Natural Science. 2nd ed., revised. and enlarged. M. : Unity-Dana, 2006. 447 p. (In Russ.)

14. Dariusz S., Mariusz Z. Legal Tech: Information technology tools in the administration of justice. Nomos Verlagsgesellschaft mbH & Co. KG. 2021. 665 p.

Информация об авторе:
Харисова З. И. – кандидат технических наук, доцент.

Information about the author:
Kharisova Z. I. – Candidate of Technology, Associate Professor.

Статья поступила в редакцию 27.01.2025; одобрена после рецензирования 31.01.2025; принята к публикации 21.03.2025.

The article was submitted 27.01.2025; approved after reviewing 31.01.2025; accepted for publication 21.03.2025.