Научная статья

УДК 343.9
EDN: DAMNJR

СОЦИАЛЬНАЯ ПРИРОДА ПРЕСТУПЛЕНИЯ В СФЕРЕ ЦИФРОВОЙ ИНФОРМАЦИИ

Ирина Владимировна Семёнова
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии, Санкт-Петербург, Россия
9053202867@mail.ru

Аннотация. Современные условия диктуют определенные правила развития государственной и общественной деятельности. Развитие технологического процесса оказало существенное влияние на формирование современной молодежи. Интернет, социальные сети, современные гаджеты прочно закрепились в нашей жизни. Изменения, происходящие в обществе, неизбежно затрагивают информационное поле и способы трансляции информации. Появление все большого объема информации, требующей соответствующего качества, повлекло трансформацию телекоммуникативных систем ее передачи. Автором проанализированы периоды развития систем передачи информации, взаимосвязь между развитием общественных отношений в сфере цифровой информации и совершенными преступлениями. Выделены факторы, отражающие социальную сущность преступления и оказывающие влияние на формирование преступности в данной сфере.

Ключевые слова: цифровая информация, системы передачи, статистика, преступление, общество, социальная сущность, факторы, развитие

Для цитирования: Семёнова И.В. Социальная природа преступления в сфере цифровой информации // Вестник Санкт-Петербургского военного института войск национальной гвардии. 2024. № 2 (27). С. 63–71. URL: https://vestnik-spvi.ru/2024/06/007.pdf. EDN: DAMNJR.

Original article

THE SOCIAL NATURE OF CRIME IN THE FIELD OF DIGITAL INFORMATION

Irina V. Semyonova
Saint-Petersburg Military Order of Zhukov Institute of the National Guard Troops, Saint-Petersburg, Russia
9053202867@mail.ru

Abstract. Modern conditions dictate certain rules for the development of state and public activities. The development of the technological process has had a significant impact on the formation of modern youth. The Internet, social networks, modern gadgets are firmly entrenched in our lives. The changes taking place in society inevitably affect the information field and the ways of broadcasting information. The appearance of an increasing volume of information requiring appropriate quality has led to the transformation of telecommunication systems for its transmission. The author analyzes the periods of development of information transmission systems, the relationship between the development of public relations in the field of digital information and committed crimes. The factors reflecting the social essence of the crime and influencing the formation of crime in this area are highlighted.

Keywords: digital information, transmission systems, statistics, crime, society, social essence, factors, development

For citation: Semyonova I.V. The social nature of crime in the field of digital information. Vestnik Sankt-Peterburgskogo voennogo instituta vojsk nacional'noj gvardii. 2024;2(27): 63–71. (In Russ.). Available from: https://vestnik-spvi.ru/2024/06/007.pdf. EDN: DAMNJR.

Введение

Государственная и общественная деятельность в современных условиях подвержена цифровизации, являющейся характерным признаком современности. В научной криминалистической литературе отмечалось, что Г. В. Лебниц в XVIII веке пророчил будущее за машинами, считая их

беспристрастными, современными и объективными средствами осуществления правосудия [4, С. 10; 6]. Развитие технологического процесса оказало существенное влияние на формирование современной молодежи. Интернет, социальные сети, современные гаджеты прочно закрепились в нашей жизни.

В эпоху стремительного развития технологий, цифровизация проникает во все сферы нашей жизни. Она обещает улучшить эффективность работы предприятий, повысить комфортность жизни граждан и дать мощный толчок для инноваций. Однако, как и любое мощное средство, цифровые технологии имеют и обратную сторону – они создают новые угрозы и способы для совершения преступлений.

Основные положения

Однако зарождение современных систем передачи информации произошло в Советском Союзе. Изначально появление сигнала, позволяющего передавать информацию, ввели в различные отрасли народного хозяйства, обеспечили общение населения путем развития телефонного, телеграфного сообщения, радио- и телевизионного вещания[1]. Сигнал передавался по средствам линии связи, которые на тот момент, да и еще долгое время, оставались в ведении государства. Доступность современных средств передачи информации была не повсеместной, в зависимости от финансовой обеспеченности.

Передача информации осуществлялась по различным линиям связи: общественные, внутриведомственные и внутрипроизводственные. За функционированием каждой из них Министерство связи СССР по поручению государственных органов осуществляло контроль.

Переформатирование и модификация линий связей началось после распада Советского Союза, с изменением общественных отношений изменилось и законодательство.

С появлением новой Конституции произошло упразднение коллективной собственности путем образования частной, государственной, муниципальной и иной (статья 8)[2].

Изменения, происходящие в обществе, неизбежно затрагивают информационное поле и способы трансляции информации. Появление все большого объема информации, требующей соответствующего качества, повлекло трансформацию телекоммуникативных систем ее передачи. Переход от государства в частный сектор данных линий передачи повлек поступление большого объема финансовых средств на их развитие и совершенствование. Стали появляться мобильные устройства, позволяющие разговаривать, передавать сообщения, со временем и фото, не по линии связи, а с помощью цифрового сигнала [2, С. 17].

Появление компьютеров и Интернета позволило развивать информационные технологии в условиях трансграничности и глобальности. Введение цифровых технологий во все сферы деятельности повлекло издание Доктрины[3], обобщающей теоретические положения в сфере информационной безопасности. На их основе был сформирован комплекс мер, осуществляющих правовое регулирование, определение предписаний и требований по пользованию системами, по передаче информации, одновременно с этим создание нормативной правовой базы, направленной на проведение оперативно-розыскных, следственных мероприятий в сфере цифровой информации [9; 8; 14].

В последнее время все чаще стало наблюдаться совершение противоправной деятельности, происходящее с применением технических средств, в частности Интернета и цифровых сетей передачи информации, программного обеспечения, вирусов, что негативным образом отражается на геополитической стабильности [3, С. 130].

Развитие и внедрение в общественную жизнь современных цифровых объектов создает предпосылки для развития и расширения круга составов преступления, несмотря на сложившуюся законодательную основу, регулирующую общественные отношения в сфере цифровой информации [11, С. 83].

---

[1] Постановление Совмина СССР от 27.05.1971 г. № 316 «Об утверждении Устава связи Союза ССР» // Свод законов СССР. 1990. Т. 8. 365 с.

[2] Конституция Российской Федерации: [принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.]. URL: https://base.garant.ru/10103000/ (дата обращения: 10.04.2023).

[3] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50, Ст. 7074.

Государство является гарантом информационной безопасности и приоритетным направлением среди национальных интересов[4], на что Президентом Российской Федерации В. В. Путиным было обращено особое внимание. Говоря о внедрении цифровых продуктов, Президент Российской Федерации конкретизировал, что доступ к полной информации о личных цифровых данных исключен для организаций, относящихся к банковской, предпринимательской сфере, тем самым исключается возможность оказания любого рода вмешательства[5].

Однако, исходя их статистических данных за 2021 и 2022 года о состоянии преступности с использованием информационно-телекоммуникативных технологий, можно наблюдать рост преступности.

По аналитическим данным Банка России, в банковской сфере противозаконную деятельность на себе ощущают граждане наиболее экономически активного возраста 25–64 года[6] (рисунок 1).

По данным МВД Российской Федерации, преступлений с использованием информационно-телекоммуникативных технологий в 2021 году составило 26,5 % от общего числа совершенных преступлений, что составило 271,1 тыс. зарегистрированных преступлений, в 2022 году – 42 % от общего числа, несмотря на то, что раскрываемость выросла на 4,4 %, в 2023 году – больше, чем в предыдущем на 29,7 %[7]. Данные цифры демонстрируют рост числа преступлений в данной сфере. При этом специалисты отмечают снижение числа преступлений, совершенных путем незаконного списания денежных средств с банковских карт, начиная с марта месяца 2022 года. Указанная дата не случайна, поскольку на территории Российской Федерации введены санкционные ограничения использования таких платежных систем, как Visa, Vastercard, Fppl – Google-, Samsung-Pay, у ряда коммерческих банков были отозваны лицензии Центральным банком Российской Федерации[8].

Следует сказать, что любые статистические данные необходимы для формирования представления о наличии, развитии преступности в той или иной сфере, определения ее географического расположения, определения стратегий борьбы и формирования превентивных мер. Исходя из латентности преступлений в сфере цифровой информации, их трансграничного характера, статистические данные могут быть неточными.

Существует множество факторов, влияющих на формирование сведений о преступности. Так, например, не каждая жертва заявит о совершенном в отношении нее преступлении. У начинающих market place, служб доставки, по сравнению с банками, информация, внесенная в приложение, не находится в полной безопасности. В результате хакерской атаки или по вине сотрудников, работающих с обработкой персональных данных, происходит их «утечка». В случае выявления, организация не спешит сообщать об этом в полицию, поскольку такая информация может не лучшим образом отразиться на их репутации. Незначительность наступивших последствий порождает нежелание граждан втягивать себя в процесс, связанный с расследованием преступления.

Отдельные преступления, как отмечается в научной литературе, попросту теряются на просторах Интернета [12, С. 13].

---

[4] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: https://pravo.gov.ru (дата обращения: 03.11.2023).

[5] Выступление Президента Российской Федерации на конференции // URL: https://yandex.ru/video/preview/?text=конференция%20по%20информационной%20безопасности%2012%20ноября%202021%20выступление%20путина&path=yandex_search&parent-reqid=1650960687784472-1119663258361221459 0-vla1-2882-vla-l7-balancer-8080-BAL-4183&from_type=vast&filmId=7693856425870508655 (дата обращения: 20.02.2024).

[6] Кибермошенничество: портрет пострадавшего Банк России // URL: https://cbr.ru/statistics/information_security/cyber_portrait/ (дата обращения: 02.04.2024).

[7] Статистические сведения о состоянии преступности в 2022 году // URL: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2022-godu (обращение 17.03.2023 г). Статистические сведения о состоянии преступности в 2023 году // URL: https://мвд.рф/news/item/47052005 (дата обращения: 02.04.2024).

[8] Сведения о проведении ликвидационных мероприятий в кредитных организациях с отозванными лицензиями на осуществление банковских операций (не исключенных из ЕГРЮЛ) по состоянию на 01.09.2023 // URL: https://cbr.ru/vfs/credit/likvidbase/likvid.pdf (дата обращения: 02.04.2024).

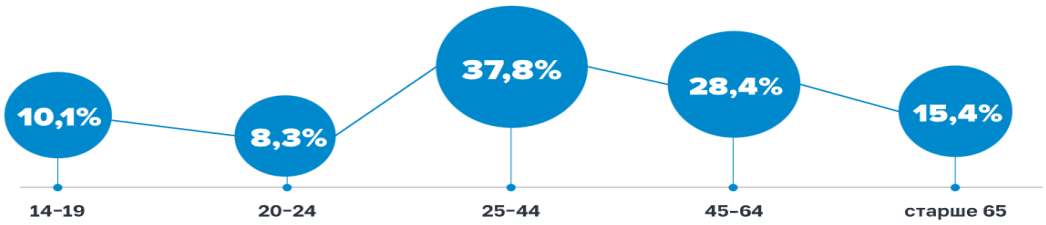

Рисунок – Экономически активный возраст

Figure – Economically active age

В связи с этим статистику представляется необходимо воспринимать как средство достижения общих целей, как информацию для разработки систем национальной безопасности, как сигнал, свидетельствующий об образовании новых видов и разновидности преступлений.

С появлением коронавирусной инфекцией и возникшей в мире пандемией были введены ограничения по передвижению населения, дистанционная работа в различных сферах, путем повсеместного использования сети Интернет. Практически все сферы (образование, здравоохранение, социальная, торговая, финансовая и многие другие) перешли на удаленную дистанционную работу, что сразу же нашло отражение в деятельности злоумышленников. Возросший объем цифровых данных в информационных системах является целью преступных действий.

Можно привести множество примеров совершения незаконных входов в инфраструктуру по всему миру с 2019 года. Так, например, в Аргентине при взломе банка данных были украдены все данные об удостоверениях личности населения. Введение цифровых способов работы правительства привело в греческом городе Салоники к параличу работы налоговиков, транспортной системы, после хакерской атаки на IT-системы.

Интернет-торговые платформы на территории Российской Федерации предоставили возможность незаконного получения доступа к персональным сведениям с помощью использования бонета[9].

Трансграничный характер преступлений свидетельствует о необходимости использования комплексного подхода в борьбе с цифровыми преступлениями, о чем свидетельствует практика. Так, в результате поступившей из США информации при взаимодействии Следственного департамента МВД Российской Федерации в результате проведенных оперативно-следственных мероприятий в России пресечена деятельность хакерской группы[10].

Современные способы совершения преступных действий сменяют устаревшие, такие как финансовые пирамиды, рейдерские захваты. Современные преступники для достижения своих целей используют современные достижения техники в области IT-разработок [16, С. 41–42; 15; 5; 13].

Мы стоим на пороге эпохальных перемен, когда предстоящая интеллектуальная революция обещает преобразить наш мир, позволяя преодолеть текущие вызовы мышления и развития общества. Это станет новым витком в эволюции человеческого разума, расширяя границы его применения в разнообразных аспектах нашей жизни [19, С. 26].

Цифровая преступность является новым вызовом для правоохранительных органов.

Быстрый прогресс в области искусственного интеллекта (далее – ИИ) является серьезным испытанием для людей, так как современная культура не успевает адаптироваться к изменениям, которые он вносит в нашу жизнь. Эти изменения уже заметны [7, С. 103]. Прежде всего, следует отметить рост числа преступлений в данной сфере. Взломы баз данных, фишинговые атаки, распространение вредоносного программного обеспечения – это лишь верхушка айсберга. С появлением криптовалют злоумышленники получили возможность осуществлять финансовые операции анонимно, что значительно усложняет процесс их выявления и пресечения.

[9] В России зафиксировали крупнейшую ботнет-атаку на ритейл // URL: https://www.fishnet.ru/news/novosti_otrasli/v-rossii-zafiksirovali-krupneyshuyu-botnet-ataku-na-riteyl/ (дата обращения 1.10.2023).

[10] Пресечена противоправная деятельность членов организованного преступного сообщества // URL: http://www.fsb.ru/fsb/press/message/single.html!id=10439388@fsbMessage.html (дата обращения 12.04.2024).

Е. В. Виноградова, С. И. Захарцев пишут, что современные разработки в IT-сфере, «современные технологии, в том числе медицинские, информационные и др., создавая невероятные возможности для человека, ставят перед человечеством ряд проблем, решение которых предполагает выход на новые формы правового знания, существующего на стыке философских, этических, нравственных основ, без этого, очевидно, невозможно противостоять глобальным угрозам, которые стоят перед всем человечеством» [1, С. 221]. С одной стороны, появление и развитие ИИ способствует быстрому решению задач интеллектуального характера, с которыми человеческому разуму потребуется продолжительное время [10, С. 180]. Так, с развитием нейросетевых генеративных моделей (образы изображений, тексты) появляется возможность создавать поддельные материалы высокой достоверности – так называемые "deepfake". Эти материалы могут использоваться для дискредитации личностей или как средство манипуляции общественным мнением. На просторах сети Интернет набирает обороты аутентификация личности: двойная игра. Цифровая аутентификация личности позволяет управлять доступом к сервисам и данным. Однако злоумышленники находят способы обхода биометрических систем защиты через подделку отпечатков пальцев или использование технологий для имитации голоса пользователя.

Потенциальная уязвимость Интернет вещей является вектором уязвимости безопасности цифровых данных. Расширение систем Интернета вещей повлекло за собой рост числа устройств, подключаемых к Интернету. Каждое из таких устройств может быть потенциальной точкой неавторизированного доступа в корпоративную или частную сеть.

Развитие такого вида преступности достигло высокого уровня, они находятся в непрерывном поиске слабых мест в информационной безопасности различных отраслях общественных отношений. Зачастую такие преступления совершаются в условиях анонимности, объединяясь в группировки и ведя свою деятельность в конфиденциальных мессенджерах. Имеющиеся наработки в борьбе с IT-преступлениями в сравнении с эволюционированной преступностью являются устаревшими и вынуждают теоретиков и практиков исследовать и совершенствовать способы и методы борьбы с преступностью в рассматриваемой сфере.

Социальная инженерия (далее – СИ) вместе с отсутствием кибергигиены населения приводит к увеличению числа преступлений в сфере цифровой информации. Оказывая психологическое воздействие на лицо, мошенники получают информацию необходимых им данных. Рассылка фишинговых писем сотрудникам организаций, несложные комбинации паролей является угрозой для безопасности данных и информационных коммуникаций организаций.

Существует много мнений и толкований термина «социальная инженерия», но тем не менее у них всех есть общее, все авторы схожи в одном, что это деятельность человека, направленная на манипулирование психологическими особенностями личности, с целью завладения цифровыми данными [20, С. 135; 16, С. 74], вид совершения компьютерных преступлений, направленный на несанкционированное получение информации путем использования уязвимостей человеческой психики.

Информационные технологии, СИ в таком тандеме выступают одним из наиболее эффективных методов для совершения цифровых преступлений. СИ обозначает практику использования психологических манипуляций с целью получения конфиденциальной информации, доступа к защищённым системам или выполнения определённых действий лицом, на которое направлено воздействие. Суть СИ заключается в эксплуатации человеческого фактора как самого слабого звена в системе безопасности. В отличие от традиционных хакерских атак, где используются технические уязвимости программного и аппаратного обеспечения, здесь основным «орудием» является мастерство убеждения и обмана. Примеры социальной инженерии уже сформировались. Это может быть фишинг-отправка электронных сообщений под видом надёжного источника для получения паролей или банковской информации; предоставление ложной личности для неправомерного доступа к офисам или IT-инфраструктуре; или даже «разброс документов» – оставление на видном месте USB-накопителей с вредоносным ПО в надежде, что любопытные работники подключат их к корпоративным компьютерам. Последствия таких атак могут быть чрезвычайно серьёзными. Потеря конфиденциальности данных не только наносит ущерб репутации компаний, но и приводит к финансовым потерям.

Защититься от таких атак сложно, поскольку они направлены на эксплуатацию человеческих слабостей. Однако возможно минимизировать риски через комплексный подход: проведение регулярных тренировок персонала по распознаванию признаков СИ; создание строгой политики безопасности; использование двухфакторной аутентификации; разработка процедур быстрого реагирования на инциденты.

Важность осознания этой проблемы не может быть переоценена. В условиях постоянно развивающегося цифрового мира социальная инженерия будет продолжать оставаться ключевой угрозой для всех пользователей Интернета – от больших корпораций до обычных граждан. Будучи осведомленными о методиках и приемах злоумышленников, мы можем значительно повысить свою защиту в борьбе с этим скрытым видом преступления.

Несмотря на выстроенные системы безопасности, человек является самым уязвимым и слабым звеном в этой системе. Центральный банк Российской Федерации постоянно проводит работы по выявлению схем, с помощью которых злоумышленники похищают и проводят информационную пропаганду среди населения[11].

Беспечность общества, не оценивающего в полной мере опасность преступлений в сфере цифровой информации, позволит нанести большой ущерб не только отдельной личности, но и обществу и государству в целом.

В настоящее время наблюдается связь межу современными информационными технологиями и современной преступностью [10, С. 9].

По статистическим данным МВД Российской Федерации в 2023 году зарегистрировано увеличение числа преступлений в IT-сфере и составило 676951, что на 154 886 больше, чем в предыдущем году. Из них преступлений в сфере компьютерной информации в 2023 году – 37101, что на 27074 больше, чем в предыдущем[12].

Данная статистика позволяет сделать вывод, что число преступлений в сфере цифровой информации склонно к увеличению и охвату новых общественных сфер деятельности.

Проведя анализ 18 обвинительных приговоров суда разных регионов, было выделено обстоятельство, которое оказывает существенное влияние на принцип неотвратимости наказания. Так, при расследовании преступлений, совершенных группой лиц, в число которых входили IT-специалисты, в 15 случаях следствие не может установить их личности. Что свидетельствует о скрытности преступлений, совершенных в IT-сфере, об использовании ими особенностей интернет- пространства.

Заключение

Таким образом, на основе проведенного исследования, можно отметить факторы, отражающие социальную сущность преступления и оказывающие влияние на формирование преступности в данной сфере. К ним относятся:

1. Нестабильная геополитическая обстановка, развитие и внедрение в различные сферы жизни современных цифровых технологий, развивающиеся способы конфиденциальности позволяют появляться новым разновидностями современных цифровых преступлений.

2. Государство заинтересовано в современном развитии своих территорий, особенно находящихся удаленно от центра страны, путем выделения больших финансовых вложений. Такие программы являются долгосрочными. Данные обстоятельства позволяют злоумышленникам рассматривать государственный сектор в качестве цели для совершения своих противозаконных изысканий слабых мест цифровой безопасности.

3. Специальный субъект, неквалифицированно подобранные кадры, имеющие допуск к охраняемой законом цифровой информации, становятся лицами, осуществляющими противоправные действия.

4. Развитие новых цифровых продуктов (цифровой рубль, цифровой паспорт) и введение их в общественные отношения, распространение цифровых преступлений в общественные правоотношения породят новые составы преступлений.

5. Растущее число закрытых информационных ресурсов в сети Интернет, на которых осуществляется незаконная деятельность, негативным образам сказывается на борьбе с преступностью.

[11] Противодействие мошенническим практикам // URL: https://cbr.ru/information_security/pmp/ (дата обращения: 12.04.2024).

[12] Состояние преступности в Российской Федерации за январь – декабрь 2023 года // URL: https://xn--b1aew.xn--p1ai/reports/item/47055751; Состояние преступности в Российской Федерации за январь – декабрь 2022 года // URL: https://xn--b1aew.xn--p1ai/reports/item/35396677 (дата обращения: 12.04.2024).

6. Совершенствование методов социальной инженерии и отсутствие среди населения понимания и соблюдения правил безопасности в интернет пространстве и особенностей размещения личной информации с использование цифровых систем ее передачи.

Системный подход и отлаженный механизм, состоящий из международного сотрудничества, структурированной единой законодательной базы в сфере информационной безопасности, общество, ориентированное на соблюдение и поддержание цифровой гигиены позволит усилить противостояние цифровой преступности.

Цифровизация неотъемлемо связана с рисками роста цифровой преступности. Важно понимать эти риски и активно работать над созданием более безопасных систем защиты информации. Только комплексный подход со стороны государства, бизнес-структур и частных лиц может минимизировать негативные последствия этого процесса.

В заключении хочется подчеркнуть: мы должны быть всегда на шаг впереди злоумышленников, используя все возможные инструментарии для предотвращения киберугроз. Это требует не только постоянного обновления программного обеспечения безопасности, но и широкого информирования пользователей о методах и способах защиты своих цифровых данных.

Список источников

1. Виноградова Е. В. Актуальные мысли о праве / Е. В. Виноградова, С. И. Захарцев. М. : Юрлит, 2023. 232 с.

2. Дерендяева Т. М. Принцип законности и компьютерные преступления в условиях формирования информационного общества / Т. М. Дерендяева, Г. А. Мухина // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 2(56). С. 17–21.

3. Захарцев С. И. Оперативно-розыскная деятельность и информационная безопасность как часть военной безопасности России / С. И. Захарцев, В. П. Сальников, А. С. Алексанин // Известия Российской академии ракетных и артиллерийских наук. 2018. № 2(102). С. 102–106.

4. Ищук Я. Г. Цифровая криминология: учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов М. : Академия управления МВД России, 2021. 242 с.

5. Каримов В. Х. Современное состояние и тенденции дальнейшего развития системы криминалистического обеспечения борьбы с преступностью в информационно-телекоммуникационной сфере / В. Х. Каримов, А. В. Каримов // Проблемы правовой и технической защиты информации. 2020. № 8. С. 66–72.

6. Квашис В. Е. О новой теории прикладной криминологии: рецензия на учебник В. С. Овчинского «Криминология цифрового мира» // Общество и право. 2018. № 1 (63). С. 122–124.

7. Колин К. К. Цифровая революция и искусственный интеллект: новые горизонты и опасности // Партнерство цивилизаций. 2020. № 1-2. С. 100–106.

8. Лавицкая М. И. Структурно-содержательная характеристика главы 28 Уголовного кодекса Российской Федерации: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации / М. И. Лавицкая, И. Н. Крапчатова // Российский следователь. 2021. № 6. С. 35–41.

9. Лобач Д. В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети Интернет // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 21–27.

10. Осипова И. Н. Искусственный интеллект – угроза или помощник человека? // Экономика. Общество. Человек: материалы Всероссийской научно-практической конференции с международным участием / ред. Е. Н. Чижова. Т. 1. Вып. XXXVII. Белгород: Белгородский государственный технологический университет им. В. Г. Шухова, 2019. С. 179–182.

11. Ровина Е. Е. Компьютерные преступления вчера и сегодня / Е. Е. Ровина, З. З. Гурьянова // Научный дайджест Восточно-Сибирского института МВД России. 2022. № 3(17). С. 81–85.

12. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М. : ИНФРА-М, 2023. 351 с.

13. Савенков А. Н. Вектор развития криминалистической науки в условиях глобальной цифровизации / А. Н. Савенков, Е. Р. Россинская // Государство и право. 2023. № 5. С. 100–110.

14. Семенова И. В. Нормативное правовое регулирование ответственности за правонарушения в сфере информационной безопасности // Образование и право. 2023. № 5. С. 119–124.

15. Серебренникова А. В. Цифровая криминалистика и ее значение для расследования преступлений // International Law Journal. 2019. Т. 2. № 4. С. 126–133.
16. Суворова, В. В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В. В. Суворова, Л. А. Суворова // Теория и практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научно-практической конференции, Смоленск, 13 августа 2019 года. Смоленск: МНИЦ «Наукосфера», 2019. С. 71–74.
17. Тамбовцев А. И. Эволюция оперативно-розыскных мероприятий: монография / А. И. Тамбовцев, Н. В. Павличенко. М. : Академия управления МВД России, 2021. С. 41–42.
18. Шаталов А. С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). URL: https://cyberleninka.ru/article/n/razrabotka-metodicheskih-osnov-rassledovaniya-prestupleniy-sovershaemyh-s-pomoschyu-kompyuternyh-i-setevyh-tehnologiy-problemy (дата обращения: 26.05.2023).
19. Яковец Ю. В. Функции интеллекта Человека разумного – первоисточники института партнерства цивилизаций // Партнерство цивилизаций. 2020. № 1-2. С. 100–106.
20. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133–138.

References

1. Vinogradova E. V. Aktual'nye mysli o prave / E. V. Vinogradova, S. I. Zaharcev. M.: Yurlit, 2023. 232 s. (In Russ.).
2. Derendyaeva T. M. The principle of legality and computer crimes in the context of the formation of an information society / T. M. Derendyaeva, G. A. Muhina // Vestnik Kaliningradskogo filiala Sankt-Peterburgskogo universiteta MVD Rossii. 2019;2(56): 17–21. (In Russ.).
3. Zaharcev S. I. Operational investigative activities and information security as part of Russia's military security / S. I. Zaharcev, V. P. Sal'nikov, A. S. Aleksanin // Izvestiya Rossijskoj akademii raketnyh i artillerijskih nauk. 2018;2(102): 102–106. (In Russ.).
4. Ishchuk Ya. G. Cifrovaya kriminologiya: uchebnoe posobie / Ishchuk Ya. G., Pinkevich T. V., Smol'yaninov E. S. M. : Akademiya upravleniya MVD Rossii, 2021. 242 s. (In Russ.).
5. Karimov V. H. The current state and trends in the further development of the system of forensic support for combating crime in the information and telecommunications sector / V. H. Karimov, A. V. Karimov // Problemy pravovoj i tekhnicheskoj zashchity informacii. 2020;8: 66–72. (In Russ.).
6. Kvashis V. E. On the new theory of applied criminology: a review of V. S. Ovchinsky's textbook "Criminology of the Digital World"// Obshchestvo i pravo. 2018;1 (63): 122–124. (In Russ.).
7. Kolin K. K. The digital Revolution and artificial intelligence: new horizons and dangers // Partnerstvo civilizacij. 2020;1-2: 100–106. (In Russ.).
8. Lavickaya M. I. Structural and substantive characteristics of Chapter 28 of the Criminal Code of the Russian Federation: legal, technical and legal implementation problems of crimes in the field of computer information / M. I. Lavickaya, I. N. Krapchatova // Rossijskij sledovatel'. 2021;6: 35–41. (In Russ.).
9. Lobach D. V. The development of Russian criminal legislation in the field of countering crimes committed on the Internet // Ugolovnoe pravo: strategiya razvitiya v XXI veke. 2023;3: 21–27. (In Russ.).
10. Osipova I. N. Iskusstvennyj intellekt – ugroza ili pomoshchnik cheloveka? // Ekonomika. Obshchestvo. Chelovek: materialy Vserossijskoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem / red. E. N. Chizhova. T. 1. Vyp. XXXVII. Belgorod: Belgorodskij gosudarstvennyj tekhnologicheskij universitet im. V. G. Shuhova, 2019. S. 179–182. (In Russ.).
11. Rovina E. E. Computer crimes yesterday and today / E. E. Rovina, Z. Z. Gur'yanova // Nauchnyj dajdzhest Vostochno-Sibirskogo instituta MVD Rossii. 2022;3(17): 81–85. (In Russ.).
12. Russkevich E. A. Ugolovnoe pravo i «cifrovaya prestupnost'»: problemy i resheniya: monografiya. 2-e izd., pererab. i dop. M. : INFRA-M, 2023. 351 s. (In Russ.).
13. Savenkov A. N. The vector of development of forensic science in the context of global digitalization / A. N. Savenkov, E. R. Rossinskaya // Gosudarstvo i pravo. 2023;5. S. 100–110. (In Russ.).
14. Semenova I. V. Regulatory legal regulation of liability for violations in the field of information security // Obrazovanie i pravo. 2023;5: 119–124. (In Russ.).

15. Serebrennikova A. V. Digital forensics and its importance for crime investigation // International Law Journal. 2019. T. 2;4: 126–133. (In Russ.).

16. Suvorova, V. V. Sovershenie prestuplenij s ispol'zovaniem social'noj inzhenerii: postanovka problemy / V. V. Suvorova, L. A. Suvorova // Teoriya i praktika prioritetnyh nauchnyh issledovanij: sbornik nauchnyh trudov po materialam VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii, Smolensk, 13 avgusta 2019 goda. Smolensk: MNIC «Naukosfera», 2019. S. 71–74. (In Russ.).

17. Tambovcev A. I. Evolyuciya operativno-rozysknyh meropriyatij: monografiya / A. I. Tambovcev, N. V. Pavlichenko. M. : Akademiya upravleniya MVD Rossii, 2021. S. 41–42. (In Russ.).

18. Shatalov A. S. Development of methodological foundations for the investigation of crimes committed using computer and network technologies: problems, prospects and trends // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. 2018;3 (32). URL: https://cyberleninka.ru/article/n/razrabotka-metodicheskih-osnov-rassledovaniya-prestupleniy-sovershaemyh-s-pomoschyu-kompyuternyh-i-setevyh-tehnologiy-problemy (data obrashcheniya: 26.05.2023). (In Russ.).

19. Yakovec Yu. V. The functions of the intellect of a reasonable Person – primary sources of the Institute of Partnership of Civilizations // Partnerstvo civilizacij. 2020;1-2: 100–106. (In Russ.).

20. Yangaeva M. O. Social engineering as a way to commit cybercrimes // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. 2021;1 (42): 133–138. (In Russ.).

Информация об авторах

И. В. Семёнова *– кандидат юридических наук*

Статья поступила в редакцию 01.04.2024;
одобрена после рецензирования 18.06.2024;
принята к публикации 20.06.2024.

Information about the authors

I. V. Semyonova *– Candidate of Sciences (Law)*

The article was submitted 01.04.2024;
approved after reviewing 18.06.2024;
accepted for publication 20.06.2024.