УДК 349, 343 DOI: 10.31249/iajpravo/2024.04.06

АЛФЕРОВ О.Л.[1], АЛФЕРОВА Е.В.[2] ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И «ЦИФРОВАЯ» ПРЕСТУПНОСТЬ (Обзор)

Аннотация. В данном обзоре представлены новые монографии, касающиеся вопросов использования информационных технологий в уголовном праве и уголовном процессе, и точки зрения ряда исследователей на проблемы их правового регулирования. Внимание к этой теме обусловлено активным развитием процессов информатизации и цифровизации и использованием их достижений в жизни человека, общества и государства. Вместе с тем, по оценкам исследователей, всё чаще информационные технологии находят свое применение не только в профессиональной и повседневной деятельности людей, но и в криминальной среде, используются в преступных целях и становятся всё более изощренными и опасными. Авторы книг не только классифицируют и характеризуют составы преступления в сфере информационных технологий, но и предлагают конкретные правовые решения многих проблем, связанных с ними.

Ключевые слова: информационно-коммуникационные технологии; информационное право; цифровое право; компьютерная преступность; информационная преступность: технотронная преступность.

ALFEROV O.L., ALFEROVA E.V. Information technologies and «digital» crime (Review)

[1] *Алферов Олег Леонидович*, ведущий редактор отдела правоведения ИНИОН РАН.

[2] *Алферова Елена Васильевна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН.

Abstract. This review presents new monographs on the use of information technologies in criminal law and criminal procedure, and the views of a number of researchers on the problems of their legal regulation. Attention to this topic is due to the active development of the processes of informatization and digitalization and the use of their achievements in human life, society and the state. At the same time, according to researchers, information technologies are increasingly being used not only in people's professional and daily activities, but also in the criminal environment, used for criminal purposes and becoming more sophisticated and dangerous. The authors of the books not only classify and characterize the elements of crime in the field of information technology, but also offer specific legal solutions to many problems related to them.

Keywords: information and communication technologies; information law; digital law; computer crime; information crime: technotronic crime.

Для цитирования: Алферов О.Л., Алферова Е.В. Информационные технологии и «цифровая» преступность (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер: Государство и право. – 2024. – № 4. – С. 83–96. – DOI: 10.31249/iajpravo/2024.04.06

Введение

Информационно-цифровые технологии проникли практически во все сферы деятельности современного человека. Их внедрение происходит быстрее, чем любых других инновационных разработок в истории человечества; их эффективное применение отражается на всех сторонах жизни общества и государства, в том числе негативной, обусловленной использованием таких технологий в противоправных целях. Как отмечают исследователи, количество преступных деяний возрастает параллельно с динамикой распространения этих технологий [2, с. 5–6]. Так, по данным ГИАЦ МВД России, в 2022 г. зарегистрировано 522, 1 тыс. преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации. При этом доля таких преступлений в общей структуре преступности составляет более четверти (26,5%) [2, с. 68]. Наиболее массовыми видами преступлений с использованием ИКТ в

России признаются мошенничества и кражи денежных средств со счетов граждан и организаций. Ущерб исчисляется миллиардами рублей (в 2022 г. составил 65 млрд руб.) [2, с. 69]. То есть с развитием информационных технологий и стремлением государства к полной цифровой трансформации всех сфер общественной жизни, совершенствуются также инструменты совершения преступлений.

Информационные технологии и угрозы безопасности: уголовно-правовые риски

Наиболее значимые угрозы информационной безопасности возникают в следующих областях: 1) алгоритмическая обработка данных цифровыми платформами; 2) цифровая дискриминация; 3) персональные данные и большие данные; 3) кибератаки и компьютерное мошенничество; 4) кибербуллинг, троллинг и иные акты агрессии в цифровой среде; 5) информационные войны; 6) новые способы мониторинга и контроля со стороны государств, основанные на сборе и анализе данных [2, p. 15]. Криминогенные риски наиболее распространены в случаях использования технологий ИИ, блокчейна, Интернета вещей. Отдельные примеры таких рисков приводит доктор юридических наук С.В. Маликов; эти риски касаются в том числе угроз безопасности систем ИИ, реализуемых в разных сферах: в транспортной отрасли, в системах контроля доступа и обнаружения мошенничества с кредитными картами, в системах интеллектуальной идентификации человека. Так, при использовании блокчейна известны мошеннические атаки с фишингом, атаки троянцами, на владельцев криптокошельков и на смарт-контракты. Инфраструктуры и устройства Интернета вещей уязвимы в случаях обнаружения слабых паролей, использования небезопасных сетевых серверов, ненадежных облачных и мобильных интерфейсов, недостаточной защиты конфиденциальности и др. [2, с. 16–31]. По мнению С.В. Маликова, анализ уязвимости отдельных информационных технологий, позволяет сделать вывод о том, что в отечественном уголовном законодательстве в части обеспечения информационной безопасности практически не учитывается следующая специфика информационной сферы: 1) информация об уязвимостях таких систем и программного обеспечения, которые

создают возможность совершать преступления, распространяется свободно; 2) уязвимости возникают и выявляются непрерывно, запросы к требованиям по обеспечению безопасности растут постоянно, что требует перманентной актуализации законодательства; 3) средства реализации преступления (специализированное программное обеспечение) может создавать человек, имеющий определенные навыки, в любой точке мира; 4) не существует средств, которые заведомо предназначены для совершения преступного деяния, любое средство атаки может использоваться как инструмент контроля защищенности; 5) распределение сфер ответственности осуществляется лишь в рамках одной информационной системы, не существует общего подхода к распределению ответственности за создание условий для преступления и др. [2, с. 31–32].

Научное исследование в рассматриваемой области, предпринятое в рамках монографии «Информационные технологии в уголовно-правовой сфере», подготовленной профессорско-преподавательским составом Московской академии Следственного комитета РФ и Института государства и права РАН, представляется весьма актуальным, оно сосредоточено на вопросах правового регулирования информационных технологий, проблемах уголовно-правового противодействия использованию этих технологий в преступных целях, специфике информационных технологий в уголовном судопроизводстве. Прежде всего авторы характеризуют ключевые стратегические документы, федеральные законы и постановления Правительства РФ, принятые в последние годы в России в области применения новых информационных (цифровых) технологий. Использование этих технологий связано со многими противоправными рисками, длинный список которых представлен в данной работе [2, с. 42–46]. В центре внимания авторов правовые запреты и обязанности, установленные законом в целях минимизации этих рисков, в том числе в критической информационной инфраструктуре, имеющей особое значение для национальной экономики и безопасности стран, а также обязанности владельцев социальной сети и цифровых платформ выявлять угрозы и риски, осуществлять их мониторинг в целях обеспечения безопасности интернет-ресурсов и предупреждения противоправных деяний.

Неправомерное воздействие на информационно-коммуникационную инфраструктуру признается уголовным преступлением. Так, в целях обеспечения безопасности и устойчивости функционирования критической информационной инфраструктуры при проведении в отношении ее компьютерных атак принят Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации». В соответствии с этим Законом создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГопСОПКА).

В обозреваемом исследовании акцент также делается на правовых проблемах обеспечения защиты персональных данных (далее – ПД); цифровых финансовых активах, цифровой медицине, где развитие информационных технологий имеет высокий потенциал влияния на качество жизни; специфике применения искусственного интеллекта, квантовых коммуникаций и перспективных космических систем. Если говорить, в частности, об обеспечении защиты ПД, то этому способствует, по мнению докторов юридических наук Т.А. Поляковой и А.А. Смирнова, а также кандидата юридических наук А.И. Химченко, определение видов угроз безопасности ПД, применение организационных и технических мер и процедур оценки соответствия средств защиты информации и их эффективности до ввода в эксплуатацию информационной системы ПД, обнаружение фактов несанкционированного доступа к ПД и принятие соответствующих мер; восстановление ПД, уничтоженных или модифицированных вследствие несанкционированного доступа к ним, установление правил доступа к ПД и контроля над применяемыми мерами и обеспечения безопасности ПД и уровня защищенности информационных систем ПД и др. [2, p. 51–52]. Анализ обеспечения функционирования систем ИИ и робототехники, считают авторы, требует решения ряда вопросов, связанных с юридической ответственностью в этой сфере, а также правового статуса соответствующих технологий, правосубъектности ИИ, информационной безопасности [2, p. 63].

Правовой режим информационных технологий в целях борьбы с киберпреступностью

Компьютерная преступность, прежде всего, в кредитно-финансовой сфере, в области прав и свобод человека, в том числе касающейся неприкосновенности частной жизни, личной и семейной тайны, персональных данных, в Доктрине информационной безопасности РФ 2016 г. и Стратегии национальной безопасности РФ 2021 г. рассматриваются как угрозы национальной и международной безопасности. Проблема противодействия использованию ИКТ в криминальных целях находится постоянно в центре внимания Генеральной Ассамблеи ООН; особо важное значение в борьбе с киберпреступностью имеют специальные резолюции ГА ООН A/55/63 и A/RES/56/121 «Борьба с преступным использованием информационных технологий, A/73/187 и A/74/247 «Противодействие использованию информационно-коммуникативных технологий в преступных целях». Однако, как отмечают Т.А. Полякова и А.А. Смирнов, до настоящего времени отсутствует универсальный международный договор, который регламентировал бы сферу борьбы с киберпреступностью [2, с. 71]. Первый проект Конвенции о сотрудничестве в сфере противодействия информационной преступности еще в 2017 г. Россия представила в ООН. В 2024 г. итоговый текст проекта конвенции должен быть предъявлен ГА ООН Специальным комитетом ООН по разработке этой международной конвенции.

Следует учитывать, что в 2018 г. в рамках СНГ было принято Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (первое такое Соглашение было принято еще в 2001 г.). Перечень уголовно наказуемых деяний с 2001 г. расширился с четырех до восьми, включая хищения имущества с использованием ИКТ и распространением экстремистских материалов в информационно-телекоммуникационных сетях.

Ученые признают, что до сих пор понятийный аппарат в сфере информационных технологий в полной мере не сформирован. Отсутствует единый подход в международных и национальных документах. Так, если в Будапештской конвенции о киберпреступности используется термин «киберпреступность», то в официальных

документах Российской Федерации и других стран СНГ, ШОС и ОДКБ – «информационная преступность», «преступность в сфере информационных технологий», «преступность в сфере компьютерной информации» и др. Наибольшие различия наблюдаются в научных исследованиях, где употребляются понятия «цифровая преступность», «киберпреступность», «преступность в сфере высоких технологий» и др. Авторы книги «Информационные технологии в уголовно-правовой сфере» придерживаются термина «преступления в сфере информационных технологий», полагая, что понятие «киберсфера» может быть без всяких потерь заменено понятием «информационная сфера» [2, с. 77].

По сравнению с Будапештской конвенцией в сфере компьютерной безопасности 2001 г., предусматривающей четыре вида киберпреступлений, в вышеупомянутом российском проекте конвенции ООН о противодействии использованию ИКТ в преступных целях 2021 г. данный перечень включает 23 состава преступления (ст. 6–28 проекта). Наряду с этим Т.А. Полякова и А.А. Смирнов замечают, что в уголовном законодательстве РФ сегодня отсутствует как общепринятая терминология для обозначения преступлений в сфере информационных технологий, так и четкий перечень таких преступлений – и это отражается на правоприменительной практике. В связи с этим упоминается указание Генерального прокурора РФ № 11/11 и МВД России № 1 от 17.01.2023 г., в котором называются 25 преступлений, совершенных с использованием ИКТ и в сфере компьютерной информации. Полный их список, с указанием конкретных статей УК РФ, дан в книге [2, с. 85].

Таким образом, исследование, проведенное авторским коллективом ученых, показывает значительное расхождение терминологических, содержательных подходов к определению преступлений в сфере информационных технологий, и проблема совершенствования правового регулирования рассматриваемой сферы остается актуальной [2, с. 90].

Информационные технологии как объект уголовно-правовой защиты

Участие ученых Московской академии Следственного комитета РФ и ИГП РАН в написании книги «Информационные техно-

логии в уголовно-правовой сфере» позволяет взглянуть на проблемы использования информационных технологий не только с точки зрения науки уголовного права, но и раскрыть криминологические, криминалистические и процессуальные аспекты борьбы с преступлениями в сфере информационных технологий. Такой подход отражается в статьях глав 2–4, в которых комплексно рассматриваются следующие темы: информационные технологии как объект уголовно-правовой защиты (С.В. Маликов); соучастие и стадии преступлений, совершенных с использованием информационных технологий (Я.Н. Ермолович, В.А. Перов); уголовно-процессуальные основы досудебного производства по рассматриваемой категории уголовных дел (Н.В. Османова); цифровые технологии в уголовном процессе (Ю.А. Цветков) и алгоритмы формирования доказательств (В.А. Прорвич); теория и практика расследования компьютерных преступлений (О.Ю. Антонов, Т.А. Сааков, С.Ю. Скобелин, А.А. Бессонов, А.И. Бастрыкин). Важно то, что в этих главах работы содержатся выводы и практические рекомендации, которые могут быть использованы в науке и практике борьбы с «цифровыми» преступлениями.

Криминологическая характеристика технотронной преступности и противодействие этому виду преступности

Книга К.Н. Евдокимова, доктора юридических наук, профессора кафедры государственно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры РФ, «Противодействие технотронной преступности: теория, законодательство, практика», в рамках рассматриваемой темы обзора заслуживает особого внимания не только ввиду значимости исследования технотронной преступности и широкого круга исследованных автором вопросов, но и высокого уровня его профессионального мастерства, глубины познания проблем этого вида преступлений. Системное и аргументированное изложение сложных вопросов, касающихся криминологической характеристики технотронной преступности, факторов, детерминирующих эту преступность, а также криминологической организации (инжиниринга) противодействия технотронной преступности, заслуживает

внимания законодателей, ученых-юристов и представителей IT-технологий.

Термин «технотронная преступность» по отношению к понятиям «преступность в сфере информационных технологий», «компьютерная преступность», «киберпреступность», «цифровая преступность», по мнению К.Н. Евдокимова, выступает родовым понятием и включает в себя всю совокупность преступных деяний, посягающих на общественные отношения в сфере безопасного создания, использования, распространения не только коммуникационных и компьютерных технологий. но и когнитивных, космических, робототехнических и иных высоких технологий, основанных на использовании микроэлектроники (микропроцессоров) [1, с. 14]. Современное состояние, тенденции и перспективы развития технотронной преступности позволяют автору выдвинуть научную (частную) теорию «Анекселенктотичной (неконтролируемой) технотронной преступности» о появлении «нового вида высокотехнологической преступности, пришедшей на смену традиционной компьютерной преступности и являющейся дальнейшей формой развития преступности с использованием высоких технологий, которая в силу латентности, организационного, профессионального, трансграничного, транснационального характера и самодетерминации вышла из-под контроля личности, общества и государства, представляя опасность для всех жизненно важных общественных отношений» [1, с. 16–17].

Технотронную преступность как сложное социальное и государственно-правовое понятие К.Н. Евдокимов определяет в узком и широком смыслах [1, с. 25–26] и на этом основании выделяет и рассматривает наиболее значимые признаки, характеризующие сущность этого вида российской преступности, взаимосвязанной с другими видами преступности в России [1, с. 26–29]. Структуру технотронной преступности в России автор рассматривает исходя из анализа нормативных, экспертных и доктринальных источников, прежде всего УК РФ, Доктрины информационной безопасности, указаний и официальной статистики Генеральной прокуратуры РФ и др. Обобщенные данные об удельном весе, интенсивности совершения отдельных видов наиболее распространенных общественно опасных деяний в структуре российской технотронной преступности, динамика роста зарегистрированных, а также прекращен-

ных, приостановленных или направленных в суд за 2015–2022 гг., представлены в таблицах 1–6 [1, с. 37–47]. Из анализа этих таблиц следует, что зарегистрированные технотронные преступления и лица их совершившие составили за последние пять лет почти 300%. То есть технотронная преступность растет в геометрической прогрессии. Так, коэффициент преступности на 100 тыс. населения, достигшего возраста привлечения к уголовной ответственности, вырос с 36,1 в 2015 г. до 430,8 в 2022 г., т.е. почти в 12 раз (1193, 4%) [1, с. 47]. Анализируя тенденции развития технотронной преступности, автор замечает значительное увеличение количества корыстных преступлений, совершенных с использованием информационных технологий (краж, мошенничеств, вымогательств, сбыта наркотических средств и др.). Изменяется и направленность хищений. Жертвами преступников всё чаще становятся обычные граждане, являющиеся клиентами банков, финансово-кредитных организаций. Хищения происходят с использованием средств социальной инженерии, их доля составила 50,4% [1. с. 49].

На основе анализа эмпирических данных, представленных в таблицах 7–12 [1, с. 52–62], автор «рисует» криминологический портрет «технотронного» преступника, который значительно изменился за последние десятилетия. Так, если в конце 1990-х – начале 2000-х среди компьютерных преступников преобладала молодежь в возрасте 16–25 лет, не обладающая профессиональными навыками в сфере IT-технологий, в настоящее время – это люди более зрелого возраста, работающие (либо уволенные) квалифицированными специалистами в сфере предоставления дистанционных, банковских, коммерческих, информационных и иных высокотехнологических услуг [1, с. 65].

Изучая судебно-следственную практику, статистические данные, экспертные оценки, результаты анкетирования сотрудников правоохранительных органов и компьютерных пользователей, контента интернет-ресурсов, публикаций в СМИ и других источников, К.Н. Евдокимов классифицирует детерминанты – основные факторы совершения технотронных преступлений в Российской Федерации (причины, условия, обстоятельства совершения преступления) – по сферам общественной жизни: социальные, экономические, кадровые, организационно-технические, политические

и др. Все эти факторы взаимосвязаны между собой и образуют комплекс таких факторов.

Значительное внимание в своей монографии К.Н. Евдокимов уделяет системе противодействия технотронной преступности, определяя ее основные цели, задачи, объекты, специализированные субъекты и меры, среди которых обозначаются экономические, общесоциальные, духовно-культурные, общие научно-технические меры противодействия технотронной преступности. К последним автор относит: формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений; развитие информационной и коммуникационной инфраструктуры Российской Федерации; создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне; обработку больших данных; искусственный интеллект; доверенные технологии электронной идентификации и аутентификации; роботехнику и биотехнологии и др. [1, с. 139].

Наряду с вышеуказанными общими мерами в работе рассматриваются и специальные правовые меры противодействия этому виду преступных деяний. Они касаются как совершенствования действующего уголовного законодательства, так и гражданского, административного, информационного и иного отраслевого законодательства. Если говорить об уголовном законе, то автор предлагает дополнить гл. 28 УК РФ новыми составами преступлений, например, ввести: ст. 272.1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации»; ст. 273.1 «Приобретение, создание, использование и распространение вредоносной компьютерной сети (ботнета)»; ст. 274.2 «Незаконная рассылка компьютерной информации (спама) в нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации или информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям». Кроме того, предлагается переименовать гл. 28 УК РФ «Преступления в сфере компьютерной информации» на «Технотронные преступления» [1, с. 142]. Вместе с тем К.Н. Евдокимов считает важным сохранение преемственности, концептуального единства

«цифровой» криминологии и уголовно-правовой доктрины XXI в. с традиционной криминологической теорией и классической школой российского уголовного права, основанных на принципах законности, равноправия, гуманизма и социальной справедливости [1, с. 139].

Хищения, совершаемые с использованием информационных технологий

Как действуют сегодня преступники, используя информационные технологии при совершении хищений, например, при кражах безналичных денежных средств, мошенничеств в отношении таких средств, присвоении и растрате, речь идет в монографии эксперта лаборатории антикоррупционной политики НИУ ВЭШ Р.М. Ушакова. Анализ уголовно-правового регулирования таких преступлений, судебной практики и официальной статистики позволил автору выявить негативную тенденцию увеличения количества зарегистрированных хищений, совершенных с использованием информационных технологий. По данным МВД России, в период с 2019 по 2022 г. оно увеличилось с 294 348 до 522 065 преступлений (рост 77,4%), из них краж – 21,7%, мошенничеств – 49.3% [3, с. 118–119]. Регионами наибольшего прироста являются: Московская область, Республика Саха (Якутия), Краснодарский край, Республика Адыгея, Ярославская, Челябинская, Тульская области и ряд других субъектов РФ.

Как замечает автор, для жертв хищений характерны доверчивость, неосторожность, неосмотрительность или рассеянность, отсутствие технических познаний. Криминологический портрет личности «цифрового» мошенника характеризуют такие его качества, как достаточно высокий уровень интеллектуального развития и материально-технического обеспечения своей деятельности, познаний в сфере юриспруденции и экономики. Использование информационных технологий в процессе совершения хищений увеличивает их общественную опасность. В связи с этим автор предлагает ввести новый п. 5 в ст. 158 УК РФ, предусматривающий уголовную ответственность за такого рода хищения, и увеличить санкции.

На основе анализа более 200 актов судов первой, апелляционной, кассационной и надзорной инстанций Р.М. Ушаков выделяет ряд проблем квалификации хищений, совершаемых с применением информационных технологий. Это проблемы, касающиеся: рассмотрения криптовалюты в качестве предмета хищения; квалификации преступлений, совершаемых в отношении криптовалюты, либо по ст. 159 и 272 УК УР, либо по ст. 159.6 и 272 УК РФ; разграничения составов хищений, совершенных с применением информационных технологий, и компьютерных преступлений, предусмотренных гл. 28 УК РФ; конкуренции составов преступлений, предусмотренных п. «г» ст. 158 (кража, совершенная с банковского счета, а равно в отношении электронных денежных средств), и ч. 1 и 2 ст. 159.3 УК РФ; разграничения понятий кражи или мошенничества, совершенных «с банковского счета» и «в отношении электронных денежных средств»; квалификации присвоения и растраты, совершенных с применением информационных технологий; отграничения соответствующих составов кражи, мошенничества, злоупотребления служебными полномочиями и самоуправства и др. [1. с. 122–123].

Заключение

Обзор новых исследований ученых-юристов показывает, как важно сегодня не упустить из внимания законодателю и научной общественности проблемы использования информационно-коммуникационных технологий, обеспечения должного правового регулирования их применения в различных сферах общественной жизни, в том числе в криминальной, связанной с высокотехнологичной преступностью. В последние пять лет опубликовано много книг, исследующих влияние цифровизации на уголовное право и процесс судопроизводства[1]. Для организации системной работы по

[1] См., напр.: Противодействие преступлениям, совершаемым в сфере информационных технологий / А.В. Андреев, В.В. Гончар, Н.Н. Горач [и др.]; под ред. И.А. Калиниченко. – Москва, 2022; Риски цифровизации: виды, характеристика, уголовно-правовая оценка / под ред. Ю.В. Грачевой. – Москва, 2021; Овчинский В.С. Криминология цифрового мира. – Москва, 2018; Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. – Москва, 2022; Уголовно-юрисдикционная деятельность в условиях цифровизации /

предотвращению преступлений, совершаемых с использованием информационных технологий, в этих книгах содержатся рациональные предложения по совершенствованию уголовного и уголовно-процессуального законодательства, криминалистической тактики и техники их расследования, по созданию единого информационного ресурс-портала с ограниченным доступом, содержащим необходимую литературу, методические рекомендации по расследованию киберпреступлений, с персональной авторизацией следователей и криминалистов для использования информации о возможностях расследования.

Список литературы

1. Евдокимов К.Н. Противодействие технотронной преступности: теория, законодательство, практика: монография / Иркутский юрид. ин-т (филиал) Университета прокуратуры РФ. – Иркутск, 2023. – 171 с.
2. Информационные технологии в уголовно-правовой сфере: монография / Моск. акад. Следственного комитета РФ, ИГП, РАН; под ред. А.И. Бастрыкина, А.Н. Савенкова. – Москва: ЮНИТИ-ДАНА, 2023. – 279 с.
3. Ушаков Р.М. Классификация хищений, совершаемых с использованием информационных технологий: монография. – Москва: Юстицинформ, 2023. – 160 с.

Н.А. Голованова, А.А. Гравина, О.А. Зайцев [и др.]; Ин-т законодат. и сравн. правоведения при Правительстве РФ. – Москва, 2019; Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию») / отв. ред. Л.Н. Масленникова. – Москва, 2022; Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики. – Москва, 2020 и др.