УДК 343
ББК 67.408
https://doi.org/10.31862/3033-7909-2025-02-92-101

ВОПРОСЫ УГОЛОВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В МЕХАНИЗМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.Я. Минин

Аннотация. *В статье рассматриваются проблемы развития уголовно-правового регулирования и обеспечения национальной безопасности в целях совершенствования качества подготовки «цифрового юриста» в рамках цифровизации образования. На основе проведенного исследования сформулированы выводы по следующим важным аспектам указанной тематики: особенности анализа деяний, совершаемых в сфере электронной информации и/или связанных с цифровыми технологиями; характеристики личности человека, совершающего преступные деяния в сфере электронной информации; особенности аналитического обеспечения расследования преступлений, совершенных с применением электронной информации и цифровых технологий; потенциальные возможности применение IT-технологий в цифровой криминалистике; основные сферы применения цифровых технологий в уголовном судопроизводстве. Кроме того, принимая во внимание, что в условиях активной цифровой трансформации общества также достаточно интенсивно развивается цифровая криминалистика, в том числе цифровая внеэкспертная, отмечено, что при раскрытии и расследовании сложных преступлений используется поиск, извлечение, восстановление, иная обработка данных в электронном виде, связанная с обнаружением и исследованием информации на электронных носителях и цифровых устройствах. В этой связи обоснован вывод о том, что на процесс подготовки специалистов в области юриспруденции существенно влияют уровень и темпы роста профессионализма обучающих и обучающихся, ряд социальных факторов, включая последствия цифровизации общества.*

Ключевые слова: *киберпреступления, национальная безопасность, личность правонарушителя, цифровизация, цифровая криминалистика, уголовное судопроизводство, компетенции подготовки «цифрового юриста».*

Для цитирования: *Минин А.Я.* Вопросы уголовно-правового регулирования в механизме обеспечения национальной безопасности // Социально-гуманитарные исследования: социология, экономика, право. 2025. № 2. С. 92–101. DOI: 10.31862/3033-7909-2025-02-92-101

© Минин А.Я., 2025

Контент доступен по лицензии Creative Commons Attribution 4.0 International License
The content is licensed under a Creative Commons Attribution 4.0 International License

ABOUT PROBLEMS CRIMINAL LAW REGULATE IN THE MECHANISM OF ENSURING NATIONAL SECURITY

A.Ia. Minin

Abstract. *The article discusses the problems of the development of criminal law regulation and ensuring national security in order to improve the quality of training of a "digital lawyer" in the framework of digitalization of education. Based on the conducted research, conclusions are formulated on the following important aspects of this topic: features of the analysis of acts committed in the field of electronic information and/or related to digital technologies; characteristics of the personality of a person committing criminal acts in the field of electronic information; features of analytical support for the investigation of crimes committed with the use of electronic information and digital technologies; potential application of IT-technologies in digital criminology; the main areas of application of digital technologies in criminal proceedings. In addition, considering that in the conditions of active digital transformation of society, digital criminology is also developing quite intensively, including digital non-expert, it is noted that in the disclosure and investigation of complex crimes, search, extraction, recovery, and other data processing in electronic form is used, related to the detection and research of information on electronic media and digital devices. In this regard, the conclusion is substantiated that the process of training specialists in the field of jurisprudence is significantly influenced by the level and growth rates of professionalism of teachers and students, a number of social factors, including the consequences of digitalization of society.*

Keywords: *cybercrime, national security, identity of the offender, digitalization, digital criminalistics, criminal proceedings, competence of the training of a "digital lawyer".*

Cite as: Minin A.Ia. About problems criminal law regulate in the mechanism of ensuring national security. *Sotsialno-gumanitarnye issledovaniia: sotsiologiia, ekonomika, pravo.* 2025, No. 2, pp. 92–101. DOI: 10.31862/3033-7909-2025-02-92-101

Особенности анализа деяний, совершаемых в сфере электронной информации и/или связанных с цифровыми технологиями. В процессе формирования нового миропорядка нарастает уровень трансграничных угроз безопасности суверенных государств и всего мирового сообщества. Эти угрозы и вызовы приобрели системный характер и создают реальную опасность для современной цивилизации. К ним относятся: распространение оружия массового уничтожения, кибер- и международный терроризм, трансграничная оргпреступность, наркоторговля, дефицит ресурсов и продовольствия, незаконная миграция, изменение климата и проч. Так, если в 2018 г. средствами российской Государственной системы обнаружения, предупреждения и ликвидации компьютерных или кибератак на электронные ресурсы страны выявлено 4,3 млн кибер-воздействий на критическую информационную

инфраструктуру (КИИС РФ), то в 2020 г. число кибератак на цифровые объекты России превысило 1 млрд[12].

Кибератаки и киберконфликты между крупными государствами превратились в элемент политической реальности. Возникла тактика непрямых действий: психологическое давление, фейк (fake – фальшивки медийные; псевдоновости, фотоподделки, сайты мошеннические с фальшивыми комментариями несуществующих экспертов, аккаунты фальшивые, троллинг), астротурфинг (astroturfing) как использование программного обеспечения для управления общественным мнением, посредством создания видимости какого-либо социального эффекта; цифровые IT-технологии, ИКТ, иной инструментарий (диагностика, дескриптивный анализ, компаративный метод для выявления особенностей использования ИКТ в деятельности компетентных ведомств зарубежных государств), а также формы, методы и средства информационного воздействия.

Недружественные государства применяют различные методы вытеснения России с внешнего информационного рынка, разрабатывают концепции информационных кампаний, войн, ресурса «мягкой силы», направленных на сдерживание активности РФ на международной арене. Сознательно дискредитируется внутренняя и внешняя политика России, в инфосфере особенно, формируется образ государства, якобы нарушающего нормы международного права и подрывающего основы глобальной безопасности.

Таким образом, возрастает значимость правовой аналитики наряду с информационно-аналитической работой, актуализацией аналитических записок, осмыслением достижений различных институтов по изучению электронной информации, специализированных исследовательских центров философии информации, развития информационного общества, цифрового права и правовых основ национальной безопасности как в РФ, так и за рубежом.

Отметим, что российские субъекты информационного обеспечения внутренней и внешней политической и управленческой деятельности действуют успешно и добиваются значительных результатов. Но война информационная против России – это бессрочный проект, требующий не только постоянных ответных шагов в инфосфере и оперативного реагирования на современные информационные вызовы и кибератаки, но и стратегически продуманной государственной политики на длительную перспективу информационного позиционирования России, вовне в том числе.

Личность человека, совершающего преступные деяния в сфере электронной информации [4, с. 619–712]. Выделяют различные группы лиц, совершающих деяния в сфере электронной информации с применением информационно-телекоммуникационных технологий (ИТКТ) и информационно-телекоммуникационных сетей (ИТКС): высококвалифицированные IT-специалисты, информационные посредники (провайдеры) и компьютерные взломщики (IT-хакеры, крэкеры); психически больные (так называемыми «информационными болезнями») лица; профессиональные преступники, противоправные действия которых характеризуются прямым умыслом. Мотивы и цели совершения деяний в сфере электронной информации, связанных с цифровыми технологиями, ИТКТ, как правило, корыстные – присвоение денежных средств и чужого имущества или прав на его; либо

[12] МИД России зафиксировало в 2020 г. свыше 1 млрд кибератак на цифровые объекты // ТАСС. 29 июня 2020 г. URL: https://tass.ru/politika/8838577 (дата обращения: 13.03.2023).

политические – деяния, направленные на захват или удержание власти, ослабление политического противника, подрыв финансовой и денежно-кредитной политики, валютной системы страны, шпионаж; либо хулиганские – озорство, явное неуважение к информационному сообществу; месть, любознательность – исследовательский интерес; иные побуждения.

Возрастную группу 16–21-летних правонарушителей представляют в основном обучающиеся, которые активно ищут пути самовыражения в виртуальном мире ИТКС. Движет ими, скорее, любознательная мотивация и желание проверить свои познания, а не корыстные побуждения. К числу особенностей, указывающих на совершение компьютерного деяния вменяемыми лицами рассматриваемой категории, можно отнести: отсутствие продуманной подготовки и планирования преступления; оригинальный или не характерный способ – относительно простой в техническом исполнении; непринятие мер к сокрытию виртуальных или традиционных следов деяния; факты случайного мошенничества или немотивированного озорства.

Возрастную группу 22–28 лет представляют IT-специалисты с высшим и связанным с компьютерными науками образованием (математическим, инженерно-техническим), то есть личности вполне сформировавшиеся, обладающие определенным жизненным опытом, профессиональными IT-компетенциями и устойчивыми преступными навыками; входящие в организованные группы и преступные сообщества, технически хорошо оснащенные, специальной техникой в том числе, совершаемые ими деяния носят осознанный корыстный характер; при этом, как правило, серийные или много эпизодные преступления обязательно сопровождаются действиями по сокрытию (специальные приемы и средства, например, инсценировка следов компьютерного деяния, которые будут вести к невиновным лицам) и ими предпринимаются меры по противодействию раскрытию преступления.

Возрастную группу 29–35 лет (и старше) представляют высококвалифицированные специалисты в области цифровых технологий, нередко объединившиеся в организованную группу с лицами, имеющими высокую экономическую и юридическую подготовку, а также необходимый уровень криминального профессионализма. В этом возрасте преступникам присущи обдуманные преступления, требующие подготовки и тщательного планирования, в том числе сокрытия соответствующих следов.

На долю таких групп приходится большинство особо опасных преступлений в сфере электронной информации, должностных и/или корыстных деяний, совершаемых с использованием средств компьютерной техники, технологий и сетей (ИТКТ и ИТКС), включая присвоение денежных средств в особо крупных размерах, экономическое мошенничество. Особенности объективной стороны совершения мошеннических действий обусловлены пособничеством со стороны лиц определенных должностей и профессий, например, в экономической сфере – кредитно-финансовой или банковской.

Так, в группе «мошеннического риска» рассматривают такие профессии, как бухгалтер, работник финансовой службы, банковский служащий. Также выделяют ряд особенностей личности экономического мошенника: высокий интеллектуальный уровень, позволяющий постоянно совершенствовать механизм осуществления преступных деяний; обладание предельно устойчивыми эмоциональными и волевыми

свойствами личности; высокие потребности, что определяет особую тщательность при выборе ими способов совершения и сокрытия преступных деяний для их удовлетворения.

Для лиц, оказывающих противодействие расследованию преступлений в сфере электронной информации[13], характерно наличие значимых качеств: высокая стрессоустойчивость, проявляющаяся в том, что несмотря на повышенную реальную опасность разоблачения и наказания за совершенное деяние, эти субъекты проявляют самообладание, необходимое для принятия верных решений; способность сконцентрироваться в критических ситуациях для поиска наиболее эффективных способов выхода из них; высокая критичность в оценке складывающейся ситуации, позволяющая выбрать адекватные ситуации действия; эмоциональная устойчивость, позволяющая избегать решений, принимаемых на основе испытываемых сильных эмоций; практически нет причин для постановки их на учет в психоневрологический, наркологический диспансер; уверенность в своем интеллекте и в своих силах, позволяющая не опасаться разоблачения в оказываемом противодействии; наличие высокого интеллекта, позволяющего состязаться с интеллектом следователей (использующих государственные информационные системы, ГИС с искусственным интеллектом), или лиц, оказывающих им содействие в расследовании деяний в сфере электронной информации, или связанных с названными технологиями и сетями преступлений.

От развития инфосферы государства, от подготовки IT-специалистов и пользователей технологий и сетей (ИТКТ и ИТКС), от уровня их компетенций, знаний, умений и навыков применения ими новых технологий, зависит качество киберзащиты и противодействия киберпреступности в цифровой среде. В обеспечении безопасности инфосреды важно учитывать все аспекты криминальных деяний, особенно компьютерных преступлений, совершаемых с применением цифровых технологий и сетей, или по международному соглашению, так называемых киберпреступлений, которые считаются таковыми и в национальном (страновом) уголовном законодательстве.

Особенности аналитического обеспечения расследования преступлений, совершенных с применением электронной информации и цифровых технологий. В условиях цифровой трансформации общества развивается цифровая криминалистика, в том числе цифровая внеэкспертная, при расследовании сложных преступлений используется поиск, извлечение, восстановление, иная обработка данных в электронном виде, связанная с обнаружением и исследованием информации на электронных носителях и цифровых устройствах.

Следственный комитет России готовит специалистов по расследованию киберпреступлений. Для обучения квалифицированных специалистов в области цифровых технологий в Санкт-Петербургской, Московской академиях СК России создаются кафедры цифровых технологий и организации расследования киберпреступлений. Разработаны элективные курсы учебных дисциплин: «Основы кибербезопасности», «Использование IT-технологий при исследовании цифровых

[13] Под электронной (компьютерной) информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (Примечание 1 к ст. 272 УК РФ), то есть, включая преобразование оконечным оборудованием волоконно-оптической линии связи электрических сигналов в оптические (световые), и наоборот.

следов» [1]. Организовано электронное взаимодействие межведомственное – следственные и кадровое подразделения центрального аппарата СК России получили удаленный доступ к базам данных систем: «Безопасный город», «Безопасный регион», возможность оперативного использования электронной информации оперативно-справочных и криминалистических учетов МВД России, ФНС России, других госорганов.

Одна из форм использования специальных знаний в уголовном процессе – обладание ими (даже в малом объеме) следователем. Следователю важно знать определенный минимум специальных знаний, например, возможности судебной компьютерно-технической экспертизы, перечень вопросов, на которые она способна ответить; какая информация может быть им получена в результате проведения следственных действий в ходе расследования преступления, при совершении которого применялась та или иная цифровая технология; какое противодействие установлению истины оказывают лица, не заинтересованные в успешном завершении расследования [5]. Поэтому и целесообразно организовать обучение следователей, как и «цифровых юристов», минимуму знаний в сфере цифровых технологий для правильной оценки конкретной следственной ситуации, планирования следственные и иных процессуальных действий.

Практика показывает, что уже на момент поступления сообщения о совершении преступления правоохранительные органы нередко испытывают трудности в правильном реагировании на это сообщение: как оценить деяние по причине использования при его подготовке, совершении или сокрытии цифровых технологий, возможно, это за пределами их правовых знаний и знаний о деятельности по выявлению и закреплению информации о признаках преступления. Значит, первоочередной задачей становится определение того, какие первоначальные действия следует предпринять при получении сообщения о совершении преступления, в котором применена конкретная цифровая технология. Использование следователем специальных познаний в сфере цифровых технологий позволит еще на стадии возбуждения уголовного дела заложить основы успешного предварительного расследования и последующего судебного разбирательства.

Цифровизация юридической подготовки и профессии юриста вносит коррективы в юридическую деятельность. Так, цифровые технологии во всем мире изменяют форму отправления правосудия. Арбитражные суды в РФ ввели систему видео-конференц-связи, перевели в цифровой формат практически все документы (электронный документооборот); применение платформы LegalTech – одна из обсуждаемых тем в юридическом сообществе России. Высшие уголовные суды Англии и Уэльса перешли на виртуальные слушания дел, использование оцифрованных файлов доказательств; службу HM Courts & Tribunal Service реформировали и расширили доступ к правосудию, создав общую платформу для всех участников уголовного процесса [8, с. 122].

Важное условие успешного расследования деяний, совершенных с применением цифровых технологий, – это грамотное взаимодействие следователя с «цифровыми юристами» – лицами, обладающими специальными познаниями в цифровых технологиях. Формы и способы электронного взаимодействия отражены в частной криминалистической методике расследования преступлений с использованием цифровых технологий и телекоммуникационных сетей.

Необходима и подготовка рекомендаций по использованию специальных познаний при расследовании таких преступлений и решении проблем, с которыми сталкиваются практики и компетентные органы.

Чтобы суд вынес приговор в соответствии с действующим уголовным и уголовно-процессуальным законодательством, необходимы основные действия от компетентных органов, а именно: доказать, что само событие киберпреступления произошло, для чего определить и документировать время, место, способ, иные обстоятельства совершения деяния; доказать вину конкретных лиц в его совершении; исследовать характеризующие личность обвиняемого обстоятельства; документировать причиненный деянием вред; выявить обстоятельства, способствовавшие совершению преступления, определить меры профилактики.

Применение IT-технологий в цифровой криминалистике. Деяния в сфере компьютерной информации (киберпреступность) обратили внимание практиков и ученых на совершенствование правоохранительных профессий (правовой аналитик, «цифровой юрист», эксперт-криминалист и др.) в целях подготовки специалистов к применению достижений компьютерных наук, цифрового права, цифровой криминалистики, иных новых теорий для совершенствования методики и возможностей сбора и анализа доказательств. Так, цифровая криминалистика включает обнаружение цифровых следов, восстановление электронных данных, электронной информации, собирание электронных доказательств, криминалистический анализ цифровых технологий, компьютерных средств, цифровых данных, направленных на раскрытие и расследование преступлений, совершенных с применением телекоммуникационных технологий и сетей.

Специалист в сфере цифровой криминалистики выполняет ряд функций: сбор данных; дублирование и сохранение электронных данных, их восстановление; поиск электронных документов; преобразование мультимедиа; выступление в суде в качестве эксперта, специалиста, свидетеля; исследование компьютерных инцидентов, электронных данных; выполнение компьютерно-технической экспертизы, иные функции.

Правоохранительные органы ряда стран имеют специальные аппаратно-программные комплексы, позволяющие извлекать из смартфона представляющие служебный интерес электронные данные (информацию, текстовые сообщения, фото-, видео-, аудиофайлы); клонировать SIM-идентификатор, анализировать содержимое техники без сетевых операций и необходимости «взламывать» заблокированную PIN-кодом SIM-карту. Применяют в полевых условиях и мобильную судебную лабораторию. В целях компьютерно-технической экспертизы используют пакет Software EnCase Forensic [5, с. 163–164] как стандарт поиска цифровых улик, предоставления в суд доказательственной информации.

В специальной литературе отмечены основные проблемы [2, с. 429] развития судебно-экспертной деятельности в РФ, особенно негосударственной, – это и отсутствие ответственности за недостоверность заключения эксперта, и применение авторских методик, показавших свою неработоспособность при апробации в судебно-экспертных госучреждениях. Констатируются случаи расхождения (до 80 %) выводов первичных (негосударственных) экспертиз и повторных экспертиз (государственных, как правило), что свидетельствует

и об уровне профессиональной квалификации ряда негосударственных экспертов, и об отсутствии единых правил, методического единообразия при решении типовых (автотехнических, почерковедческих, строительно-технических) экспертных задач.

Применение цифровых технологий в уголовном процессе. При расследовании компьютерных преступлений [3, с. 882–890] исследование электронной информации и компьютерной техники возможно в следственно-экспертных ситуациях: наличие объектов преступных посягательств в виде фальсифицированных данных бухучета или иного учета, наличие защитных программных средств с признаками взлома, скорректированных либо измененных персональных данных и проч.; компьютерная информация и техника – средства совершения преступления средствами связи; компьютерная информация (или техника) характеризует определенный объект по уголовному делу, при этом не являясь объектом преступного воздействия или средством совершения преступления (данные с видеокамер наблюдения, информация о деятельности предприятия).

Особенности деяний в сфере электронной информации определяют и необходимость в исследовании их криминалистической характеристики (научной абстракции, по В.А. Мещерякову). В качестве характерных признаков выделяют: информацию о предмете преступного посягательства (вид, назначение такой информации, на которую направлено преступное посягательство, используемые при этом материальные носители для хранения и обработки электронной информации); информацию об обстановке или среде совершения преступления (вид информационного обеспечения компьютерной системы, в которой совершено преступление, порядок его действия, схема обработки и защиты информации в соответствии с назначением конкретной информационной системы); сведения о личности преступника, цели и мотивы преступного поведения при совершении данного вида преступлений; типичные способы подготовки, орудия или средства совершения деяния; обстоятельства совершения преступления (обстановка, время, место, вид выполняемой технологической операции при обработке информации); следы совершения преступления: виртуальные либо материальные (Д.А. Степаненко); характеристика исходной информации на первоначальном этапе расследования компьютерных преступлений.

Во всем мире – в странах с разными правовыми системами – система уголовного правосудия вынуждена приспосабливаться к быстро меняющимся условиям цифровизации. Изменения влияют на уголовные процедуры как на стадии расследования, так и на стадии разрешения дела, что повлекло ограничения и в области прав человека, в том числе на квалифицированную юридическую помощь.

Отметим также, что российское законодательство, во многом следуя за мировым трендом, не возражает против применения на практике цифровых технологий, методов правовой аналитики и/или предиктивной (прогнозной) аналитики, но при этом не предусматривает создание предиктивных судов, а также возможности проведения превентивных задержаний лишь на основании прогнозов, сделанных методами предиктивной аналитики, в рамках пресечения преступлений и другой деятельности компетентных органов профилактической направленности или действий упреждающего характера по отношению к индивидам и коллективам, организованным группам с отклоняющимся поведением, от которых с высокой вероятностью можно ожидать экстремистских действий.

СПИСОК ЛИТЕРАТУРЫ

1. *Бастрыкин А.И.* При расследовании сложных преступлений развивается цифровая криминалистика // Российская газета. URL: https//rg.ru/2021/10/18/bastrykin-pri-rassledovanii-prestuplenij-razvivaetsia-cifrovaia-kriminalistika.html (дата обращения: 18.01.2022).
2. *Замараева Н.А., Сальников В.П.* Проблемы проведения экспертизы в негосударственной экспертной организации // Юридическая техника. 2022. № 16. С. 427–431.
3. *Лантух Э.В., Ишигеев В.С., Грибунов О.П.* Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 882–890.
4. *Минин А.Я.* Расследование преступлений в сфере комп. информации и комп. технологий // Криминалистика: Учебник / Под ред. А.И. Бастрыкина, А.Ф. Волынского, С.В. Дубровина. 3-е изд.: перераб. и доп. М.: Юнити-Дана: Закон и право, 2017. С. 619–712.
5. *Подольная Н.Н., Подольный Р.Н.* Особенности использования специальных знаний при расследовании преступлений, совершенных с применением цифровых технологий // Огарев-online. 2023. № 1. URL: https://journal.mrsu.ru/arts/osobennosti-ispolzovaniya-specialnyx-znanij-pri-rassledovanii-prestuplenij-sovershennyx-s-primeneniem-cifrovyx-texnologij (дата обращения: 18.01.2022).
6. Обзор Forensic v7. URL: f7_0.pdf (la.by) (дата обращения: 02.04.2023).
7. *Соловьева С.М.* Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51 (289). С. 163–164.
8. *Четвернина Т.Я., Четвернина А.В.* Профессия юриста: основные векторы изменений в период цифровой трансформации // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Серия 4: Государство и право. 2022. № 3. С. 120–129.
9. *Ryan F., McFaul H.* Innovative technologies in UK legal education // Key directions in legal education. National and international perspectives. London; New York: Routledge, 2020. P. 68–69.

REFERENCES

1. Bastrykin A.I. Pri rassledovanii slozhnykh prestuplenii razvivaetsya tsifrovaya kriminalistika. Rossiiskaya gazeta. *Available at:* https//rg.ru/2021/10/18/bastrykin-pri-rassledovanii-prestuplenij-razvivaetsia-cifrovaia-kriminalistika.html (accessed: 18.01.2022).
2. Zamaraeva N.A., Salnikov V.P. Problemy provedeniya ekspertizy v negosudarstvennoi ekspertnoi organizatsii. *Yuridicheskaya tekhnika.* 2022, No. 16, pp. 427–431.
3. Lantukh E.V., Ishigeev V.S., Gribunov O.P. Ispolzovanie spetsialnykh znanii pri rassledovanii prestuplenii v sfere komp'yuternoi informatsii. *Vserossiiskii kriminologicheskii zhurnal*. 2020. Vol. 14, No. 6, pp. 882–890.
4. Minin A.Ya. Rassledovanie prestuplenii v sfere komp. informatsii i komp. tekhnologii. *Kriminalistika: Uchebnik.* Ed. by A.I. Bastrykin, A.F. Volynskii, S.V. Dubrovin. Moscow: Yuniti-Dana: Zakon i pravo, 2017, pp. 619–712.
5. Podolnaya N.N., Podolnyi R.N. Osobennosti ispolzovaniya spetsialnykh znanii pri rassledovanii prestuplenii, sovershennykh s primeneniem tsifrovykh tekhnologii. Ogarev-online. 2023, No. 1. *Available at:* https://journal.mrsu.ru/arts/osobennosti-ispolzovaniya-specialnyx-znanij-pri-rassledovanii-prestuplenij-sovershennyx-s-primeneniem-cifrovyx-texnologij (accessed: 18.01.2022).

6. Obzor Forensic v7. *Available at:* f7_0.pdf (la.by) (accessed: 02.04.2023).
7. Soloveva S.M. Primenenie tsifrovykh tekhnologii v kriminalistike. *Molodoi uchenyi.* 2019, No. 51 (289), pp. 163–164.
8. Chetvernina T.Ya., Chetvernina A.V. Professiya yurista: osnovnye vektory izmenenii v period tsifrovoi transformatsii. *Sotsialnye i gumanitarnye nauki. Otechestvennaya i zarubezhnaya literatura: IAZh. Seriya 4: Gosudarstvo i pravo*. 2022, No. 3, pp. 120–129.
9. Ryan F., McFaul H. Innovative technologies in UK legal education. *Key directions in legal education. National and international perspectives*. London; New York: Routledge, 2020, pp. 68–69.

Сведения об авторе / About Author:

Минин Анатолий Яковлевич, доктор юридических наук, профессор, профессор кафедры права, Московский педагогический государственный университет, e-mail: aya.minin@mpgu.su

Minin Anatoly Yakovlevich, ScD in Law, Professor, Professor, Law Department, Moscow Pedagogical State University, e-mail: aya.minin@mpgu.su

Статья поступила в редакцию 14.05.2025/The article was received on 14.05.2025

Статья принята к публикации 27.05.2025/The article accepted for publication 27.05.2025