КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ЦИФРОВОЙ ИНФОРМАЦИИ И СИСТЕМ ЕЕ ПЕРЕДАЧИ

Семёнова И.В.[1]

Ключевые слова: *преступления, цифровая информация, системы передачи, элементы, криминалистическая характеристика, специфика.*

Аннотация

Цель статьи: уяснить особенности преступлений в сфере цифровой информации и систем ее передачи, которые представляют собой элементы криминалистической характеристики в части, касающейся предмета преступления, и выявить новые, предложив их в качестве указанных элементов.

Материалы и методы: научные труды по исследованию вопросов расследования компьютерных преступлений, правоприменительная практика — приговоры федеральных судов.

Результаты исследования: проведен анализ обобщенной криминалистической характеристики преступлений, выделены специальные элементы, касающиеся преступлений в сфере цифровой информации, определена их взаимосвязь в их структуре.

Обсуждение и заключение: криминалистика фокусируется на определенных аспектах предметов и объектов преступления, существенных для понимания противоправных действий. Это необходимо для совершенствования методик выявления и анализа следов преступлений, улучшения работы следователей и повышения эффективности судебного процесса. В рамках заявленной тематики особое внимание следует уделить факторам противостояния совершению противозаконного действия с учетом цифровой специфики, выделив тем самым основные специальные элементы, которые непосредственно ее отражают.

DOI: 10.24412/2226-0692-2024-4-45-50

Введение

Цифровые преступления стали ключевым элементом цифровой преступности, включая обман, кражу и незаконный оборот наркотиков. Раньше преступления в этой области совершались людьми с глубокими знаниями в IT и опытом интернет-деятельности. Однако сегодня, ради увеличения прибыли и расширения клиентской базы, к этим преступлениям причастны также менеджеры и самостоятельные бизнесмены, что указывает на рост числа потенциальных преступников в этой сфере.

Преступные элементы активно используют мессенджер ICQ под вымышленными именами, предлагая пользователям деньги за выполнение определённых заданий. Они занимаются нелегальным проникновением в чужие компьютерные системы, крадут информацию, разделяя между собой роли: один предоставляет данные для входа в электронные почты и различные онлайн-сервисы, второй же занимается взломом и передачей паролей заказчику.

Основная часть

Преступления в цифровом мире часто отличаются высокой степенью сложности, и не всегда однозначно понятно, подпадает ли потеря цифровых активов под уголовную ответственность. Такая неопределенность часто встречается при анализе инцидентов, связанных с компьютерными технологиями. На начальных этапах расследования критически важно располагать специфической информацией, которая поможет установить факт наличия преступления и обосновать его квалификацию [1].

Научное сообщество демонстрирует растущий интерес к разработке методик, которые бы способствовали предупреждению, предотвращению и раскрытию преступлений такого рода.

В начальной фазе расследования следователя часто сопровождают неуверенность и недостаток данных. Следователю необходимо анализировать ограниченные данные, стремясь выявить скрытые аспекты. Эффективность этого процесса зависит от способности применять логику и структурированный подход, опираясь на предыдущий опыт и мето-

[1] Семёнова Ирина Владимировна, кандидат юридических наук, начальник кафедры публичного и частного права Военной ордена Жукова академии войск национальной гвардии Российской Федерации, г. Санкт-Петербург, Россия. E-mail: 9053202867@mail.ru

ды, которые были разработаны для расследования сходных преступлений. Это подчеркивает значимость анализа и изучения таких дел.

В следственной деятельности анализ преступления, который обеспечивает глубокое понимание механизмов его совершения, занимает приоритетное направление. Этот анализ включает разнообразную информацию: методы, используемые для преступления, характерные улики, особенности личности как нарушителя закона, так и жертвы, а также детали места преступления. Расследование, представляя собой совокупность информации, которая позволяет понять и реконструировать обстоятельства совершенного деяния, включает в себя данные о способах совершения преступлений, типичных следах, личности преступника и жертвы, а также обстановке происшествия.

Следователям помогает эффективно систематизировать информацию и выдвигать обоснованные версии использование криминалистической характеристики: например, знание характерных признаков определенного типа преступления может сократить время на поиск улик и потенциальных подозреваемых.

Кроме того, анализ криминалистических характеристик способствует разработке профилактических мер. Понимание типичных методов совершения правонарушений позволяет правоохранительным органам предвидеть возможные угрозы и разрабатывать стратегии по их предотвращению. Предупреждение противоправного поведения, как хорошо известно, является важным средством борьбы с преступностью [2—5].

Таким образом, криминалистическая характеристика является незаменимым инструментом в арсенале современного следователя, повышающим эффективность раскрытия преступлений и обеспечивающим безопасность общества.

Важность особенностей криминалистической оценки напрямую зависит от конкретного типа преступлений, так как у каждого из них есть своя специфика. Эту мысль изначально выразил В.Д. Зеленский, который указал на уникальность каждой преступной категории [6, с. 8—11].

Криминалистическая характеристика преступления выполняет несколько ключевых функций: информационная, служебная. Характеристики определенного вида преступления служат важным инструментом для расследования. Они помогают формировать гипотезы и стандартные модели для выявления ключевых доказательств, создавая тем самым общую модель преступления. Это важно также для прогнозирования, поскольку на основе полученных данных можно разработать целенаправленные рекомендации. Эти рекомендации улучшают организационную структуру расследования определенных преступлений и включают в себя тактические и криминалистические методы для проведения следственных действий [7, с. 152].

Концепция криминалистической характеристики является отдельным элементом в структуре методов криминалистического исследования. Этот аспект выделяет особенности и характеристики, характерные для определенного типа преступлений, и образует индивидуальный подход к их изучению. Криминалистическая характеристика объединяет уникальные черты и схемы, которые отражают специфику каждого вида преступления [8, с. 89].

При этом другие ученые отмечают отдельные факторы, которые влияют на совершение преступления, такие как уязвимости в защите информационных систем корпоративных сетей, сосредоточение важных данных в неадекватно защищенных базах, возможность нелегального доступа к информации для неуполномоченных лиц, при этом отмечая проблему недостаточной подготовки сотрудников правоохранительных структур в области выявления и исследования киберпреступлений, которая снижает вероятность раскрытия таких дел, что создает благоприятные условия для их совершения [9, с. 115].

Отдельные авторы, давая криминалистическую характеристику преступлениям в рассматриваемой сфере, выделяют необязательную часть криминалистического описания преступлений, которая затрагивает противодействие работе правоохранителей. Это связано с особыми законами, влияющими на процесс расследования и выходящими за его пределы. Такой элемент часто встречается в преступлениях с высокими технологиями и в деяниях организованных групп. В него входят лица, мешающие следствию, и методы влияния на информацию и участников расследования. Можно также учесть другие, менее важные аспекты, вроде условий препятствия [10, с. 219].

Преступления, направленные против систем цифровой коммуникации и самой цифровой информации, составляют уникальную группу, которую следует именовать «цифровые преступления». Они обладают специфическими характеристиками, что позволяет выделить их в отдельную группу для более детального изучения. Подобные правонарушения охватывают широкий спектр деяний, и их криминалистический анализ уже был темой множества исследований. Такая работа помогает усовершенствовать методы расследования и обогащает теорию криминалистики новыми подходами и определениями.

Ученые, занимающиеся изысканием проблем характеристики преступления, часто оперируют терминами «криминологическая» и «криминалистическая», которые представляют собой дихотомию понятия «знания» человека о событиях и участниках совершенного преступления.

Данные, полученные при исследовании вопросов элементов криминалистической характеристики, дали основание Е.А. Старцевой полагать о наличии необходимости выделения таких ключевых компонентов в структуре преступной активности, как: лицо, совершающее преступление; условия, при

DOI: 10.24412/2226-0692-2025-1-45-50

которых оно совершается; методы, используемые для этого; и следы, оставляемые после совершения преступления. Другие элементы, по ее мнению, отображают уровень противодействия определённым видам преступлений и их распространённость [11, с. 110]. Хочется обратить внимание на сложившийся ситуационный подход, который доказал практическую значимость в достижении необходимого или желаемого результата.

Среди особенностей криминалистической характеристики преступлений в сфере цифровой информации А.А. Бессонов выделяет следующие элементы: орудие преступления — информационные технологии; дистанционность и возможность сетевого совершения; неприкосновенность к их совершению [12, с. 35; 13].

В процессе детального анализа преступлений, связанных с цифровой информацией, критически важно выявлять стандартные категории данных: детали методов совершения преступлений, способы их скрытия, а также меры противодействия в процессе следствия. Важно учитывать информацию о личности злоумышленника, его поведении, а также о жертвах и их действиях до, во время и после инцидента. Необходимо рассматривать пространственно-временные аспекты места события, мотивы, связанные с использованием информационных технологий, и их влияние на ход события. Имея в виду уникальность таких преступлений, следует признать, что нет универсального согласия относительно ключевых элементов криминалистической структуры в контексте компьютерных преступлений.

Исследования в области криминалистики указывают на то, что ученые сходятся во мнении относительно основополагающих элементов преступлений, в том числе в контексте цифровых преступлений. Основные категории и критерии их систематизации у различных авторов примерно схожи. Компоненты криминалистического анализа тесно взаимосвязаны, формируя структуру, которая должна содержать лишь информацию, способствующую продвижению от зафиксированных фактов к неизвестным данным и последовательному построению логики расследования [14].

Таким образом, можно прийти к выводу, что в результате изучения признаков преступлений, относящихся к 28 главе Уголовного кодекса Российской Федерации (ст. 272—274.2), были выделены две ключевые категории. Одна из них охватывает характеристики, связанные с личностью правонарушителя. Это включает в себя уровень его умственных способностей, знание информационных технологий, особенности психологии и поведения, финансовое состояние, а также степень уязвимости к кибератакам. Другая группа характеристик, акцентирующая внимание на поведении субъекта преступления и вытекающих из этого последствиях, включает разнообразные аспекты. К ним относятся методы, применяемые во время совершения преступления, следы, оставленные на месте происшествия, взаимоотношения между злоумышленником и его жертвой, а также контекст и обстоятельства преступления.

Концепция криминалистической характеристики отображает знания следователя о преступлении, объединяющие всю необходимую для расследования информацию. Эти сведения помогают формировать обоснованные предположения и эффективно проводить действия по раскрытию преступления. Таким образом, важно выстроить структуру данных знаний в определённой последовательности.

Представляется возможным предложить определять «криминалистическую характеристику преступлений в сфере цифровой информации» как систематизированное изложение множества подлинных фактов и научных выводов в отношении наиболее распространенных элементов, составляющих преступную деятельность в сфере цифровой информации, необходимых для создания формирования базы фактов, установленных и проверенных, в целях выдвижения следственных теорий и определения основных путей расследования и принятия обоснованных и законных процессуальных решений.

В центре внимания при анализе структуры преступлений, связанных с цифровой информацией, находится объект преступных действий, иначе говоря, знания. Слово «знания» здесь означает не всё множество информации, доступной или обнаруживаемой в ходе расследования преступления, а те данные, которые становятся достоверно известны следствию в процессе оперативных мероприятий и экспертиз. Это и есть та информация, на основе которой строится дальнейшее расследование.

В сфере цифровых преступлений предметом выступает информация — это данные, их надежность, неизменность и инфраструктура для их трансляции. Важно подчеркнуть, что в рамках этого рода незаконных действий цифровой характер информации является существенным условием.

Дела, касающиеся нарушений в области цифровых данных, хранящихся на устройствах, внутри их систем и сетевых структур, следует квалифицировать не просто как компьютерные преступления, а как деяния, затрагивающие цифровую информацию. Ведь цифровые записи представляют собой не что иное, как наборы сигналов, организованные в форме цифрового кода [15, с. 23].

Основой для анализа преступлений, совершенных в цифровом пространстве, служат данные о факте преступления. Важны такие характеристики цифровых данных, как целостность, подлинность, защищённость и легальность передачи. Расследование таких преступлений требует информации о местоположении данных и способах их защиты. Формат информации имеет ключевое значение, поскольку без цифрового вида она не может быть предметом преступления в сфере цифровой информации. Знание предмета преступления позволяет субъектам, проводящим расследование, сформировать

эффективную команду, включая IT-специалистов, для поиска и извлечения и анализа цифровых доказательств. Неверные действия во время сбора доказательств, такие как отключение электронных устройств, могут привести к их потере [16]. В связи с этим можно выделить специфические элементы криминалистической характеристики, свойственные преступлениям в сфере цифровой информации и систем ее передачи.

Информация о потерпевшем: данные о человеке (его пол, возраст, уровень дохода и общественное положение; насколько он разбирается в цифровых технологиях и защите информации, а также насколько активен в соцсетях) или сведения о компании (отрасль работы, количество работников, стабильность рабочих мест).

Сведения о защите цифровой информации: для обеспечения надёжной работы компаний важно сохранять конфиденциальность данных и оберегать их от неправомерного доступа или перехвата. В связи с этим значимым элементом криминалистической характеристики будет защита цифровой информации. При этом следует различать информационную безопасность (на англ. InfoSec) — это состояние систем, при котором элементы её инфраструктуры, например, оборудование, каналы передачи данных и хранилища данных, устойчивы к внешним и внутренним угрозам, и цифровую безопасность, которая предполагает защиту цифровой информации от кражи в интернет-пространстве. Информационная безопасность включает методы защиты информации, которая может храниться на различных носителях — в облачном хранилище, на серверах и на обычной печатной бумаге.

Обеспечение защиты требует проведения различных мероприятий, цель которых — обеспечить сохранность электронных документов, переговоров и другой информации, требующей конфиденциальности. Блокирование и установка препятствий для любых тайных подключений является важной частью обеспечения безопасности данных, поскольку в настоящее время существует множество способов для удаленного незаконного подключения.

В области защиты информации применяются разнообразные методы, направленные на предотвращение доступа к данным несанкционированных лиц. Одним из них является создание преград, как физических, так и виртуальных, способствующих усложнению задачи потенциальных взломщиков (это может включать в себя управление безопасностью системы или её модификацию). Ещё один инструмент — это использование криптографии для скрытия или изменения информации, делая её недоступной для посторонних. Кроме того, важную роль играют юридические меры и разработка процедур, которые должны стимулировать сотрудников к соблюдению правил в обработке данных. Путём установления правил или создания определённой рабочей среды можно достигнуть соблюдения протоколов безопасности. Эти два направления — принуждение к соответствию нормам и мотивация к правильному поведению — являются ключевыми стратегиями в обеспечении информационной безопасности, для которых применяются различные ресурсы, включая технические и организационные инструменты.

Преступления в сфере цифровой информации включают действия, нарушающие нормы, поддерживающие целостность и безопасность информационных систем. Характерной чертой таких нарушений является сознательное вмешательство или недобросовестность, скрывающаяся за внешней небрежностью. Так, например, некоторые нарушения могут быть совершены с целью экстремизма, под видом технической халатности; критически важно различать их. Ввиду того, что информационно-коммуникативные сети являются частью соименной инфраструктуры, любое нарушение нельзя списывать на простую ошибку или халатность без учета умысла. В связи с указанными обстоятельствами защита, предоставляемая системами, важна для идентификации возможного злоумышленника и методов, которые он использовал для сокрытия своей деятельности и похищения конфиденциальных данных. Для выяснения, каким образом вредоносное ПО проникло к жертве и как преступник маскировал свои действия, требуются специальные знания и навыки в области IT.

Условия, благоприятные для совершения преступления, и лѝца, их создавшие: в ходе расследования преступлений важно выявить тех, кто мог способствовать нарушениям, и оценить их роль в создании условий, которые способствуют совершению преступления в организациях и учреждениях. В таких ситуациях важно обнаружить любые отступления от требований и правил в соответствующей области, а также исследовать психоэмоциональную, поведенческую реакцию сотрудников и руководства на эти нарушения. Такие меры помогают определить как потенциальных участников и соучастников преступления, так и условия, которые могли им в этом способствовать. Необходимо также уделить внимание работникам других отделов, так как среди них могут быть свидетели или очевидцы подготовки преступления.

Заключение

Для определения фактов преступной деятельности следует исследовать все обстоятельства, которые могут указывать на совершение умышленного преступления. При обнаружении доказательств не стоит ограничиваться только очевидными данными, так как истинные причины и последствия могут быть связаны с другими факторами. Определение обстоятельств, имеющих отношение к преступлению, поможет выявить реальную картину событий и предотвратить в будущем совершение серьезных

DOI: 10.24412/2226-0692-2025-1-45-50

преступлений с потенциально более тяжкими последствиями.

На основе исследования, проведенного через призму толкования категории «преступления в сфере цифровой информации», представляется возможным выделить специфические элементы характеристики таких преступлений, что обеспечит лучшее понимание их взаимосвязанности и взаимозависимости. В качестве фундамента для создания криминалистической модели предлагается использовать профессиональные знания сотрудника, полученные в результате проведения оперативно-следственной и экспертной работы.

Литература

1. Захарцев С.И., Кийко А.Ю., Семенова И.В. Цифровая информация как квалифицирующий признак формирования частной методики расследования преступлений // Юридическая наука: история и современность. 2022. № 11. С. 126—134.
2. Сальников В., Захарцев С. Преступления, которых могло не быть // Защита и безопасность. 2020. № 4 (95). С. 30—31.
3. Виноградова Е.В., Захарцев С.И., Сальников В.П. Профилактика преступности: от концепта к конструкту // Юридическая наука: история и современность. 2023. № 3. С. 111—119.
4. Петровский А.В. Институционно-нормативная система предупреждения преступного поведения: теоретико-прикладное исследование : дис. ... докт. юрид. наук. 5.1.4. Краснодар : Кубанский государственный ун-т, 2024. 597 с.
5. Яковлева М.А. Органы внутренних дел как один из субъектов в системе профилактики преступности : автореф. дис. … канд. юрид. наук. 12.00.08. СПб. : Санкт-Петербургский ун-т МВД России, 2019. 23 с.
6. Криминалистическая методика расследования отдельных видов и групп преступлений / В.Д. Зеленский и др. Краснодар : КубГАУ, 2013. 355 с.
7. Сафонова Ю.С. Криминалистическая характеристика преступления: понятие и назначение // Форум. 2023. № 1 (30). С. 151—154.
8. Харзинова В.М., Небратенко Г.Г. Криминалистическая характеристика умышленного распространения заведомо ложной информации в СМИ и телекоммуникационных сетях // Вестник Уфимского юридического института МВД России. 2022. № 2 (96). С. 88—93.
9. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АлтГУ. 2013. № 2 (78). С. 114—116.
10. Поляков В.В. Высокотехнологичные преступления: концептуальные основы криминалистической методики расследования // Вестник Томского гос. ун-та. 2024. № 498. С. 217—224.
11. Старцева Е.А. Особенности криминалистической характеристики мошенничества в сфере компьютерной информации // Научный вестник Омской академии МВД России. 2021. Т. 27. № 2 (81). С. 109—113.
12. Бессонов А.А. О некоторых направлениях совершенствования криминалистического обеспечения расследования киберпреступлений // Расследование преступлений: проблемы и пути их решения. 2024. № 2 (44). С. 31—37.
13. Бессонов А.А. Киберпреступность: тенденции и перспективы // Расследование преступлений: проблемы и пути их решения. 2024. № 3 (45). С. 23—30.
14. Корнакова С.В. Содержание и значение криминалистической характеристики преступления (на примере насильственных половых преступлений, совершенных несовершеннолетними в отношении несовершеннолетних) // Российский следователь. 2019. № 5. С. 14—15.
15. Бегишев И.Р., Бикеев И.И. Преступления в сфере обращения цифровой информации. Казань : Познание, 2020. 299 с.
16. Семенова И.В. Преступления в сфере компьютерной информации как элемент киберпреступности // Право и управление. 2023. № 3. С. 114—119.

THE CRIMINALISTICS CHARACTERISATION OF OFFENCES IN THE FIELD OF DIGITAL INFORMATION AND SYSTEMS FOR ITS TRANSFER

Irina Semenova[2]

Keywords: *offences, digital information, transfer systems, elements, criminalistics characterisation, specifics.*

Abstract

Purpose of the paper: clarifying the specific features of offences in the field of digital information and systems for its transfer which are elements of the criminalistics characterisation as regards the target of the crime, and to identify new ones, suggesting them in the capacity of the said elements.

Materials and methods used in the study: research works on the matter of investigating computer crimes and law enforcement practice, i. e. judgments of federal courts.

[2] Irina Semenova, Ph.D. (Law), Head of the Department of Public and Private Law of the Military Academy of the National Guard Troops of the Russian Federation, Saint Petersburg, Russian Federation. E-mail: 9053202867@mail.ru

Study findings: an analysis of the generalised criminalistics characterisation of offences was carried out, special elements related to offences in the field of digital information were singled out, and their interrelations within their structure were determined.

Discussion and conclusions: criminalistics is focused on certain aspects of targets and objects of crime which are essential for understanding unlawful actions. It is needed to improve the methodologies for identifying and analysing the traces of crime, bettering the work of investigators and raising the efficiency of the judicial process. Within the framework of the topics of this work, special focus should be made on factors of counteracting the commission of illegal actions considering the specifics of the digital sphere, emphasising thus the main special elements directly reflecting the specifics.

References

1. Zakhartsev S.I., Kiiko A.Iu., Semenova I.V. Tsifrovaia informatsiia kak kvalifitsiruiushchii priznak formirovaniia chastnoi metodiki rassledovaniia prestuplenii. Iuridicheskaia nauka: istoriia i sovremennost'. 2022. No. 11. Pp. 126–134.
2. Sal'nikov V., Zakhartsev S. Prestupleniia, kotorykh moglo ne byt'. Zashchita i bezopasnost'. 2020. No. 4 (95). Pp. 30–31.
3. Vinogradova E.V., Zakhartsev S.I., Sal'nikov V.P. Profilaktika prestupnosti: ot kontsepta k konstruktu. Iuridicheskaia nauka: istoriia i sovremennost'. 2023. No. 3. Pp. 111–119.
4. Petrovskii A.V. Institutsionno-normativnaia sistema preduprezhdeniia prestupnogo povedeniia: teoretiko-prikladnoe issledovanie : dis. ... dokt. iurid. nauk. 5.1.4. Krasnodar : Kubanskii gosudarstvennyi un-t, 2024. 597 pp.
5. Iakovleva M.A. Organy vnutrennikh del kak odin iz sub"ektov v sisteme profilaktiki prestupnosti : avtoref. dis. … kand. iurid. nauk. 12.00.08. SPb. : Sankt-Peterburgskii un-t MVD Rossii, 2019. 23 pp.
6. Kriminalisticheskaia metodika rassledovaniia otdel'nykh vidov i grupp prestuplenii. V.D. Zelenskii i dr. Krasnodar : KubGAU, 2013. 355 pp.
7. Safonova Iu.S. Kriminalisticheskaia kharakteristika prestupleniia: poniatie i naznachenie. Forum. 2023. No. 1 (30). Pp. 151–154.
8. Kharzinova V.M., Nebratenko G.G. Kriminalisticheskaia kharakteristika umyshlennogo rasprostraneniia zavedomo lozhnoi informatsii v SMI i telekommunikatsionnykh setiakh. Vestnik Ufimskogo iuridicheskogo instituta MVD Rossii. 2022. No. 2 (96). Pp. 88–93.
9. Poliakov V.V. Obstanovka sovershenіia prestuplenii v sfere komp'iuternoi informatsii kak element kriminalisticheskoi kharakteristiki. Izvestiia AltGU. 2013. No. 2 (78). Pp. 114–116.
10. Poliakov V.V. Vysokotekhnologichnye prestupleniia: kontseptual'nye osnovy kriminalisticheskoi metodiki rassledovaniia. Vestnik Tomskogo gos. un-ta. 2024. No. 498. Pp. 217–224.
11. Startseva E.A. Osobennosti kriminalisticheskoi kharakteristiki moshennichestva v sfere komp'iuternoi informatsii. Nauchnyi vestnik Omskoi akademii MVD Rossii. 2021. T. 27. No. 2 (81). Pp. 109–113.
12. Bessonov A.A. O nekotorykh napravleniiakh sovershenstvovaniia kriminalisticheskogo obespecheniia rassledovaniia kiberprestuplenii. Rassledovanie prestuplenii: problemy i puti ikh resheniia. 2024. No. 2 (44). Pp. 31–37.
13. Bessonov A.A. Kiberprestupnost': tendentsii i perspektivy. Rassledovanie prestuplenii: problemy i puti ikh resheniia. 2024. No. 3 (45). Pp. 23–30.
14. Kornakova S.V. Soderzhanie i znachenie kriminalisticheskoi kharakteristiki prestupleniia (na primere nasil'stvennykh polovykh prestuplenii, sovershennykh nesovershennoletnimi v otnoshenii nesovershennoletnikh). Rossiiskii sledovatel'. 2019. No. 5. Pp. 14–15.
15. Begishev I.R., Bikeev I.I. Prestupleniia v sfere obrashcheniia tsifrovoi informatsii. Kazan' : Poznanie, 2020. 299 pp.
16. Semenova I.V. Prestupleniia v sfere komp'iuternoi informatsii kak element kiberprestupnosti. Pravo i upravlenie. 2023. No. 3. Pp. 114–119.

DOI: 10.24412/2226-0692-2025-1-45-50