Научная статья
УДК 343.985.7:343.3/.7:004.77(470)

Роман Александрович Кокорев
Московский областной филиал Московского университета МВД России имени В. Я. Кикотя, Руза, Россия, Kokorev_Roman@mail.ru

АКТУАЛЬНЫЕ АСПЕКТЫ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматривается классификация ключевых элементов криминалистической характеристики преступлений, совершенных с использованием информационных технологий. Приведен анализ взглядов исследователей в отношении следов преступления и личности преступника. Предложена дифференциация этапов совершения преступлений с использованием информационных технологий. Обращено внимание на вопросы совершенствования методики расследования рассматриваемых преступлений.

Ключевые слова: компьютерные преступления, киберпреступления, информационные технологии, криминалистическая характеристика, преступления в сфере информационных технологий, методика расследования преступлений

Для цитирования: Кокорев Р. А. Актуальные аспекты методики расследования преступлений, совершенных с использованием информационных технологий // Общество, право, государственность: ретроспектива и перспектива. 2024. № 1 (17). С. 56–64.

Original article

Roman A. Kokorev
Moscow regional branch of Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikotya, Ruza, Russia, Kokorev_Roman@mail.ru

CURRENT ASPECTS OF THE METHODOLOGY FOR INVESTIGATING CRIMES COMMITTED USING INFORMATION TECHNOLOGY

Abstract. The article discusses the classification of key elements of the forensic characteristics of crimes committed using information technology. An analysis of the views of researchers regarding the traces of a crime and the identity of the criminal is presented. A differentiation of the stages of crimes committed using information technology is proposed. Attention is drawn to the issues of improving the methodology for investigating the crimes under consideration.

Keywords: computer crimes, cybercrimes, information technology, forensic characteristics, crimes in the field of information technology, crime investigation techniques

For citation: Kokorev R. A. Current aspects of the methodology for investigating crimes committed using information technology // Society, law, statehood: retrospective and perspective. 2024 No. 1 (17). P. 56–64. (In Russ.)

Введение

За последнее десятилетие количество преступлений, совершаемых в сфере использования информационно-телекоммуникационных технологий, резко возросло. На проблему противодействия киберпресту-

плениям неоднократно указывал в своих выступлениях Президент Российской Федерации В. В. Путин. В 2023 г. на расширенном заседании коллегии МВД России глава государства вновь обратил внимание на остроту данного, безусловно, проблемного вопроса[1]. Согласно результатам официальных статистических данных, «в январе–ноябре 2023 г. зарегистрировано 614,8 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 30,8 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8 % в январе–ноябре 2022 г. до 34,1 %»[2]. Отметим, что уровень профилактики и раскрываемости преступлений, совершаемых с использованием информационных технологий, остается невысоким.

В таких обстоятельствах требуется поиск путей оптимизации, повышения эффективности организации и проведения мероприятий по расследованию киберпреступлений. И, на наш взгляд, «флагманом» такого поиска должно выступить криминалистическое обеспечение методики расследования данной категории преступлений. Вне развития и совершенствования соответствующих частных и общих аспектов данной методики, без их имплементации в правоохранительную деятельность успешность работы по расследованию и профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий, крайне сомнительна. В этой связи требуется исследование общетеоретических и практических вопросов совершенствования методики расследования рассматриваемых преступлений.

Методы

В исследовании применялись диалектический метод как всеобщий универсальный метод познания, общенаучные формально-логические методы познания (анализ и синтез, дедукция и индукция, аналогия), системный подход.

Результаты

Одним из основных направлений развития криминалистической науки можно считать выработку криминалистической характеристики преступлений, в которой важное место отводится именно орудиям совершения преступлений [1, с. 27]. В рассматриваемом контексте к орудиям совершения рассматриваемых преступлений можно отнести техническое и сетевое оборудование, используемое злоумышленниками, так как реализация преступных замыслов невозможна без использования указанных устройств [2, с. 32].

Анализ материалов судебной и следственной практики позволяет выделить несколько основных видов технического и сетевого оборудования, которое используется злоумышленниками при совершении преступлений с использованием информационных технологий.

Во-первых, это технические устройства. Наиболее распространенным техническим устройством, фигурирующим в уголовных делах рассматриваемой категории, является мобильный телефон с функцией выхода в сеть Интернет. С его помощью злоумышленники подключаются к сети Интернет, осуществляют поиск жертв (или иных объектов посягательства), вступают с ними в контакт, совершают непосредственно преступные деяния. Помимо мобильных телефонов, при совершении рассматриваемых преступлений могут быть также использованы стационарные компьютеры, ноутбуки или планшеты.

Во-вторых, это устройства, предназначенные для подключения и доступа в сеть Интернет. Не во всех случаях злоумышленники используют внутреннюю функцию самого мобильного телефона для доступа в

[1] Выступление В. В. Путина на заседании коллегии МВД России 20 марта 2023 года // Президент России. URL: http://www.kremlin.ru/events/president/transcripts/70744 (дата обращения: 11.01.2024).

[2] Краткая характеристика состояния преступности в Российской Федерации за январь–ноябрь 2023 года. https://мвд.рф/reports/item/45293174/ (дата обращения: 15.01.2024)

сеть. В большинстве стационарных компьютеров, а также ноутбуков данная функция вообще отсутствует. В этой связи преступниками могут использоваться специальные технические устройства – Wi-Fi-роутеры. В отдельных случаях, в целях сокрытия следов своей преступной деятельности, злоумышленники используют Wi-Fi-роутеры, установленные в общественных местах.

В-третьих, это отдельные виды технического и сетевого оборудования (коммуникаторы, адаптеры сети, концентраторы, сетевые карты, маршрутизаторы, мультиплексоры, шлюзы и др.).

В целях реализации преступных планов злоумышленники используют следующие технические устройства и сетевые средства.

1. VPN-сервисы. Данные средства представляют собой безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность.

2. Сетевые соединения, хостинги, сетевые провайдеры, вышки сотовой связи. Данные средства используются для обеспечения интернет-соединения, увеличения скорости поступления информации.

3. Различные интернет-приложения. К примеру, социальные сети, мессенджеры. Также для реализации своих преступных намерений злоумышленники могут использовать и другие приложения. Например, это могут быть приложения, корректирующие голос человека (используются в случае, если с жертвой осуществляются телефонные переговоры, и преступник не хочет, чтобы жертва слышала его настоящий голос), внешность и др.

Следующим элементом криминалистической характеристики, который объединяет преступления, совершенные с использованием информационно-телекоммуникационных технологий, и позволяет говорить о них как об общности, выступают электронные следы преступления, которым в юридической литературе уделяется пристальное внимание [3, с. 204–208; 4, с. 226–230; 5, с. 136–141; 6, с. 120–123]. При рассмотрении этого вопроса нами учитывается классификация электронных следов, предложенная В. А. Перовым [7, с. 94–96] и принятая многими авторами. Обратим внимание на две разновидности электронных следов, а именно, статическом и динамическом. В первом случае речь идет о следообразовании, происходящем на неподвижной основе (например, это может быть IP-адрес). Во втором случае речь идет об образовании следов на движущейся основе (например, в результате совершения различных действий со стороны злоумышленников).

Относительно места совершения преступления киберпреступления могут быть определены через понятие информационно-телекоммуникационного пространства. Именно последнее чаще всего выступает местом совершения преступных деяний. Прежде всего, это может быть информационно-телекоммуникационная сеть Интернет.

Следующим элементом криминалистической характеристики рассматриваемых преступлений выступает личность преступника. Характеристика личности преступника занимает важное место в понимании механизма следообразования рассматриваемых преступлений.

Представляет определенный научный интерес классификация предложенная Э. Т. Халилуллиной. На основе проведенного исследования она выделяет следующие типы личности злоумышленников, совершающих компьютерные преступления [8, с. 91]:

– хакеры – обладающие высокой степенью знаний в сфере информационных технологий, совершающие преступления путем взлома защитных систем с целью причинения ущерба данным, хищения информации, нанесения иного вреда;

– киберпреступники – получающие доступ к данным в корыстных целях не путем взлома систем, а путем обмана, злоупотребления доверием и т. д.;

– шпионы – лица, добывающие информацию в сети;

– кибертеррористы – выводящие из строя сети и системы различных организаций и предприятий в определенных целях (корысть, для того, чтобы заставить организации совершить определенные действия и др.).

В свою очередь, полагаем, что можно ограничиться классификацией, предлагаемой А. Л. Осипенко [9, с. 62]:

– традиционные преступники – лица, осознавшие возможности и преимущества информационных технологий для совершения хищений денежных средств;

– представители хакерского сообщества – лица, обладающие специальными знаниями в сфере компьютерных технологий, совершающие деяния, которые возможны только в данной сфере (ввод, блокировка, уничтожение и информации и т. д.).

По мнению исследователей, киберпреступления совершаются лицами мужского пола, в возрасте от 18 до 24 лет, преимущественно имеющими высшее или среднее специальное образование [10, с. 189].

Преступная деятельность, как и любая другая целенаправленная деятельность, может быть разделена на этапы в зависимости от степени достижения результата. Последовательность действий лица, совершающего преступления с использованием информационных технологий, необходимо рассматривать с учетом обязательной привязки к использованию технических средств и сетевого оборудования. Проведенный анализ следственной и судебной практики позволил выделить несколько основных этапов совершения преступлений с использованием информационных технологий.

Первый этап – это возникновение умысла на совершение преступления, а также осознание возможности (необходимости) использования при этом информационных технологий. Умысел может возникнуть в силу различных обстоятельств и под воздействием разных, по своей сути и содержанию, акторов. Например, это может быть реализация потребности незаконного обогащения (корыстный мотив), осуществление коммерческого интереса и др.

Второй этап – это создание условий, необходимых для реализации преступного умысла. В рамках данного этапа осуществляется множество действий (создание необходимого информационного ресурса, поиск объекта совершения преступления, жертвы и др.).

Третий этап – непосредственное совершение преступления. В зависимости от конкретного вида преступления содержание данного этапа может быть различным. Определяющее значение в данном случае следует отводить тем средствам, которые используются преступниками для реализации своих противоправных замыслов. В данном случае следует отметить, что в значительной степени распространено использование средств мобильной связи и расчетных (пластиковых) карт. Эти средства в основном используются для совершения хищений – краж и мошенничеств. В особенности это проявляется при совершении преступлений на бесконтактной основе. Так, например, для бесконтактных мошенничеств в плане определения обстановки их совершения важное значение имеют условия, создание и обеспечение которых позволяет реализовывать соответствующие преступные замыслы по хищению собственности, путем обмана или злоупотребления доверием.

К таковым условиям следует относить наличие специальных технических средств и специальных технологических возможностей. В первом случае речь идет о технических средствах, которые злоумышленники используют в качестве предметов преступных посягательств – мобильные телефоны, смартфоны, средства электронных платежей, компьютеры, планшеты и т. д. Особое значение в данном случае имеют электронные платежные системы. Именно посредством них совершается значительная часть мошеннических действий, схем и операций.

Отдельно следует учитывать использование преступниками различных программных средств. В данном случае следует выделять несколько основополагающих тенденций.

1. Использование преступниками различных программных средств, которые позволяют анонимизировать «преступный след» (свою преступную деятельность) и сам факт использования тех или иных технологий.

2. Использование специальных программ, предназначенных для шифрования.

3. Использование различных сайтов-зеркал.

4. Активное использование криптовалюты, а также электронных платежных систем.

5. Использование электронной цифровой подписи в целях совершения мошенничеств.

Четвертый этап – это сокрытие следов преступной деятельности. Отметим, что по множеству преступлений меры, направленные на сокрытие следов, принимаются злоумышленниками на первоначальных стадиях своей противоправной деятельности. В частности, это может быть использование VPN-сервисов, а также различных программ «анонимайзеров», которые позволяют пользоваться сетевыми ресурсами с сокрытием данных об IP-адресе, а также иных сведений, позволяющих установить конечного пользователя. На стадии после совершения преступления, злоумышленники также предпринимают различные меры. В частности, это может быть стирание переписки, удаление аккаунта, «чистка» истории браузера, смена мобильного телефона и других технических устройств, физическое скрытие (переезд в другой город) и т. д.

Основной задачей при расследовании рассматриваемых преступлений является обнаружение максимально возможного количества следов совершенного деяния, их фиксация и изъятие. В дальнейшем данные следы должны привести к конкретному лицу, совершившему то или иное преступление и использовавшему для этого соответствующие информационные технологии.

Работа со следами во многом обеспечивается посредством производства следственных действий. В этой связи важно обеспечивать, во-первых, правильную последовательность и своевременность производства следственных действий (методический аспект), во-вторых, верную тактику их производства (тактический аспект).

Начальной точкой проведения следственных действий по уголовным делам рассматриваемой категории является место происшествия. В большинстве научных источников указывается, что первоначальным следственным действием при расследовании преступлений данной категории выступает осмотр места происшествия [11, с. 135–143].

После работы на месте происшествия необходимо получить дополнительную информацию о преступлении из так называемых внешних источников. Необходимость данной задачи обусловлена тем, что интернет-соединение, функционирование социальных сетей обеспечивается отдельно взятыми организациями. Для получения максимально доказательственной информации необходимо составить ряд запросов. Во-первых, следует направить запросы представителю юридического лица – социальной сети, в рамках функционирования которой совершалось преступление («Вконтакте», «Телеграм» и др.). Как правило, предмет запрашиваемой информации составляют: адрес личной страницы пользователя; дата создания страницы; номер телефона и электронной почты пользователя; IP-адреса, с которых пользователь осуществлял вход на страницу; история изменений пароля, логина (имени пользователя), номера телефона; история обращений в службу поддержки; история блокировок страницы пользователя. Во-вторых, следует запросить разрешение (санкцию) суда для возможности получения сведений, затрагивающих конституционные права граждан (право на личную, семейную тайну) [12, с. 118]. Реализация данного мероприятия осуществляется в случае необходимости доступа следователя к соответствующим данным.

Важнейшим этапом расследования преступлений рассматриваемой категории является назначение и производство судебных экспертиз. Следует отметить многочисленность возможных вариантов и видов судебных экспертиз, которые могут быть проведены при расследовании преступлений, совершенных с использованием информационных технологий. При этом все проводимые экспертизы условно можно подразделить на два вида.

Первый вид судебных экспертиз обусловлен отраслевой спецификой данных

преступлений, а именно их совершением с использованием информационных технологий. Чаще всего по таким делам назначается и проводится судебная компьютерно-техническая экспертиза. Так, до недавнего времени выделялись различные виды судебных компьютерно-технических экспертиз (информационная, программная, сетевая и др.). Вместе с тем практика показывает, что на сегодняшний день при расследовании уголовных дел соответствующей категории чаще всего проводится именно комплексная экспертиза, в рамках которой уточняются все интересующие вопросы. Поэтому в постановлении на производство судебной экспертизы целесообразно указывать родовое наименование экспертизы – «судебная компьютерно-техническая экспертиза» [13, с. 278].

Установив необходимость производства судебной компьютерно-технической экспертизы, следователь должен определить ряд аспектов. Прежде всего, это объекты, которые будут представлены эксперту для производства соответствующего экспертного исследования. Зачастую таковыми объектами выступают компьютерное или иное техническое устройство, с которого производилось подключение и выход в глобальную информационно-телекоммуникационную сеть.

Далее следователю необходимо сформулировать вопросы, которые будут поставлены перед экспертом для их разрешения. Конечные перечни вопросов, как правило, определяются в зависимости от конкретных обстоятельств и типовой следственной ситуации, сложившейся на момент расследования уголовного дела. Вместе с тем можно утверждать о более или менее общих направлениях, в рамках которых должны быть сформулированы вопросы.

Первое направление – это характеристика компьютерного или иного технического устройства (марка, модель, индивидуальный номер, фактическое состояние, техническая исправность и т. д.).

Второе направление – это характеристика данных, содержащихся на компьютерном устройстве как в целом, так и в контексте соотношения с обстоятельствами совершенного преступления (имеются ли какие-либо данные, их тип, форма, содержание, дата формирования, особенности получения, обработки и т. д.).

Третье направление – это характеристика доступа компьютерного или иного устройства в сеть Интернет (имело ли место, какой IP-адрес, на какие ресурсы осуществлялся доступ, дата, место и время такого доступа, продолжительность и т. д.).

Второй вид судебных экспертиз обусловлен видовой спецификой того преступления, которое было совершено. Данный вопрос полагаем возможным рассмотреть на примере совершения преступлений с использованием информационных технологий в отношении особой категории лиц, а именно несовершеннолетних. Как показывает анализ материалов правоприменительной практики, в отношении указанных лиц могут быть совершены преступления против их половой свободы (неприкосновенности), против жизни, а также иные виды преступлений. В каждом таком случае могут быть назначены соответствующие виды судебных экспертиз. Например, по делам, связанным с совершением преступлений против половой свободы и половой неприкосновенности несовершеннолетнего, чаще всего назначается и проводится судебная экспертиза видеоизображений, видеозаписей порнографического содержания. «Экспертиза для определения порнографического характера видеоизображений или других объектов является комплексной и комиссионной, которая выполняется экспертами, имеющими специальные знания в области психологии, лингвистики, искусствоведения, культурологии. Задачи экспертизы – установление специальных признаков порнографического содержания в исследуемых объектах. Эта задача решается в рамках комплексной психолого-лингвистической, психолого-культурологической, психолого-искусствоведческой экспертиз или же отдельными указанными экспертизами. Определяющим выступает установление того факта, что обнаруженные объекты являются порнографическими» [14, с. 202].

Обратим внимание, что в качестве объектов экспертизы могут быть представлены: материалы, размещенные в компьютерных сетях, в том числе в сети Интернет; аудиозаписи, видеозаписи на любых носителях; изображения на электронных носителях; предметы, имеющие отношение к осуществлению сексуальных действий в отношении несовершеннолетних [15, с. 263–268].

Дальнейшие следственные действия (в частности, обыск, допрос, при возможности очная ставка, выемка и др.) проводятся с целью получения доказательственной информации, обнаружения, фиксации и изъятия следов совершенного преступления.

Заключение

В итоге следует констатировать, что знание криминалистической характеристики преступлений, совершенных с использованием информационных технологий, ее структуры и содержания – это важнейший элемент, без которого представить себе эффективную работу по расследованию и профилактике рассматриваемых преступлений крайне сложно. Проведенное исследование показало возможность представления криминалистической характеристики рассматриваемых преступлений в качестве интегральной системы, которая характеризуется несколькими основными признаками, а именно: технологической стороной совершения преступлений, действиями, совершаемыми преступниками, а также особенностями личности преступника.

Основной задачей при организации расследования преступлений, совершенных с использованием информационных технологий, видится обнаружение, фиксация и изъятие, прежде всего, цифровых следов. В дальнейшем при использовании криминалистически значимой информации необходимо обеспечить установление злоумышленника, а также всех обстоятельств совершенного преступного деяния.

СПИСОК ИСТОЧНИКОВ

1. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисова. Уфа : Уфимский ЮИ МВД России, 2023. 96 с.

2. Нугаева Э. Д. Тактика производства отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : научно-практическое пособие / Э. Д. Нугаева, З. И. Харисова, А. Л. Арипов. Уфа : Уфимский ЮИ МВД России, 2022. 96 с.

3. Хламов Н. Э. О некоторых проблемах расследования преступлений, совершенных с использованием компьютерных средств // Юристъ-Правоведъ. 2021. № 3 (98). С. 204–208.

4. Некипелова Е. И. Электронные следы и способы их изъятия // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: Всероссийская научно-практическая конференция. М. : Московская академия Следственного комитета Российской Федерации, 2021. С. 226–230.

5. Смушкин А. Б. Проблемы поиска электронных следов в системах распределенного хранения данных в процессе расследования // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий : Всероссийская научно-практическая конференция. М. : Московская академия Следственного комитета Российской Федерации, 2021. С. 136–141.

6. Кокорева Л. В. Электронные носители информации: некоторые проблемы теории и практики // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сборник статей Международной научно-практической конференции. М. : Академия управления МВД России, 2018. С. 120–123.

7. Перов В. А. Компьютерная криминалистика: электронный след понятие и виды // Уголовное судопроизводство: проблемы теории и практики. 2021. № 1. С. 94–96.

8. Халиуллина Э. Т. Личность компьютерного преступника в современной России // Вестник Академии Следственного комитета Российской Федерации. 2018. № 2 (16). С. 91.

9. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск : Омская академия МВД России, 2009.

10. Родивилина В. А., Родивилин И. П. К вопросу о личности преступника, совершающего преступления в сфере компьютерной информации // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования : сборник материалов межвузовской научно-практической конференции. 2017. С. 189.

11. Сидорова К. С. Направления поисковых действий следователя в информационно-телекоммуникационной сети Интернет при расследовании преступлений // Актуальные проблемы расследования преступлений : материалы Всероссийской научной конференции памяти И. Ф. Герасимова, Екатеринбург, 31 января 2020 года / Под редакцией Д. В. Бахтеева. Екатеринбург : Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2020. С. 135–143.

12. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 118.

13. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. 4-е изд., перераб. и доп. М. : Норма, ИНФРА-М, 2018.

14. Хмелева А. В. Особенности использования специальных знаний при расследовании преступлений сексуального характера, совершенных в отношении несовершеннолетних с использованием сети «интернет» // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сборник материалов. Орел : Орловский юридический институт Министерства внутренних дел Российской Федерации имени В. В. Лукьянова, 2018. С. 202.

15. Кокорева Л. В., Кузнецов В. А., Кузнецова Е. В.Обеспечение информационной безопасности несовершеннолетних в сети «Интернет»: проблемы и основные направления совершенствования // Проблемы применения уголовно-процессуального законодательства: пути их решения: материалы Международной онлайн-конференции / под ред. к.ю.н., доцента С. В. Власовой. Нижний Новгород : Нижегородская академия МВД России, 2018. С. 263–268.

REFERENCES

1. Features of the initial stage of investigation of illegal access to computer information : educational manual / E. D. Nugaeva, S. R. Nizaeva, V. R. Gainelzyanova, Z. I. Kharisova. Ufa : Ufa Law Institute of the Ministry of Internal Affairs of Russia, 2023. (In Russ.)

2. Nugaeva E. D. Tactics of individual investigative actions for crimes committed using information and telecommunication technologies: scientific and practical guide / E. D. Nugaeva, Z. I. Kharisova, A. L. Aripov. Ufa : Ufa Law Institute of the Ministry of Internal Affairs of Russia, 2022. (In Russ.)

3. Khlamov N. E. About some problems in the investigation of crimes committed with the use of computer tools // Yurist-Pravoved. 2021. No. 3 (98). P. 204–208. (In Russ.)

4. Nekipelova E. I. Electronic traces and methods of their seizure // Combating cybercrimes and crimes in the field of high technologies: All-Russian scientific and practical conference. M. : Moscow Academy of the Investigative Committee of the Russian Federation, 2021. P. 226–230. (In Russ.)

5. Smushkin A. B. Problems of searching for electronic traces in distributed data storage systems during the investigation // Combating cybercrimes and crimes in the field of high technologies : All-Russian scientific and practical conference. M. : Moscow Academy of the Investigative Committee of the Russian Federation, 2021. P. 136–141. (In Russ.)

6. Kokoreva L. V. Electronic media: some problems of theory and practice // Forensic science in the conditions of the development of the information society (59th annual forensic readings) : collection of articles of the International Scientific and Practical Conference. M. : Academy of Management of the Ministry of Internal Affairs of Russia, 2018. P. 120–123. (In Russ.)

7. Perov V. A. Computer forensics: electronic trace concept and types // Criminal proceedings: problems of theory and practice. 2021. No. 1. P. 94–96. (In Russ.)

8. Khaliullina E. T. Personality of a computer criminal in modern Russia // Bulletin of the Academy of the Investigative Committee of the Russian Federation. 2018. No. 2 (16). P. 91. (In Russ.)

9. Osipenko A. L. Network computer crime: theory and practice of struggle : monograph. Omsk : Omsk Academy of the Ministry of Internal Affairs of Russia, 2009. (In Russ.)

10. Rodivilina V. A., Rodivilin I. P. On the issue of the identity of a criminal who commits crimes in the field of computer information // Criminal Law of the Russian Federation: problems of law enforcement and

prospects for improvement : collection of materials from the interuniversity scientific and practical conference. 2017. P. 189. (In Russ.)

11. Sidorova K. S. Directions of search actions of an investigator in the information and telecommunication network “Internet” when investigating crimes // Current problems of crime investigation : materials of the All-Russian Scientific Conference in memory of I. F. Gerasimov / Edited by D/ V. Bakhteeva. Ekaterinburg : Federal State Budgetary Educational Institution of Higher Education “Ural State Law University”, 2020. P. 135–143. (In Russ.)

12. Rossinskaya E. R., Saakov T. A. Problems of collecting digital traces of crimes from social networks and instant messengers // Forensics: yesterday, today, tomorrow. 2020. No. 3 (15). P. 118. (In Russ.)

13. Rossinskaya E. R. Forensic examination in civil, arbitration, administrative and criminal proceedings : monograph. 4th ed., revised and expanded M. : Norma, INFRA-M, 2018. (In Russ.)

14. Khmeleva A. V. Features of the use of special knowledge in the investigation of crimes of a sexual nature committed against minors using the Internet // Criminal procedural and forensic problems in the fight against crime: collection of materials. Orel : Orel Law Institute of the Ministry of Internal Affairs of the Russian Federation named after V. V. Lukyanov, 2018. P. 202. (In Russ.)

15. Kokoreva L. V., Kuznetsov V. A., Kuznetsova E. V. Ensuring information security of minors on the Internet: problems and main directions for improvement // Problems of application of criminal procedural legislation: ways to solve them: materials of the International online-conference / ed. Candidate of Law, Associate Professor S. V. Vlasova. Nizhny Novgorod: Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2018. P. 263–268. (In Russ.)

Информация об авторе:
Кокорев Р. А. – кандидат юридических наук.

Information about the author:
Kokorev R. A. – Candidate of Law.

Статья поступила в редакцию 21.01.2024; одобрена после рецензирования 07.02.2024; принята к публикации 21.03.2024.

The article was submitted 21.01.2024; approved after reviewing 07.02.2024; accepted for publication 21.03.2024.