Научная статья
УДК 343.326:343.98
https://doi.org/10.24412/2073-0454-2025-3-160-165
EDN: https://elibrary.ru/giiupa
NIION: 2003-0059-3/25-315
MOSURED: 77/27-003-2025-03-514

Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: актуальные вопросы правового обеспечения

Инна Валериевна Тишутина
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия, inna_tishutina@mail.ru

Аннотация. Характеризуются актуальные проблемы правового обеспечения раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Обращается внимание на изменение традиционной структуры криминалистически значимой информации за счет появления цифровой информации и постоянного увеличения ее доли в общем объеме информации, значимой для целей расследования. Предлагается ее классификация и отмечается приоритетность отдельных групп для формирования системного подхода к ее собиранию, обработке и накоплению. Подчеркивается особое значение правового обеспечения для расширения перечня методов и средств выявления, раскрытия и расследования таких преступлений. Аргументируется важность унификации информационных систем и баз данных, содержащих сведения, характеризующие элементы состава преступления, а также целесообразность расширения перечня и характеристик учитываемой информации. Рассматриваются основные положения действующего законодательства, регулирующие создание и функционирование таких систем, а также перспективы повышения эффективности получения и использования цифровой криминалистически значимой информации в свете законодательных новелл.

Ключевые слова: цифровая криминалистически значимая информация, преступление, цифровая среда, расследование, информационно-телекоммуникационные технологии, правовое обеспечение, накопление, использование

Для цитирования: Тишутина И. В. Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: актуальные вопросы правового обеспечения // Вестник Московского университета МВД России. 2025. № 3. С. 160–165. https://doi.org/10.24412/2073-0454-2025-3-160-165. EDN: GIIUPA.

Original article

Investigation of crimes committed with the use of information and telecommunication technologies: current issues of legal support

Inna V. Tishutina
Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia, inna_tishutina@mail.ru

Abstract. Current problems of legal support of disclosure and investigation of crimes committed with the use of information and telecommunication technologies are characterized. Attention is drawn to the change in the traditional structure of criminally significant information due to the emergence of digital information and the constant increase in its share in the total volume of information significant for the purposes of investigation. Its classification is proposed and the priority of certain groups for the formation of a systematic approach to its collection, processing and accumulation is noted. The special importance of legal support for expanding the list of methods and means of detection, disclosure and investigation of such crimes is emphasized. The importance of unification of information systems and databases containing information characterizing the elements of a crime is argued, as well as the expediency of expanding the list and characteristics of the information taken into account. The main provisions of the current legislation regulating the creation and functioning of such systems are considered, as well as the prospects for increasing the efficiency of obtaining and using digital forensically significant information in the light of legislative novelties.

Keywords: digital forensically significant information, crime, digital environment, investigation, information and telecommunication technologies, legal support, accumulation, use

For citation: Tishutina I. V. Investigation of crimes committed with the use of information and telecommunication technologies: current issues of legal support. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025;(3):160–165. (In Russ.). https://doi.org/10.24412/2073-0454-2025-3-160-165. EDN: GIIUPA.

На протяжении первой четверти текущего века ежегодно расширяется число сфер жизни и деятельности граждан и областей функционирования государственных институтов, охватываемых цифровизацией. С одной стороны, это предоставляет новые возможности, повышает скорость и качество оказывае-

мых услуг, а с другой, — увеличивает вероятность стать объектом преступлений, подготавливаемых и совершаемых с использованием информационно-телекоммуникационных технологий. Не случайно расширяется и перечень статей уголовного закона, в которых в качестве квалифицирующего признака фигурирует «использование средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет. Только за последние пять лет в два с половиной раза увеличилось количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий (с 294,4 тыс. в 2019 г. до 765,4 тыс. в 2024 г.), а их доля в общем массиве выросла с 15 до 40 % и продолжает расти. Практически половина таких преступлений (48 %) относится к категории тяжких и особо тяжких. [1; 2]. Не осталось ни одной сферы преступной деятельности, в которой не использовались бы возможности информационно-телекоммуникационных технологий. Особую обеспокоенность здесь вызывает преступная деятельность в отношении несовершеннолетних, в рамках которой использование технологий ориентировано на: сбор сведений о них и составление баз данных по определенным критериям на основе изучения информации открытого доступа в сети Интернет; вовлечение в преступную деятельность и т. п. [3, с. 27–28].

Видоизменение форм и способов «традиционных» преступных деяний, появление новых направлений преступной деятельности закономерно влияет на модификацию криминалистически значимой информации о таких деяниях и ее источниках. С каждым годом все большую долю в общей массе значимой для расследования информации занимают данные, сосредоточенные в цифровом пространстве и выраженные в цифровой форме. Это может быть информация, образующаяся при совершении как правомерных, так и преступных действий — цифровой след, а также сведения, накапливаемые в информационных базах. В частности, это данные различных государственных органов, учреждений и организаций, а также результаты использования гражданами возможностей цифровой коммуникации.

Результаты изучения практики позволяют дифференцировать цифровую информацию на группы по ряду оснований:

♦ форме накопления: систематизированная информация, сосредоточенная в различных информационных системах и базах данных, и несистематизированная информация, расположенная в информационном пространстве сети Интернет;

♦ форме передачи ее содержания: аудио, видео, фото, текст, рисунок, реакция-эмоджи;

♦ способу доступа: частного (закрытого), общего (открытого);

♦ содержанию в криминалистическом аспекте: о личности преступника, потерпевшего, о способе преступления, орудиях и средствах, обстановке, механизме следообразования.

Предлагаемая классификация способствует формированию системного и целенаправленного подхода к обработке и накоплению цифровой информации, в том числе той, которая может представлять интерес для правоохранительных органов в рамках расследования преступной деятельности. Такой подход обеспечивает надлежащую организацию информационного обеспечения предварительного расследования и в перспективе может существенно повысить эффективность выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Результаты изучения практики приводят к закономерному выводу о важности трансформации системы криминалистического обеспечения раскрытия и расследования как новых видов и групп преступлений, так и традиционных преступлений, совершаемых с использованием новейших технологий. Данная потребность обусловлена необходимостью эффективного использования новых возможностей по сбору, накоплению и анализу криминалистически значимой информации в условиях цифровой трансформации преступной деятельности. Именно надлежащий уровень криминалистического обеспечения, охватывая все принципиально важные стороны расследования, позволяет обеспечивать повышение его эффективности и соответствие потребностям правоохранительных органов в реалиях времени.

В последнее время вполне обоснованно внимание ученых привлекают вопросы криминалистического обеспечения получения и использования в расследовании преступлений цифровой информации открытого доступа. К источникам таковой, в частности, относятся: сайты, телеграмм-каналы, группы в мессенджерах, аккаунты в социальных сетях, цифровые платформы агрегаторов каршеринга и кикшеринга и т. п. В международной прак-

тике эти действия получили наименование OSINT-разведки [4; 5].

Одним из важнейших элементов криминалистического обеспечения выступает правовое обеспечение, особое значение которого обусловливается тем, что без надлежащего нормативного закрепления невозможно применение в практике раскрытия и расследования преступлений никаких современных методов и средств. В настоящее время содержание правового обеспечения в системе криминалистического сопровождения раскрытия и расследования преступлений рассматривается не только сквозь призму нормативного регулирования использования научно-технических средств и методов, но и в значительно более широком контексте. Такой подход представляется вполне обоснованным: с одной стороны, он отражает комплексный и междисциплинарный характер самой категории криминалистического обеспечения, с другой, — является следствием тенденции к укрупнению научных знаний.

Очевидно, что в сложившихся условиях повышенной востребованности для целей раскрытия и расследования преступлений цифровой криминалистически значимой информации принципиально важное значение приобретает правовая регламентация методов и средств ее получения и использования. Представляется, что для характеристики основных проблемных аспектов правового обеспечения вовлечения цифровой информации в процесс доказывания, первостепенное значение будет иметь место сосредоточения информации и ее содержание. В криминалистическом аспекте, целесообразно, на наш взгляд, вести речь о двух основных группах: информация о личности и информация о способах и средствах действий.

Бесспорно, что использование для целей расследования преступлений информации, сосредоточенной в различных базах данных и информационных системах, связано с дополнительными временными и организационными затратами. В случае унификации таких систем и объединения их информационных массивов в рамках единой универсальной системы, существенным образом упрощается обращение информации. При этом объем накапливаемой информации предопределяет эффективность системы. Аккумулирование информации, связанной исключительно с фактами ранее совершенных преступлений, искусственно ограничивает возможности таких систем. Представляется целесообразным, чтобы принцип всеобщего учета лег в основу формирования соответствующих баз данных и автоматизированных систем поиска информации. В контексте современных вызовов, связанных с необходимостью обеспечения безопасности и эффективности расследования преступлений, очевидно, что сегодня, в условиях тотального охвата цифровыми технологиями разрозненных систем хранения информации о гражданах, доступ к ней лиц, осуществляющих преступную деятельность, порой гораздо легче и проще, чем у сотрудников правоохранительных органов, остро в этом нуждающихся.

В целях создания единой универсальной системы, объединяющей базы данных, накапливающей информацию о личности физических лиц, в 2020 г. был принят Федеральный закон № 168-ФЗ, регламентирующий формирование единого федерального информационного регистра, содержащего сведения о населении Российской Федерации. В соответствии с его положениями с 31 декабря 2025 г. в России должна полноценно функционировать единая база данных о физических лицах: гражданах Российской Федерации, иностранных гражданах и лицах без гражданства, а также иностранных гражданах, временно прибывающих для осуществления трудовой деятельности. В регистре накапливаются две группы сведений, включающих информацию различных государственных органов и учреждений: Министерства внутренних дел, Министерства обороны, Федеральной налоговой службы, Пенсионного фонда, Фонда обязательного медицинского страхования и других через систему межведомственного электронного взаимодействия [8].

Однако, до последнего времени существующие базы данных, информационные системы накапливали сведения об идентификаторах персональных данных пользователя, а не об устройстве и действиях, связанных с его использованием. В то же время, давно очевидно, что высока вероятность идентификации любого устройства по определенному набору признаков [6]. В этом контексте важным этапом стало налаживание и внедрение в практическую деятельность правоохранительных органов подсистемы «Дистанционное мошенничество», обеспечивающей накопление и систематизацию информации по широкому перечню параметров, что, в свою очередь, способствует формированию практически значимого

массива сведений о средствах совершения преступления и механизме следообразования [7, с. 25].

При этом совершенно очевидно, что ограниченность объема сведений в рамках такой системы снижает ее эффективность на фоне того, что лица, совершающие преступление с использованием современных информационно-телекоммуникационных технологий, применяют средства сокрытия идентификационной информации, поддельные аккаунты, симкарты, зарегистрированные на подставных лиц, а также серверы и ресурсы, находящиеся вне юрисдикции Российской Федерации. Указанные обстоятельства объективно затрудняют процесс идентификации лиц, причастных к совершению преступления в цифровой среде, и существенно снижают эффективность оперативно-розыскной и уголовно-процессуальной деятельности. Все это затрудняет не только расследование, но и последующее судебное разбирательство.

На совершенствование правового обеспечения расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, направлено принятие федерального закона от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [9]. В нем констатируется ее создание, однако остается не определенным механизм формирования и отдельные вопросы ее функционирования. Поэтапность введения в действие положений данного закона (с 1 июня 2025 г. по 1 марта 2027 г.) должна обеспечить возможность проработки соответствующего механизма. К компетенции Правительства Российской Федерации отнесено создание Положения о данной системе, а также определение перечня обрабатываемой информации и лиц, ее предоставляющих; порядка включения, исключения информации и предоставления доступа к ней. Предполагается, что система межведомственного электронного взаимодействия будет обеспечивать доступ к информации, предоставляемой: кредитными организациями, владельцами агрегаторов, операторами связи, провайдерами хостинга.

Принятие данного закона, безусловно, важный шаг на пути объединения в общий массив данных информации, рассредоточенной по различным базам и системам разных организаций и учреждений, и упрощения доступа к ним и скорости их получения правоохранительными органами. В то же время, ознакомление с текстом закона показывает, что, прежде всего, в рамках данной системы будет накапливаться информация о лицах, совершивших противоправные действия с использованием сети связи общего пользования, и абонентских номерах, используемых в целях совершения противоправных действий. На наш взгляд, такой подход будет ограничивать возможности системы. Кроме того, нуждаются в серьезной проработке и регламентации вопросы надлежащей защиты данных, обеспечения конфиденциальности сведений, накапливаемых в системе, доступ к которым предоставляется. Не отражены и права граждан в отношении своих данных. Не представлена четкая дорожная карта внедрения системы, что может привести к несогласованности действий участников и затруднить реализацию положений закона.

На расширение перечня сведений, накапливаемых обо всех пользователях определенного вида услуг, могут быть направлены ведомственные акты. Так, в настоящее время на операторов связи возложена обязанность по передаче в Роскомнадзор сведений, включающих информацию о:

- сетевых адресах, используемых средствами связи и пользовательским оборудованием;
- местах использования соответствующих сетевых адресов;
- уникальных идентификаторах технических средств, предназначенных для противодействия угрозам функционированию сети Интернет и сети связи общего пользования на территории Российской Федерации [10].

В условиях стремительной цифровизации общественных отношений и роста преступности, совершаемой с использованием средств связи и информационно-коммуникационных технологий, особую значимость приобретает нормативное обеспечение процедур учета и контроля за техническими средствами, используемыми операторами связи. Предполагается, что соблюдение установленных требований в сфере регистрации и идентификации телекоммуникационного оборудования позволит создать централизованную базу данных, содержащую исчерпывающую информацию о параметрах средств связи, находящихся в эксплуатации на территории РФ.

Реализация указанных мер направлена, прежде всего, на обеспечение возможности оперативной

идентификации коммуникационного оборудования, что имеет ключевое значение для своевременного и эффективного расследования преступлений, совершаемых с использованием технических средств скрытой передачи данных, а также для выявления каналов несанкционированной коммуникации.

Создание и функционирование такой базы данных позволит органам предварительного расследования и оперативным подразделениям получать достоверную информацию о характеристиках и параметрах использования конкретных средств связи, что существенно расширяет возможности криминалистического анализа. В частности, речь идет об установлении владельцев устройств, трассировании трафика, выявлении связей между субъектами противоправной деятельности и восстановлении цепочек коммуникации в рамках расследуемых уголовных дел. Соответственно, внедрение системы централизованного учета телекоммуникационного оборудования следует рассматривать не только как элемент технической регламентации деятельности операторов связи, но и как важное средство повышения эффективности правоприменительной практики в сфере расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Таким образом, на фоне экспоненциального роста преступлений, совершаемых с использованием средств связи и информационно-телекоммуникационных технологий, с которым столкнулась сегодня правоохранительная практика, серьезной проблемой стало отставание законодательства от темпов технологического развития. При выявлении и расследовании преступлений большую роль играют вопросы правового обеспечения использования возможностей современных технологий правоохранительными органами и особенно — получения и использования цифровой криминалистически значимой информации. Несмотря на предпринимаемые меры, правовое обеспечение получения и использования для целей расследования цифровой криминалистически значимой информации в этой области сталкивается с рядом серьезных трудностей, от скорости решения которых зависит эффективность борьбы с преступностью.

Список источников

1. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 г. // URL: https://мвд.рф/reports/item/19412450/

2. Состояние преступности в России за январь–декабрь 2024 г. // URL: https://portal.tpu.ru//Sbornik_UOS_2024.pdf

3. Головин А. Ю., Акиев А. Р., Головина Е. В. Дистанционное вовлечение несовершеннолетних в преступную деятельность как объект криминалистического исследования // Правовое государство: теория и практика. 2024. № 2(76). С. 24–30.

4. Болвачев М. А. Использование социальных сетей при расследовании преступлений экстремистской направленности: дисс. … канд. юрид. наук. Калининград, 2022.

5. Головин А. Ю., Головина Е. В. К вопросу собирания криминалистически значимой информации по открытым цифровым данным // Актуальные проблемы криминалистики и судебной экспертизы: сб. мат. междунар. науч.-практ. конф. Иркутск, 2023. С. 29–32.

6. Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений // URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii

7. Давыдов В. О., Тишутина И. В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Серия: Юридические науки. 2020. Вып. 3. С. 20–27.

8. Федеральный закон от 8 июня 2020 г. № 168-ФЗ (ред. от 28 декабря 2024 г.) «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» // URL: https://www.consultant.ru/document/cons_doc_LAW_354474/6e484612bd84209dff27d63c34699eae510c7ad7/

9. Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // URL: https://www.garant.ru/hotlaw/federal/1805918/#review

10. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 февраля 2025 г. № 51 «Об утверждении порядка, сроков, состава и формата предоставления оператором связи в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой ин-

формации, массовых коммуникаций, информационных технологий и связи, информации, позволяющей идентифицировать средства связи и пользовательское оборудование (оконечное оборудование) в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации, территории субъекта Российской Федерации или части территории субъекта Российской Федерации в электронной форме» // URL: https://www.garant.ru/products/ipo/prime/doc/411683761/

References

1. Brief description of the state of crime in the Russian Federation in January–December 2019 // URL: https://mia.rf/reports/item/19412450/

2. The state of crime in Russia in January–December 2024 // URL: https://portal.tpu.ru//Sbornik_UOS_2024.pdf

3. Golovin A. Yu., Akiev A. R., Golovina E. V. Remote involvement of minors in criminal activity as an object of forensic research // The rule of law: theory and practice. 2024. № 2(76). P. 24–30.

4. Bolvachev M. A. The use of social networks in the investigation of extremist crimes: diss. ... candidate of legal sciences. Kaliningrad, 2022.

5. Golovin A. Yu., Golovina E. V. On the issue of collecting criminalistically significant information on open digital data // Actual problems of criminalistics and forensic examination: collection of mathematical international scientific and practical conference. Irkutsk, 2023. P. 29–32.

6. Sidorenko E. In digital footsteps: only a quarter of cybercrimes are disclosed in the Russian Federation // URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii

7. Davydov V. O., Tishutina I. V. Digital traces in the investigation of remote fraud // Proceedings of Tula State University. Series: Legal Sciences. 2020. Issue 3. P. 20–27.

8. Federal Law № 168-FZ of June 8, 2020 (as amended on December 28, 2024) «On the Unified Federal Information Register containing Information about the Population of the Russian Federation» // URL: https://www.consultant.ru/document/cons_doc_LAW_354474/6e484612bd84209dff27d63c34699eae510c7ad7/

9. Federal Law № 41-FZ of April 1, 2025 «On the Creation of a State information system for Countering Offenses Committed using Information and Communication Technologies and on Amendments to Certain Legislative Acts of the Russian Federation» // URL: https://www.garant.ru/hotlaw/federal/1805918/#review

10. Order of the Federal Service for Supervision of Communications, Information Technology and Mass Communications dated February 28, 2025 № 51 «On Approval of the Procedure, Terms, Composition and Format for the provision by a telecom operator to the federal executive Governmental body responsible for Control and Supervision in the Field of mass media, mass Communications, Information technology and Communications, Information allowing identification of communication facilities and user equipment (terminal equipment) in the information and telecommunications network Internet on the territory of the Russian Federation, the territory of the subject of the Russian Federation or part of the territory of the subject of the Russian Federation in electronic form» // URL: https://www.garant.ru/products/ipo/prime/doc/411683761/

Информация об авторе

И. В. Тишутина — профессор кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, профессор.

Information about the author

I. V. Tishutina — Professor of the Department of Criminalistics of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Doctor of Legal Sciences, Professor.

Статья поступила в редакцию 02.03.2025; одобрена после рецензирования 31.03.2025; принята к публикации 25.04.2025.

The article was submitted 02.03.2025; approved after reviewing 31.03.2025; accepted for publication 25.04.2025.