Научная статья
УДК 343.132.5; 343.985.3
EDN JWDPKQ
DOI 10.17150/2500-4255.2025.19(2).210-220

СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ, СВЯЗАННЫЕ С МОНИТОРИНГОМ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ С ПОМОЩЬЮ СРЕДСТВ ТЕЛЕКОММУНИКАЦИОННОЙ СВЯЗИ: НЕКОТОРЫЕ ПРОБЛЕМЫ РЕГЛАМЕНТАЦИИ И ПРАВОПРИМЕНЕНИЯ В СВЕТЕ СОВРЕМЕННЫХ ПОТРЕБНОСТЕЙ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

А.В. Варданян
Ростовский юридический институт Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Российская Федерация

Информация о статье

Дата поступления
19 марта 2025 г.

Дата принятия в печать
9 июня 2025 г.

Дата онлайн-размещения
17 июня 2025 г.

Ключевые слова

Следственные действия; информация; средства связи; телекоммуникационные контакты; фонограмма; осмотр; контроль телефонных и иных переговоров; получение информации о соединениях между абонентами и/или абонентскими устройствами; оперативно-розыскные мероприятия; результаты оперативно-розыскной деятельности

Аннотация. Происходящие в социуме тенденции, олицетворяющие стремительное развитие и повсеместное внедрение телекоммуникационных технологий, не могли не отразиться на трансформации преступности, предопределив возникновение новых видов или способов противоправных посягательств, совершаемых в виртуальной среде. Кроме того, средства дистанционной связи активно используются злоумышленниками для обсуждения приемов по приготовлению к успешной реализации криминального умысла, прогнозирования типичных реакций потерпевших, согласования мер по сокрытию следов.

Обозначенные обстоятельства обусловливают наличие высокого доказательственного потенциала применительно к информации, передаваемой в рамках телекоммуникационных контактов, что стимулирует исследовательский интерес к процессуальной форме поступления в уголовное судопроизводство данных сведений.

В зависимости от выбора вариантов юридически значимой активности указанные материалы поступают в основном: в результате следственных действий, непосредственно предназначенных для «перехвата» данных о состоявшемся взаимодействии с помощью средств связи (контроль и запись переговоров; получение информации о соединениях между абонентами или абонентскими устройствами); вследствие технологически сходных оперативно-розыскных мероприятий (прослушивание телефонных переговоров, снятие информации с технических каналов связи, проверка компьютерной информации); по итогам обыска, выемки, прочих следственных действий, способствующих изъятию фонограммы и иных материалов; посредством проведения следственных действий, отображающих обнаружение, фиксацию, обследование факта и проявлений коммуникации лиц в мессенджерах, каналах, на сайтах и пр.

Анализируя обозначенные выше источники формирования доказательственной информации с точки зрения их регламентации в УПК РФ, автор обращает внимание на наличие целого комплекса неоднозначных моментов, среди которых: непоследовательность и несогласованность в наименованиях следственных действий; нелогичность в определении субъектного состава их участников; наличие пробелов относительно совокупности существенных обстоятельств; спорность отнесения к категории следственных действий этапов по непосредственной фиксации информации, осуществляющейся в автоматическом режиме иными уполномоченными лицами и др.

Автор предлагает рекомендации, направленные, во-первых, на нейтрализацию выявленных проблем, пробелов, противоречий, во-вторых, на унификацию норм, регулирующих работу с источниками доказательственной информации, полученной в результате мониторинга телекоммуникационных контактов, — с учетом современных запросов и потребностей борьбы с преступностью.

ISSN 2500-1442

Original article

INVESTIGATIVE ACTIONS RELATED TO THE MONITORING OF INFORMATION TRANSMITTED BY MEANS OF TELECOMMUNICATION: SOME PROBLEMS OF REGULATION AND LAW ENFORCEMENT IN THE LIGHT OF MODERN CRIME CONTROL NEEDS

Akop V. Vardanyan
Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation, Rostov-on-Don, the Russian Federation

Article info

Received
2025 March 19

Accepted
2025 June 9

Available online
2025 June 17

Keywords

Investigative actions; information; means of communication; telecommunication contacts; phonogram; inspection; control of telephone and other negotiations; obtaining information about connections between subscribers and (or) subscriber devices; operational search activities; results of operational search activities

Abstract. The social trends of rapid development and widespread introduction of telecommunication technologies could not but influence the transformation of crimes, predetermining the emergence of new types or means of unlawful infringements in the virtual environment. Besides, the means of distance communication are actively used by perpetrators for discussing the preparations for the successful implementation of their criminal intents, predicting the typical reactions of the victims, coordinating measures to conceal the traces of their crimes.

All of this testifies to a high evidentiary potential of information transmitted through the telecommunication contacts, which stimulates the research interest in the procedural form of introducing this information in the criminal proceedings.

Depending on the choice of legally significant activity, these materials are mainly introduced in the following ways: as a result of investigatory actions specifically aimed at "intercepting" the data on some interaction that took place through means of communication (control and recording of negotiations; obtaining information about connections between subscribers or their devices); as a result of technologically similar operative search activities (telephone tapping, obtaining information from technical communication channels, verification of computer information); as a result of searches, confiscation, other investigatory actions contributing to the confiscation of audio recordings and other materials; as a result of investigatory actions reflecting the identification, recording and researching the facts and manifestations of communication using messengers, channels, sites, etc.

While analyzing the abovementioned sources of obtaining evidentiary information from the standpoint of their regulation in the Criminal Procedure Code of the Russian Federation, the author pays attention to a whole complex of controversial moments, including: a lack of consistency and coordination in naming investigatory actions; illogical definition of the subjective composition of their participants; gaps in the aggregate of significant circumstances; disputable categorization of stages of actual recording of information carried out automatically by specially authorized persons as investigative actions, etc.

The author presents recommendations aimed at, firstly, neutralizing the identified problems, gaps, contradictions and, secondly, at unifying norms that regulate work with sources of evidentiary information obtained as a result of monitoring telecommunication contacts, while taking into account modern requirements and needs of crime counteraction.

Интеграция современных высококачественных средств компьютерной техники, а также телекоммуникационных технологий во все сферы жизни общества, дальнейшая стремительная цифровизация и информатизация социума как необратимая и универсальная тенденция [1, с. 90–92] не могли не повлиять на трансформацию преступности [2, с. 108–110; 3, с. 7–12; 4, с. 500–515; 5; 6, с. 39–48]. Хорошо известно, что на смену так называемым традиционным формам и способам хищений чужого имущества, проявляющимся в непосредственном и буквальном противоправном его изъятии злоумышленниками у законного владельца, все чаще актуализируются их дистанционные разновидности, совершаемые с помощью средств связи, нередко с учетом применения знаний в области социальной инженерии [7, с. 3–13; 8, с. 175–188], и, несмотря на отсутствие прямого личного контакта с пострадавшими, влекущие причинение крупного или особо крупного ущерба [9, с. 18; 10; 11, с. 495–499].

В этой связи весьма показательны статистические данные МВД России, опубликованные на официальном сайте ведомства, согласно которым 2024 год ознаменовался, с одной стороны, снижением количества зарегистрированных разбоев (на 16,3 %), грабежей (на 20,7 %), краж

ISSN 2500-1442

(на 14,3 %, в особенности краж квартирных — на 28,7 % и краж автомобильных — на 19,5 %), с другой стороны, ростом числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий (на 13,1 %, из них тяжких и особо тяжких — на 7,8 %), причем достигших 40 % от общей массы преступных посягательств[1].

Применение информационно-телекоммуникационных технологий как орудий и средств совершения преступлений не ограничивается хищениями (традиционно признаваемыми наиболее распространенными деяниями) [12, с. 61–67]. Дистанционные формы приобрели не меньшую популярность при незаконном обороте наркотических средств, психотропных веществ [13, с. 45–53], иных запрещенных или ограниченных в гражданском обороте объектов, при посягательствах экстремистской и террористической направленности [14, с. 90–96; 15, с. 26–31] и даже при сексуальных домогательствах [16, с. 871–892; 17, с. 1614–1629; 18, с. 215–218] и пр.

Не претендуя на перечисление всех видов деяний, характеризующихся применением средств связи, констатируем как общую данность, присущую нынешним реалиям взаимодействия между людьми и проявляющуюся в том, что сами по себе «живые» встречи (независимо от наличия или отсутствия криминальной подоплеки) зачастую по различным причинам вытесняются общением в удаленном формате. В полной мере это относится и к субъектам преступлений, использующим современные технологии не только в качестве орудий и средств совершения посягательств, но также в процессе приготовления к реализации противоправного умысла, а равно осуществления действий по сокрытию следов.

Как показывают материалы уголовных дел, для субъектов характерно обсуждение тех или иных обстоятельств, деталей, особенностей предстоящего (или совершенного) деяния, вариантов действий каждого злоумышленника, прогнозирование реакций потенциальных жертв, а также согласование мер по обеспечению неуязвимости от уголовного преследования и пр. Несмотря на то, что указанными «собеседниками» во многих случаях применяются известные приемы конспиративного характера (прежде всего в виде условных наименований, обозначений предметов посягательства, средств и орудий совершения или сокрытия преступления, кличек или «псевдонимов» соучастников, потенциальных жертв, иных значимых лиц), правоприменительная практика свидетельствует, что именно результаты негласного получения сведений о содержании их переговоров (по сути, специфической разновидности цифровых следов [19]) являются одним из наиболее ценных и перспективных источников доказательственной информации.

Учет указанных кардинально изменившихся условий, влияющих на формирование механизма целого ряда преступлений, продуцирует потребность в обновленном подходе со стороны не только правоприменителей, но и прежде всего ученых в сфере уголовно-правовых наук. Помимо разработки криминалистических рекомендаций [20, с. 58–61], призванных повысить результативность борьбы с преступностью применительно к существующим реалиям, полагаем, что не меньшее значение приобретает исследование процессуальной формы поступления в уголовное судопроизводство доказательств, отражающих содержание информации, воспроизведенной в ходе удаленного взаимодействия между лицами, осведомленными относительно значимых для расследования обстоятельств.

Как следует из системного толкования норм УПК РФ, а также анализа правоприменительной практики, фонограммы и иные материалы, отражающие факт значимых для доказывания телекоммуникационных контактов, могут поступать в уголовное дело:

1) посредством производства следственных действий, специально регламентирующих основания и порядок деятельности в отношении указанных объектов: контроль и запись переговоров (ст. 186 УПК РФ); получение информации о соединениях между абонентами и/или абонентскими устройствами (ст. 186.1 УПК РФ);

2) будучи результатами оперативно-розыскной деятельности, представленными оперативными подразделениями следователю в соответствии со ст. 89 УПК РФ, а также ст. 11 Федерального закона от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (полученными путем: прослушивания телефонных переговоров; снятия информации с технических каналов связи; проверки компьютерной информации);

1 Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // Министерство внутренних дел Российской Федерации : офиц. сайт : статистика и аналитика. URL: https://мвд.рф/reports/item/60248328 (дата обращения: 15.02.2025).

3) вследствие производства следственных и иных процессуальных действий, отражающих изъятие фонограмм (в том числе вместе с носителями), а также иных материалов у лиц, проходящих по уголовным делам, путем обыска или выемки, включая добровольное и инициативное предоставление участниками уголовного судопроизводства соответствующих объектов;

4) благодаря проведению следственных действий, отображающих обнаружение, фиксацию, обследование различных проявлений коммуникации и социальной активности субъектов в мессенджерах, каналах, сайтах и пр.

Примечательно, что регламентируемое в ст. 186 УПК РФ следственное действие обозначается как «контроль и запись переговоров», тогда как в представленном в п. 14.1 ст. 5 УПК РФ определении данного понятия оно именуется как «контроль телефонных и иных переговоров». Разумеется, подобная неточность не способствует единообразию правоприменения. Определение понятия следственного действия, введенное в УПК РФ на один год позже (04.07.2003 г.) вступления в силу первоначальной редакции уголовно-процессуального закона, должно способствовать оптимизации регламентации, толкования и непосредственного производства соответствующего следственного действия, а не усиливать терминологическую путаницу.

Как следует из содержания дефиниции термина, представленного п. 14.1 ст. 5 УПК РФ, под контролем телефонных и иных переговоров следует понимать: а) прослушивание и запись переговоров путем использования любых средств коммуникации; б) осмотр и прослушивание фонограмм. Полагаем, что, действительно, самим по себе понятием «контроль» справедливо охватываются не только действия по «перехвату» контактов и ознакомлению с содержанием результатов взаимодействия, состоявшегося с помощью средств связи, но и по их процессуальной фиксации.

Другое дело, что вышеприведенная формулировка анализируемого определения оставляет вероятным предположить отнесенность фразы «путем использования любых средств коммуникации» применительно к прослушиванию и записи переговоров, а не к ведению этих переговоров самими интересующими следствие собеседниками. А ведь это не всегда само собой разумеющееся соотношение понятий. Общение может осуществляться как с использованием средств связи, так и без такового (при непосредственном контакте), что не исключает негласного применения специальных средств аудио- или видеозаписи. Полагаем, что в формате задуманного разработчиками УПК РФ следственного действия «контроль телефонных и иных переговоров» (а не технологически сходных оперативно-розыскных мероприятий) подразумевается мониторинг именно информации, транслируемой с помощью средств связи, что целесообразно было бы уточнить в п. 14.1 ст. 5 УПК РФ следующим образом: «прослушивание и запись переговоров, осуществляющихся путем использования любых средств коммуникации».

Однако формулировка определения понятия «получение информации о соединениях между абонентами и/или абонентскими устройствами», изложенная в п. 24.1 ст. 5 УПК РФ, предваряющая уточнение оснований и порядка производства одноименного следственного действия, регламентированного в ст. 186.1 УПК РФ, будучи тождественной по наименованию (в отличие от рассмотренного выше следственного действия), отражает лишь первый из основных этапов его проведения. Законодатель предлагает понимать под его сущностью получение: сведений о дате, времени, продолжительности соединений между абонентами и/или абонентскими устройствами, номерах абонентов, прочих данных, позволяющих идентифицировать абонентов; сведений о номерах и месте расположения приемопередающих станций.

Иными словами, в приведенном определении отражается фактическая сущность и техническая сторона следственного действия, но не упоминается его последующий этап, в рамках которого осуществляется изучение добытого материала самим следователем. Но именно процессуальная форма дальнейшего этапа в большей степени соответствует стандартам следственного действия — в данном случае осмотра, что свидетельствует о некоторой непоследовательности в регламентации следственных действий, обладающих технологически и тактически сходной природой.

Закономерно, что фонограмма и иные материалы, отражающие факт телекоммуникационных контактов между лицами, обладающими информацией, значимой для расследования, которые изначально были получены в результате оперативно-розыскных мероприятий, а равно поступили в уголовное дело иным процессуально допустимым путем (например, изъяты по итогам проведения обыска или выемки, в том

числе добровольно выданы их обладателями в ходе следственных действий), обследуются в формате осмотра предметов и документов, предусмотренного ст. 176 УПК РФ. Затем (при наличии оснований) принимается решение о приобщении материалов к делу.

Таким образом представляется, что, несмотря на отличительные нюансы в конструировании обозначенных выше процессуальных форм, регулирующих источник происхождения доказательственной информации, отражающей факты телекоммуникационных контактов, при работе с ней можно выделить следующие общие черты.

1. Процесс формирования доказательственной информации можно условно дифференцировать на два основных (рабочих) этапа: 1) обнаружение и техническая фиксация информации, характеризующей телекоммуникационный контакт и его основные характеристики (первоначальный этап); 2) обследование данной информации и ее отображение (процессуальная фиксация) в протоколе следственного действия, в сочетании с применением по необходимости дополнительных средств фиксации: видеозаписи, фотографирования, составления схем и пр. (последующий этап).

2. Первоначальный этап, в виде обнаружении и фиксации информации, отражающей обстоятельства и содержание контакта (кроме варианта 4), как правило, осуществляется без участия следователя (следователь может лишь назначить производство обозначенных следственных действий либо поручить выполнение оперативно-розыскных мероприятий, но не может лично и непосредственно контролировать выполнение их сугубо технических аспектов; более того, согласно нормативным положениям оперативно-розыскного законодательства, в ряде случаев оперативно-розыскные мероприятия могут проводиться уполномоченными субъектами инициативно, даже несмотря на отсутствие специального поручения следователя).

3. Последующий этап в виде непосредственного обследования данной информации (путем восприятия с помощью органов чувств, а также воспроизведения с использованием технических средств), с дальнейшим отображением в протоколе следственного действия, осуществляется следователем, в ряде случаев — при участии иных лиц: специалиста, лиц, чьи телекоммуникационные контакты зафиксированы, понятых (если следователь сочтет необходимым их пригласить).

Несмотря на то что с точки зрения процессуальной регламентации в УПК РФ в одних случаях обозначенный нами последующий этап выступает одной из стадий производства следственных действий (ст. 186, 186.1 УПК РФ), а в других случаях (при работе с материалами, представленными в уголовный процесс по итогам оперативно-розыскной деятельности, либо полученными в результате предшествовавших следственных действий: выемки, обыска и пр.) представляет собой самостоятельные следственные действия, полагаем, что именно указанный этап деятельности следователя в полной мере отвечает требованиям (руководящим положениям, условиям), соответствующим конструкции следственного действия.

Негласный, а также сугубо технический характер «перехвата» и фиксации телекоммуникационных контактов, исключающий разглашение данных о способах, средствах и непосредственных участниках (соответственно, в данной части делающий невозможной, по общему правилу, проверку доказательств), безусловно, свидетельствует об их общности с оперативно-розыскными мероприятиями. Что касается получения информации о соединениях между абонентами и/или абонентскими устройствами (в части этапа непосредственного технического мониторинга телекоммуникационных контактов), то в данном случае указанные действия носят сугубо автоматизированный характер, фактически напоминая выполнение различных запросов следователя. Как известно, в соответствии с ч. 4 ст. 21 УПК РФ следователь вправе в пределах своих полномочий направлять в различные учреждения, предприятия, организации обязательные для исполнения требования, поручения, запросы.

Таким образом, мы разделяем позицию исследователей, считающих, что спецификой следственных действий, предусмотренных ст. 186, 186.1 УПК РФ, является, во-первых, в известной степени «отстраненность» следователя от места их фактического производства (особенно применительно к первоначальному рабочему этапу), во-вторых, осуществление этого этапа учреждениями связи или специализированными подразделениями в автоматизированном формате по поручению следователя [21, с. 95–100; 22, с. 129–133]. В этой связи мы частично солидаризируемся с исследователями, критически оценивающими контроль и запись телефонных и иных переговоров, а также получение

информации о соединениях между абонентами и/или абонентскими устройствами, с точки зрения их отнесенности законодателем к категории следственных действий [23, с. 10].

Вместе с тем наша «частичная солидарность» с противниками отнесения к категории следственных действий контроля телефонных и иных переговоров, а также получения информации о соединениях между абонентами и/или абонентскими устройствами, касается лишь первого рабочего этапа, а также сочетается с отсутствием сомнения в наличии уголовно-процессуальной природы у последующих рабочих этапов указанных следственных действий.

Итак, этап осмотра и прослушивания фонограммы (а равно осмотра документов и материалов, содержащих сведения о телекоммуникационных контактах) соответствует общим требованиям производства осмотра предметов и документов — как самостоятельного следственного действия, процессуальная сущность которого заключается в непосредственном обследовании соответствующего объекта, выявлении следов преступления и иных значимых для расследования обстоятельств. Напомним еще раз, что в формате осмотра предметов и документов именно как самостоятельного действия, предусмотренного ст. 176 УПК РФ, происходит осмотр и прослушивание фонограммы, а также иных документов и материалов, полученных из оперативных или иных источников (вне процессуальной формы следственных действий, предусмотренных ст. 186, 186.1 УПК РФ).

Но при проведении осмотра и прослушивании фонограммы (осмотра документов и материалов, содержащих сведения о телекоммуникационных контактах) как этапов следственных действий, регламентированных ст. 186, 186.1 УПК РФ, законодатель устанавливает дополнительные требования и условия. В частности, согласно ч. 6–7 ст. 186 УПК РФ фонограмма, отражающая факт телекоммуникационных контактов, передается следователю для осмотра и прослушивания в опечатанном виде, снабженная сопроводительным письмом, содержащим информацию о дате, времени состоявшихся переговоров и их записи, кратких характеристиках использованных технических средств. Результаты осмотра и прослушивания фонограммы фиксируются в протоколе, где требуется дословно отразить фрагмент, имеющий непосредственное отношение к уголовному делу.

Интересным представляется подход к определению обязательных и факультативных участников анализируемого следственного действия, которые вправе изложить свои замечания, причем не только в настоящем протоколе, но и в отдельном самостоятельном материале. Специалист приглашается при необходимости, а вот участие лиц, чьи телефонные или иные переговоры запечатлены на фонограмме, как следует из буквального прочтения ч. 7 ст. 186 УПК РФ, требуется в любом случае, т.е. без каких-либо условий.

Нам представляется такой подход не совсем удачным. Необходимость участия как специалиста, так и лиц, фигурировавших в «перехваченных» телекоммуникационных переговорах, должна определяться исключительно решением следователя.

Телекоммуникационные переговоры — это взаимодействие, как минимум, двух собеседников, находящихся на удалении друг от друга, состоящих в различных взаимоотношениях, при этом далеко не всегда являющихся соучастниками. Обсуждая с помощью средств телекоммуникационной связи сведения, имеющие значение для расследования, субъекты не обязательно осведомлены о наличии криминальной подоплеки. Оба абонента могут проходить по делу в различном статусе (свидетеля, потерпевшего, подозреваемого, обвиняемого), либо таким статусом может быть наделен один из них, тогда как другой вообще не вовлечен в судопроизводство.

Не всегда тактически рационально вызывать для участия в осмотре и прослушивании фонограммы субъекта, находящегося в другом регионе. Тем более применительно далеко не к каждому случаю вообще следует приглашать обоих абонентов по различным причинам: будь это риск преждевременного получения доказательственной информации и ее разглашения либо вероятность сговора (согласование вне установленной для этого процессуальной процедуры до официального момента производства следственного действия).

Кроме того, фигурант может контактировать в удаленном формате не с одним, а с некоторым множеством абонентов. Результаты такого взаимодействия зачастую тактически целесообразно обследовать в рамках одного следственного действия, однако при этом устанавливать личность и приглашать всех собеседников, на наш взгляд, даже противоречит здравому смыслу.

Поскольку сам по себе процесс перехвата телекоммуникационных контактов носит негласный характер (за исключением случаев, когда такая мера производится по заявлению

потерпевшего, свидетеля в целях обеспечения безопасности), то и ознакомление с его результатами также не должно в обязательном порядке быть связано с вызовом и участием ранее дистанционно общавшихся лиц, иначе снижается эффект фактора внезапности.

Поэтому мы считаем, что именно следователь, исходя из оценки складывающейся ситуации, должен быть уполномочен принимать решение о выборе для участия в осмотре и прослушивании фонограммы, полученной в результате контроля и записи телефонных и иных переговоров, всех выше обозначенных участников: специалиста (криминалиста, специалиста в области фоноскопии), одного или обоих (нескольких) субъектов дистанционного взаимодействия, либо осуществить следственное действие единолично.

Участие понятых в осмотре и прослушивании фонограммы телефонных или иных переговоров, как следует из ч. 1.1 ст. 170 УПК РФ, зависит от усмотрения следователя, что представляется рациональным, поскольку применение средств аудиовидеозаписи, объективно отображающих весь процесс и результаты следственного действия (наряду с протоколом как основным средством фиксации), не только вполне достаточно, но и обладает очевидными преимуществами. При этом не исключается возможность приглашения понятых, если следователь считает такой подход более результативным.

В соответствии с ч. 8 ст. 186 УПК РФ, на основании постановления следователя фонограмма в полном объеме приобщается к материалам дела в качестве вещественного доказательства и хранится в опечатанном виде в условиях, исключающих доступ к ней иных лиц, а также обеспечивающих возможность ее дальнейшего исследования в предусмотренных законом случаях. Не оспаривая требование обеспечения сохранности фонограммы, прежде всего для достоверности зафиксированной на ней информации, отметим, что несколько удивляет определенный законодателем статус фонограммы — вещественное доказательство. И хотя отдаленно фонограмма соответствует критериям, предъявляемым к вещественным доказательствам согласно п. 3 ч. 1 ст. 81 УПК РФ («иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела»), все же более логичным представляется ее статус как иных документов, предусмотренных ст. 84 УПК РФ.

Сходный механизм формирования доказательств характерен для приобщения результатов телекоммуникационных контактов между абонентами и/или абонентскими устройствами, в соответствии со ст. 186.1 УПК РФ. Следователь обязан осмотреть представленные документы, отражающие информацию о соединениях между абонентами и/или абонентскими устройствами, отразив в протоколе как сам факт осмотра, так и непосредственно информацию, имеющую отношение к делу. При этом законодатель не требует обязательного участия в следственном действии прочих лиц. Приглашение специалиста предусматривается лишь при возникновении необходимости (ч. 5 ст. 186.1 УПК РФ), в отношении иных лиц отсутствует упоминание как таковое, что не исключает наличия у следователя такой возможности, исходя из общих требований к производству следственных действий.

Осмотренные документы аналогично правилам, изложенным применительно к контролю и записи переговоров, также надлежит на основании постановления следователя приобщить к материалам уголовного дела в качестве вещественных доказательств, что также вызывает критику. Аргументы — аналогичны приводимым выше.

Фонограммы, документы и иные материалы, отражающие факт телекоммуникационных контактов, полученные в качестве результатов оперативно-розыскной деятельности, разумеется, тоже надлежит приобщить к материалам уголовного дела, трансформировав в доказательства. Однако применительно к этой группе доказательственной информации отсутствует конкретный уголовно-процессуальный механизм, несмотря на, по сути, единую технологическую природу с рассмотренными выше разновидностями.

На практике отсутствует единство в понимании: следует ли применительно к осмотру и прослушиванию фонограммы, осмотру иных документов и материалов, полученных в качестве результатов оперативно-розыскной деятельности (причем не обязательно наработанных на основании поручения следователя, но и осуществленных оперативными подразделениями инициативно), руководствоваться требованиями ст. 186, 186.1 УПК РФ, либо достаточно обратиться к общим правилам производства осмотра предметов и документов, изложенных в ст. 176, 177, 180 УПК РФ.

Нам представляется, что, поскольку законодатель не конкретизирует механизм трансфор-

мации результатов оперативно-розыскной деятельности в доказательства, а контроль и запись переговоров (ст. 186 УПК РФ), как и получение информации о соединениях между абонентами и/или абонентскими устройствами (ст. 186.1 УПК РФ), позиционируются в качестве самостоятельных сложнокомпонентных следственных действий, в данном случае отсутствуют процессуальные основания применять положения ст. 186, 186.1 УПК РФ, а надлежит руководствоваться требованиями ст. 176, 177, 180 УПК РФ, — в части осмотра предметов и документов.

Но тогда возникают проблемы иного рода. Осмотр предметов и документов, хотя и предусматривается в указанных выше нормах УПК РФ наряду с прочими видами осмотра, тем не менее законодатель уделяет приоритетное внимание предметам или документам, которые обнаружены на месте происшествия в качестве следов преступления (ч. 2 ст. 177 УПК РФ). Законодатель рекомендует их обследовать «на месте производства следственного действия», надо полагать в рамках осмотра места происшествия (местности, жилища, иного помещения). Если для производства такого осмотра требуется продолжительное время либо осмотр на месте затруднен, то предметы должны быть изъяты, упакованы, опечатаны, заверены подписью следователя на месте осмотра (ч. 3 ст. 177 УПК РФ).

Однако при получении предметов и документов, иных материалов как результатов ОРД приоритетное значение приобретает не столько их связь с пространственной обстановкой, где они ранее находились (тем более, где были выданы следователю), сколько содержание зафиксированной информации. Аналогичная, более универсальная, проблема распространяется на все материальные объекты, полученные вне процедуры осмотра места происшествия (местности, жилища, иного помещения), например, в результате обыска, выемки и пр. Поэтому нам представляется, что законодателю целесообразно было бы прописать общие условия и порядок производства осмотра предметов и документов, независимо от обстоятельств их обнаружения, изъятия, представления в уголовное судопроизводство.

Более того, несмотря на продолжающуюся тенденцию цифровизации различных сфер общества и востребованности удаленного формата общения, в том числе в открытом доступе с неопределенно широким кругом лиц, включая публикации различных постов в соцсетях, мессенджерах, репосты, комментарии к публикациям других пользователей и т.д., в УПК РФ до сих пор отсутствуют положения, регулирующие условия, обстоятельства, порядок осмотра соответствующей информации, опубликованной в сети Интернет. При этом в УК РФ присутствует целый ряд преступлений, состав которых напрямую предусматривает использование интернет-ресурсов (прежде всего преступления, связанные с пропагандой экстремизма и др.). Это вынуждает следователей или дознавателей проводить такой осмотр по правилам осмотра предметов и документов, или в рамках осмотра места происшествия.

Однако очевидно, что ни цели производства такого осмотра, ни его сущность не вполне соответствуют тем, которые предусмотрены применительно к осмотру места происшествия, а также предметов и документов. Ведь в данном случае существует запрос не столько в обследовании компьютерного средства как предмета, сколько информации, содержащейся на определенной интернет-страничке (тем более, если это обследование осуществляется с помощью компьютерного средства, принадлежащего органу расследования).

Итак, регламентированные в ст. 186, 186.1 УПК РФ процессуальные процедуры, отражающие работу с информацией, передаваемой с помощью телекоммуникационной связи, по своей сути представляют собой не сложнокомпонентные следственные действия, а тактические (оперативно-тактические) комбинации, включающие: 1) поручение следователя, в ряде случаев подкрепленное принятием судебного решения; 2) выполнение поручения следователя иными уполномоченными субъектами (оперативными подразделениями, организациями, оказывающими услуги связи); 3) предоставление следователю результатов мониторинга телекоммуникационных контактов уполномоченными субъектами; 4) изучение следователем представленной информации, принятие решения о приобщении ее к материалам дела в качестве доказательств. Следовательно, только последний пункт в полной мере соответствует процессуальной форме следственного действия. Неудивительно, что на практике правоприменители осторожно относятся к возможностям ст. 186 УПК РФ в части назначения контроля и записи переговоров, предпочитая инициировать получение доказательственной информации через процедуру оперативно-розыскных мероприятий.

С другой стороны, технологически сходные оперативно-розыскные мероприятия, результаты которых предоставляются в органы следствия (проведенные как на основании поручения, так и инициативно), также подлежат процедуре трансформации в доказательства, одним из существенных компонентов которой является осмотр представленных носителей, в процессе которого происходит не только визуальное обследование, но и прослушивание фонограмм, анализ документов и иных материалов, с дословной фиксацией той части, которая непосредственно имеет отношение к расследованию.

Представляется, что общность технологических процедур формирования доказательственной информации, передаваемой с помощью средств телекоммуникационной связи, а также недостаточная согласованность процессуальных норм, регулирующих основания и порядок работы с соответствующими источниками сведений, свидетельствует о целесообразности их унификации в УПК РФ, что представляется одним из направлений глобальных и многогранных проблем, сопровождающих процесс цифровизации уголовного судопроизводства [24, с. 60–66].

Вариантом разрешения этих проблем представляется следующий подход, который, в случае его принятия, подлежит регламентации в УПК РФ путем корректировки действующих норм (ст. 186, 186.1, п. 14.1, 24.1 ст. 5 УПК РФ и др.) и введения новых. В рамках контроля телефонных и иных переговоров, а также получения информации о соединениях между абонентами и/или абонентскими устройствами, как следственных действий познавательного характера, следует понимать непосредственное обследование и восприятие информации, содержащейся на представленных в органы расследования носителях, отражающих факт и/или содержание взаимодействия с помощью средств телекоммуникационной связи между субъектами.

Данные материалы могут быть представлены органами дознания и иными уполномоченными лицами, как в порядке выполнения поручений следователя о производстве оперативно-розыскных мероприятий, так и, в предусмотренных законом случаях, инициативно. Более того, результаты оперативно-розыскной деятельности в ряде случаев могут быть представлены в виде не только аудио-, но и видеозаписи (если оперативно-розыскные мероприятия выполнялись инициативно либо поручением следователя допускались различные способы мониторинга). Также ранее мы уже упоминали актуальность такого метода уголовно-процессуального познания, как самостоятельное изучение следователем значимых для расследования интернет-ресурсов, алгоритм которого в целом идентичен обозначенному ниже.

В уголовно-процессуальном законе целесообразно определить универсальные требования, правила, условия применительно к обследованию этих носителей, включающие: 1) обязательных и факультативных участников следственного действия (при этом нам представляется, что факультативными участниками должны признаваться: понятые, специалист, лица, участвующие в телекоммуникационных контактах); 2) обязательность ведения видеозаписи, за исключением случаев объективной невозможности этого; 3) технические характеристики использованного оборудования; 4) общие характеристики носителей информации, выступающих объектом обследования; 5) последовательность осмотра документов и иных материалов, а также прослушивания аудиоинформации; 6) отражение в протоколе процесса обследования материалов, а также изложение информации, имеющей значение для расследования; 7) сведения об упаковке объектов, обеспечивающих достоверность и сохранность.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Репецкая А.Л. Современный криминальный рынок в период пандемии и проблемы борьбы с ним / А.Л. Репецкая. — DOI 10.51980/978-5-7889-0333-0_2022_5_1_90. — EDN HSPILB // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXV Междунар. науч.-практ. конф., Красноярск, 07–08 апр. 2022 г. — Красноярск, 2022. — Т. 1. — С. 90–92.

2. Репецкая А.Л. Современный российский криминальный рынок услуг в условиях глобальной цифровизации / А.Л. Репецкая. — EDN LNCYAB // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXVI Междунар. науч.-практ. конф., Красноярск, 20–21 апр. 2023 г. — Красноярск, 2023. — Т. 1. — С. 108–110.

3. Грибунов О.П. Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения / О.П. Грибунов, С.И. Усачев, Е.А. Усачева. — DOI 10.18572/1812-3783-2024-4-7-12. — EDN QOZDHZ // Российский следователь. — 2024. — № 4. — С. 7–12.

4. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring / B. Dupont. — DOI 10.1080/0735648X.2019.1691855 // Journal of Crime and Justice. — 2019. — Vol. 42, iss. 5. — P. 500–515.

5. Davidoff S. Network Forensics: Tracking Hackers through Cyberspace / S. Davidoff, J. Ham. — Upper Saddle River, NJ : Prentice Hall, 2012. — 576 p.

6. Антонова Е.Ю. Цифровизация и ее влияние на механизм совершения преступления (на примере посягательств против половой неприкосновенности несовершеннолетних) / Е.Ю. Антонова. — EDN FCDCOP // Уголовное право: стратегия развития в XXI веке. — 2023. — № 3. — С. 39–48.

7. Головин А.Ю. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий / А.Ю. Головин, Е.В. Головина. — DOI 10.24412/2071-6184-2021-2-3-13. — EDN EVKMDP // Известия Тульского государственного университета. Экономические и юридические науки. — 2021. — № 2. — С. 3–13.

8. Поляков В.В. Применение методов социальной инженерии при совершении высокотехнологичных преступлений / В.В. Поляков. — DOI 10.55001/2587-9820.2023.81.15.018. — EDN KKIEBE // Криминалистика: вчера, сегодня, завтра. — 2023. — № 3 (27). — С. 175–188.

9. Протасевич А.А. Эра милосердия. Пути развития преступности / Д.В. Жмуров, А.А. Протасевич, А.С. Костромина. — DOI 10.17150/2411-6262.2019.10(2).18. — EDN BPRASG // Baikal Research Journal. — 2019. — Т. 10, № 2. — С. 18.

10. Сидорова Е.З. Особенности квалификации и предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий / Е.З. Сидорова, О.П. Грибунов. — Иркутск : Изд-во Вост.-Сиб. ин-та МВД России, 2024. — 128 с. — EDN NATJFS.

11. Bossler A.M. Introduction: New Directions in Cybercrime Research / A.M. Bossler, T. Berenblum. — DOI 10.1080/0735648X.2019.1692426 // Journal of Crime and Justice. — 2019. — Vol. 42, no. 5. — P. 495–499.

12. Репецкая А.Л. Криптопреступления как следствие цифровизации преступности / А.Л. Репецкая. — EDN RBNNCU // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сб. материалов Всерос. науч.-практ. конф., Москва, 27 янв. 2021 г. — Москва, 2021. — С. 61–67.

13. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия / Е.Л. Глушков. — EDN XTXKZN // Проблемы правоохранительной деятельности. — 2018. — № 2. — С. 45–53.

14. Коломинов В.В. О криминалистической характеристике личности членов молодежных течений экстремистской направленности / В.В. Коломинов, Е.И. Фойгель, А.К. Щербаченко. — EDN CDNQHY // Юристъ-Правоведъ. — 2023. — № 1 (104). — С. 90–96.

15. Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей / В.В. Бычков. — EDN WAYXAI // Проблемы противодействия киберпреступности : материалы Междунар. науч.-практ. конф., Москва, 28 апр. 2023 г. — Москва, 2023. — С. 26–31.

16. Killean R. Sexual Violence in the Digital Age: Replicating and Augmenting Harm, Victimhood and Blame / R. Killean, A.-M. McAlinden, E. Dowds. — DOI 10.1177/09646639221086592 // Social & Legal Studies. — 2022. — Vol. 31, no. 6. — P. 871–892.

17. Sheikh M.M.R. Technology-Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review / M.M.R. Sheikh, M.M. Rogers. — DOI 10.1177/15248380231191189 // Trauma, Violence, & Abuse. — 2024. — Vol. 25, no. 2. — P. 1614–1629.

18. Михайлова Е.В. Вовлечение несовершеннолетних в сексуальную эксплуатацию с использованием информационно-телекоммуникационных технологий / Е.В. Михайлова. — EDN IKAHGP // Ученые записки Казанского юридического института МВД России. — 2021. — Т. 6, № 2 (12). — С. 215–219.

19. Цифровые следы преступлений / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. — Москва : Проспект, 2023. — 168 с. — EDN MDHESX.

20. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А.А. Бессонов. — EDN CHQQAU // Академическая мысль. — 2020. — № 4 (13). — С. 58–61.

21. Шурухнов Н.Г. Повышение результативности отдельных следственных действий (контроль и запись переговоров, получение информации о соединении абонентов и (или) абонентских устройств) / Н.Г. Шурухнов, Д.А. Гришин. — EDN AZZMQQ // Лоббирование в законодательстве. — 2024. — Т. 3, № 4. — С. 95–100.

22. Князьков А.С. Признаки и система следственных действий / А.С. Князьков. — EDN ONQFPV // Вестник Томского государственного университета. — 2011. — № 352. — С. 129–133.

23. Давыдовская М.В. Общие правила производства следственных действий : автореф. дис. … канд. юрид. наук : 5.1.4 / М.В. Давыдовская. — Москва, 2023. — 26 с.

24. Фойгель Е.И. Естественнонаучная точка бифуркации в развитии криминалистического и уголовно-процессуального обеспечения выявления и раскрытия преступлений / Е.И. Фойгель, А.К. Щербаченко. — EDN MZUTJA // Общество и право. — 2023. — № 1 (83). — С. 60–66.

REFERENCES

1. Repetskaya A.L. Modern Criminal Market in the Period of the Pandemic and the Problems of Counteracting it. *Topical Problems of Fighting Crime: Questions of Theory and Practice. Proceedings of the XV International Scientific and Practical Conference, Krasnoyarsk, 07–08 April, 2022*. Krasnoyarsk, 2022. Vol. 1, pp. 90–92. (In Russian). EDN: HSPILB.

2. Repetskaya A.L. Modern Russian Criminal Market of Services in the Conditions of Global Digitization. *Topical Problems of Fighting Crime: Questions Theory and Practice. Proceedings of the XVI International Scientific and Practical Conference, Krasnoyarsk, April 20–21, 2023*. Krasnoyarsk, 2023. Vol. 1, pp. 108–110. (In Russian). EDN: LNCYAB.

3. Gribunov O.P., Usachev S.I., Usacheva E.A. Cryptocurrency and Other Virtual Assets as a Phenomenon of Contemporary Crime: Problems of Solution, Investigation and Prevention. *Rossiiskii sledovatel = Russian Investigator*, 2024, no. 4, pp. 7–12. (In Russian). EDN: QOZDHZ. DOI: 10.18572/1812-3783-2024-4-7-12.

4. Dupont B. Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring. *Journal of Crime and Justice*, 2019, vol. 42, iss. 5, pp. 500–515. – DOI: 10.1080/0735648X.2019.1691855.

5. Davidoff S., Ham J. *Network Forensics: Tracking Hackers through Cyberspace*. Upper Saddle River, NJ, Prentice Hall, 2012. 576 p.

6. Antonova E.Yu. Digitalization and its Impact on the Mechanism of Committing a Crime (on the Example of Infringements against the Sexual Integrity of Minors). *Ugolovnoe pravo: strategiya razvitiya v XXI veke = Criminal Law: Development Strategy in the 21st Century*, 2023, no. 3, pp. 39–48. (In Russian). EDN: FCDCOP.

7. Golovin A.Yu., Golovina E.V. Social Engineering in the Mechanism of Criminal Activity in the Field of Information and Telecommunications Technologies. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of the Tula State University. Economic and Legal Sciences*, 2021, no. 2, pp. 3–13. (In Russian). EDN: EVKMDP. DOI: 10.24412/2071-6184-2021-2-3-13.

8. Polyakov V.V. Application of Social Engineering Technologies when High-Tech Crimes are Committed. *Kriminalistika: vchera, segodnya, zavtra = Criminalistics: Yesterday, Today, Tomorrow*, 2023, no. 3, pp. 175–188. (In Russian). EDN: KKIEBE. DOI: 10.55001/2587-9820.2023.81.15.018.

9. Zhmurov D.V., Protasevich A.A., Kostromina A.S. The Era of Mercy. Ways of Criminality Development. *Baikal Research Journal*, 2019, vol. 10, no. 2, pp. 18. (In Russian). EDN: BPRASG. DOI: 10.17150/2411-6262.2019.10(2).18.

10. Sidorova E.Z., Gribunov O.P. *Specific Features of Qualification and Prevention of Crimes Committed with the Use of Information (Digital) Technologies.* Irkutsk, East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2024. 128 p. EDN: NATJFS.

11. Bossler A.M., Berenblum T. Introduction: New Directions in Cybercrime Research. *Journal of Crime and Justice*, 2019, vol. 42, no. 5, pp. 495–499. DOI: 10.1080/0735648X.2019.1692426.

12. Repeckaja, A. L. Cryptocrime as a Consequence of the Digitalization of Crime. In Digital Technologies in the Fight Against Crime: Problems, Status, Trends. *Collection of Proceedings of I All-Russian Scientific-practical Conference, Moscow, 27 January 2021*. Moskow, 2021, pp. 65. (In Russian). EDN: RBNNCU.

13. Glushkov E.L. About Some Questions of Distribution in a Contactless Manner of Drugs via the Internet: Ways of Identification and Disclosure. *Problemy pravookhranitel'noi deyatel'nosti = Problems of Law Enforcement Activity*, 2018, no. 2, pp. 45–53. (In Russian). EDN: XTXKZN.

14. Kolominov V.V., Foigel E.I., Shcherbachenko A.K. On the Criminalistic Characterization of the Personality of Members of Extremist Youth Movements. *Yurist-Pravoved = Lawyer-Legal Scholar*, 2023, no. 1, pp 90–96. (In Russian). EDN: CDNQHY.

15. Bychkov V.V. On the Relevance of Researching the Problems of Counteracting Extremist Crimes Committed with the Use of Information-Telecommunication Networks. *Problems of Counteracting Cybercrime. Materials of International Scientific Conference, Moscow, April 28, 2023*. Moscow, 2023, pp. 26–31. (In Russian). EDN: WAYXAI.

16. Killean R., McAlinden A.-M., Dowds E. Sexual Violence in the Digital Age: Replicating and Augmenting Harm, Victimhood and Blame. *Social & Legal Studies*, 2022, vol. 31, no. 6, pp. 871–892. DOI: 10.1177/09646639221086592.

17. Sheikh M.M.R. Technology Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review. *Trauma, Violence, & Abuse*, 2024. vol. 25, no. 2, pp. 1614–1629. DOI: 10.1177/15248380231191189.

18. Mihailova E.V. Involvement of Minors in Sexual Exploitation Using Information and Telecommunications Technologies. *Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii = Scientific Notes of Kazan Law Institute of MIA of Russia*, 2021, vol. 6, no. 2, pp. 215–219. (In Russian). EDN: IKAHGP.

19. Bagmet A.M., Bychkov V.V., Skobelin S.Yu., Ilin N.N. *Digital Traces of Crimes*. Moscow, Prospect Publ., 2023. 168 p. EDN: MDHESX.

20. Bessonov A.A. Digital Forensic Crime Model as a Basis for Countering Cybercrime. *Akademicheskaya mysl' = Academic Thought*, 2020, no. 4, pp. 58–61. (In Russian). EDN: CHQQAU.

21. Shurukhnov N.G., Grishin D.A. Improving the Effectiveness of Individual Investigative Actions (Monitoring and Recording of Negotiations, Obtaining Information about the Connection of Subscribers and (or) Subscriber Devices). *Lobbirovanie v zakonodatel'stve = Lobbying in the Legislative Process*, 2024, vol. 3, no. 4, pp. 95–100. (In Russian). EDN: AZZMQQ.

22. Knyazkov A.S. Features and System of Investigative Actions. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2011, no. 352, pp. 129–133. (In Russian). EDN: ONQFPV.

23. Davydovskaya M.V. *General Procedures for Investigative Actions.* Cand. Diss. Thesis. Moscow, 2023. 26 p.

24. Foygel E.I., Sherbachenko A.K. The Natural Sciences' Point of Bifurcation in Developing the Criminalistic and Criminal Procedure Support for Detecting and Solving Crimes. *Obshchestvo i pravo = Society and Law*, 2023, no. 1, pp. 60–66. (In Russian). EDN: MZUTJA.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Варданян Акоп Вараздатович — начальник кафедры криминалистики и оперативно-разыскной деятельности Ростовского юридического института Министерства внутренних дел Российской Федерации, доктор юридических наук, профессор, г. Ростов-на-Дону, Российская Федерация; e-mail: avardanyan@yandex.ru.

INFORMATION ABOUT THE AUTHOR

Vardanyan, Akop V. — Head, Department of Criminalistics and Operational Investigative Activities, Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation, Doctor of Law, Professor, Rostov-on-Don, the Russian Federation; e-mail: avardanyan@yandex.ru.

ДЛЯ ЦИТИРОВАНИЯ

Варданян А.В. Следственные действия, связанные с мониторингом информации, передаваемой с помощью средств телекоммуникационной связи: некоторые проблемы регламентации и правоприменения в свете современных потребностей борьбы с преступностью / А.В. Варданян. — DOI 10.17150/2500-4255.2025.19(2).210-220. — EDN JWDPKQ // Всероссийский криминологический журнал. — 2025. — Т. 19, № 2. — С. 210–220.

FOR CITATION

Vardanyan A.V. Key Investigative Actions Related to the Monitoring of Information Transmitted by Means of Telecommunication: Some Problems of Regulation and Law Enforcement in the Light of Modern Crime Control Needs. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2025, vol. 19, no. 2, pp. 210–220. (In Russian). EDN: JWDPKQ. DOI: 10.17150/2500-4255.2025.19(2).210-220.