Научная статья
УДК 343.1
DOI: 10.55001/2587-9820.2023.15.28.005

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК ПОЛУЧЕНИЯ ГОЛОСОВОЙ ИНФОРМАЦИИ У ОПЕРАТОРОВ СВЯЗИ И ОРГАНИЗАТОРОВ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Степан Евгеньевич Гольцов
Академия управления МВД России, г. Москва, Российская Федерация, Stathamst@yandex.ru

Аннотация. В статье рассматриваются преступления, совершаемые в сети Интернет посредством цифровых средств анонимизации, а также следственная и судебная практика по уголовным делаем указанной категории. На основании проведенного сравнительно-правового анализа сделан вывод о наиболее распространенных способах совершения преступлений с использованием информационно-телекоммуникационных технологий и сокрытия цифровых следов. Помимо вышеизложенного автором выявлены проблемы, которые возникают у сотрудников подразделений следствия и дознания, осуществляющих производство по уголовным делам указанной категории, при собирании доказательственной голосовой информации. Несмотря на постоянно совершенствующиеся меры по противодействию, предотвращению, пресечению, предупреждению, раскрытию и расследованию данных преступлений, они показывают возрастающую динамику прироста в общем массиве преступлений, совершаемых в Российской Федерации.

В связи с этим автор предлагает некоторые нормативно-правовые меры, направленные на повышение эффективности противодействия, раскрытия и расследования преступлений, совершаемых с использованием компьютерных технологий, специальных программ-анонимайзеров, а также на совершенствование уголовно-процессуального законодательства, регулирующего получение голосовой информации следователями и дознавателями.

Ключевые слова: голосовая информация, уголовно-процессуальный порядок, операторы связи, организаторы распространения информации в сети Интернет, цифровые средства анонимизации.

Для цитирования: Гольцов С. Е. Уголовно-процессуальный порядок получения голосовой информации у операторов связи и организаторов распространения информации в сети Интернет// Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2023. Т. 27. № 3. С. 41–49. DOI: 10.55001/2587-9820.2023.15.28.005

CRIMINAL PROCEDURE PROCESS FOR OBTAINING VOICE INFORMATION FROM TELECOM OPERATORS AND ORGANIZERS OF INFORMATION DISSEMINATION ON THE INTERNET

Stepan E. Goltsov
Academy of Management of the MIA of Russia, Moscow, Russian Federation, Stathamst@yandex.ru

Abstract. In the article, the author examines crimes that are committed through digital means of anonymization on the Internet, investigative and judicial practice in

criminal cases of this category. Based on the conducted comparative legal analysis, the author comes to the conclusion about the most common ways of committing crimes using information and telecommunication technologies and hiding digital traces of crimes at the present time. In addition to the above, the author has identified problems that arise among employees of the investigation and inquiry units conducting criminal proceedings in this cate-gory when collecting evidentiary voice information. Despite the constantly improving measures to counteract, prevent, suppress, prevent, disclose and investigate these crimes, they continuously show an increasing dynamics of growth in the total array of crimes committed in the Russian Federation. In this connection, the author suggests some regulatory and legal measures aimed at improving the effectiveness of countering, disclosing and investigat-ing crimes committed using computer technologies, special anonymizer pro-grams used by criminals in the digital space, as well as improving criminal procedural legislation regulating the receipt of voice information by investi-gators and interrogators.

Key words: voice information, criminal procedure process, telecom operators, organizers of information dissemination on the Internet, digital means of anonymiza-tion.

For citation: Goltsov, S. E. Ugolovno-processual'nyj poryadok polucheniya golosovoj informacii u operatorov svyazi i organizatorov rasprostraneniya informacii v seti Internet [Criminal procedure process for obtaining voice information from telecom operators and organizers of information dissemination on the Internet]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2023, vol. 27, no. 3, pp. 41–49 (in Russ.). DOI: 10.55001/2587-9820.2023.15.28.005

Введение

В настоящее время наиболее эффективными средствами анонимизации в сети Интернет выступают программные технологии «VPN», «TOR», «SSL», позволяющие менять IP-адреса, создавать динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров. В свою очередь правоохранительные органы не располагают надежными и эффективными техническими инструментами противодействия современным способам сокрытия преступлений и их деанонимизации [**Ошибка! Источник ссылки не найден.**, с. 6].

Основным детерминантом развития цифровой преступности выступают все более прогрессирующие с каждым годом технические возможности человечества в цифровом пространстве. Технический прогресс в первую очередь используют преступники при совершении общественно опасных деяний, и в качестве самых распространенных информационно-телекоммуникационных технологий они активно задействуют сервисы SIP-телефонии [2 с. 9], IP-телефонии[1], технологии синтеза изображений «DeepFake» и подмены голоса «Voice cloning», компьютерные программы – анонимайзеры, в том числе VPN-сервисы и Proxy-серверы, а также технологии «Блокчейн» [3, с. 9] при криминальных финансовых взаиморасчетах посредством цифровой валюты.

Ю. В. Гаврилин утверждает: «Одним из самых распространенных на данный момент проявлений цифровой трансформации преступности является активное внедрение цифро-

[1] IP-телефония – это технология, позволяющая использовать Интернет или любую другую IP-сеть в качестве средства организации и ведения международных телефонных разговоров и передачи факсов в режиме реального времени.

вых валют в механизм совершения криминальных взаиморасчетов в сфере незаконного оборота наркотических средств, психотропных веществ, а также иных объектов, изъятых из гражданского оборота. Кроме того, они широко используются при создании «финансовых пирамид», легализации (отмывании) денежных средств, добытых преступным путем, а также как средство незаконного анонимного финансирования экстремистской и террористической деятельности» [4, с. 102].

Основная часть

Подобная ситуация в сфере цифрового, информационного пространства создает комплекс технических и юридических проблем, с которыми сталкиваются органы предварительного расследования. Анализ состояния преступности в России, следственно-судебной практики показал, что самыми популярными способами совершения противоправных деяний и сокрытия «цифровых» следов преступлений на данный момент являются VPN-сервисы и Proxy-серверы, а также IP-телефония[2].

Так, согласно приговору Агаповского районного суда Челябинской области от 07 июля 2020 г. по делу № 1-51/2020, одно из неустановленных лиц, используя электронные и информационно-телекоммуникационные сети (Интернет), а именно программное приложение, предназначенное для повседневного общения людей посредством IP-телефонии и мгновенного обмена сообщениями в сети Интернет, с целью расширения незаконной деятельности и извлечения большего материального дохода предложило ранее незнакомому Махмудову Ш. М., испытывающему временные материальные трудности, заняться незаконным сбытом наркотических средств в роли «закладчика»[3]. Это один из многих судебных актов Российской Федерации, который наглядно демонстрирует в своей описательно-мотивировочной части использование преступниками вышеперечисленных дистанционных способов совершения преступлений, что еще раз подтверждает актуальность борьбы с подобными противоправными деяниями и, как следствие, выработки эффективного уголовно-процессуального инструментария и криминалистической тактики расследования подобных общественно опасных деяний.

Таким образом, закономерным вопросом, которым задаются следователи и дознаватели при планировании расследования преступлений, совершенных с применением информационных и телекоммуникационных технологий, является выбор процессуальных и следственных действий, направленных на собирание всей криминалистически значимой информации, которая находится в цифровом пространстве.

Частным случаем такой криминалистически значимой информации для органов предварительного расследования выступает голосовая информация, которая является одним из самых распространенных видов цифровых следов, оставляемых в результате совершения преступлений в сфере информационно-телекоммуникационных технологий, особенно дистанционных мошенничеств.

[2] Число киберпреступлений в России // TAdviser – портал выбора технологий и поставщиков : Дата публикации: 23.05.2023. Режим доступа: свободный.

[3] Приговор Агаповского районного суда Челябинской области от 07 июля 2020 г. по делу № 1-51/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/qCkgxxJuGIJW/ (дата обращения: 15.04.2023). Режим доступа: свободный.

Так, в соответствии с нормативно-правовыми положениями, которыми была дополнена ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[4] (далее – ФЗ «Об информации»), организаторы распространения информации в сети Интернет[5] обязаны хранить на территории Российской Федерации и предоставлять согласно правовым предписаниям для целей уголовного процесса следующие сведения, предусмотренные Постановлением Правительства Российской Федерации от 23 сентября 2020 г. № 1526 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации»[6] (далее – Постановление Правительства № 1526):

1. Информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей и информацию о них.

2. Сведения о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей и данные о них организаторы должны хранить в течение одного года с момента окончания осуществления таких действий, а сами текстовые сообщения, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей – в течение шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

По мнению В. Б. Вехова и В. Ф. Васюкова, изложенные выше сведения возможно получать путем производ-

[4] Об информации, информационных технологиях и о защите информации : Федер. закон № 126-ФЗ : послед. ред. : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.04.2023). Режим доступа: свободный.

[5] В соответствии с ч. 1 ст. 10.1 ФЗ «Об информации», организатором распространения информации в сети «Интернет» является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет».

[6] О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации : Постановление Правительства Российской Федерации от 23 сентября 2020 г. № 1526 // Официальный интернет-портал правовой информации : сайт. URL: http://publication.pravo.gov.ru/Document/View/0001202009290021 (дата обращения: 25.04.2023). Режим доступа: свободный.

ства следственного действия, предусмотренного ст. 186.1 Уголовно-процессуального кодекса Российской Федерации[7] (УПК РФ) «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» [4, с. 11–15].

Аналогичную точку зрения можем встретить и в методических рекомендациях УОД МВД России, ФГКУ «ВНИИ МВД России» [6, с. 16], где указано, что информация о соединениях между абонентами и (или) абонентскими устройствами позволяет установить персональные данные абонентов операторов связи, место, время, количество и последовательность соединений между абонентами и абонентскими устройствами, а при необходимости и содержание отправленных или полученных абонентами сообщений в текстовой или иной форме (в виде фото-, видеоизображений или аудиозаписей). Вместе с тем, по нашему мнению, с вышеперечисленными позициями нельзя согласиться в полном объеме, так как они ошибочно отражают сущность данного следственного действия, поскольку п. 24.1 ст. 5 УПК РФ прямо определяет, какие данные могут быть получены путем его производства[8].

Таким образом, на данный момент в уголовно-процессуальном арсенале следователей и дознавателей для получения вышеперечисленных сведений находятся следственные действия, которые закреплены в ст. 186.1 УПК РФ и наименования которых звучат следующим образом: «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», и в ч. 7 ст. 185 УПК РФ «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка». Но данные следственные действия имеют иное предназначение, и их использование для собирания доказательственной голосовой информации, которая уже была обработана и сохранена в постоянной памяти серверов операторов связи и организаторов распространения информации в сети Интернет, является неуместным с точки зрения уголовно-процессуального закона.

Поясним вышесказанное. По нашему мнению, использование ст. 186.1 УПК РФ допустимо лишь для получения сведений, которые прямо указаны законодателем в п. 24.1 ст. 5 УПК РФ. Аналогично В. В. Гончар, Н. Н. Горач, Д. В. Галиев, Д. В. Гусев предлагают применять ч. 7 ст. 185 УПК РФ для получения значимой для доказывания голосовой информации, которая хранится в постоянной па-

[7] Уголовно-процессуальный кодекс Российской Федерации : УПК : послед. ред. : принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года // Гарант : сайт. URL: https://base.garant.ru/12125178/ (дата обращения: 25.04.2023). Режим доступа: свободный.

[8] В соответствии с п. 24.1 ст. 5 УПК РФ, получение информации о соединениях между абонентами и (или) абонентскими устройствами – это получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций.

мяти серверов операторов связи и организаторов распространения информации в сети Интернет [7, с. 33], что опять же не совсем соответствует процессуальным и криминалистическим целям, в которых производится данное следственное действие. Мы считаем, что производство следственного действия, предусмотренного ч. 7 ст. 185 УПК РФ, возможно лишь для получения голосовой информации, которая может содержаться в электронных сообщениях и которая собирается путем непосредственного ее обнаружения, фиксации и изъятия через персональные компьютеры, ноутбуки, планшеты и другие электронные устройства, принадлежащие участникам уголовного процесса. Примером может послужить обмен голосовыми сообщениями в различных социальных сетях и сервисах обмена мгновенными сообщениями. То есть осмотр и выемка таких голосовых сообщений производится следователем и дознавателем непосредственно через персональные компьютеры или же абонентские устройства.

В соответствии со статьей 10.1 ФЗ «Об информации», организаторы распространения информации в сети Интернет передают перечисленную информацию по запросу лишь подразделениям, осуществляющим оперативно-розыскную деятельность, в то время как о подразделениях следствия и дознания речи не идет, что негативно влияет на своевременность получения таких сведений следователями и дознавателями. Таким образом, должностные лица органов предварительного расследования вынуждены при необходимости получения такой информации выносить поручение органу дознания. Подобную ситуацию можем увидеть и в содержании ст. 46 Федерального закона от 07 сентября 2003 г. № 126-ФЗ «О связи»[9] (далее – ФЗ «О связи»), где субъектами инициирования запроса у операторов связи[10] выступают лишь подразделения, осуществляющие оперативно-розыскную деятельность, и некоторые другие органы исполнительной власти. В соответствии с ч. 2 ст. 14 УПК РФ, бремя доказывания в уголовном судопроизводстве лежит на стороне обвинения, основным должностным лицом которой является именно следователь (дознаватель). Соответственно, мы полагаем, что в ФЗ «О связи», ФЗ «Об информации» целесообразно внести полномочие вышеперечисленных должностных лиц на получение голосовой и иной информации, хранящейся у операторов связи и организаторов распространения информации в сети Интернет, а не ограничиваться органами, осуществляющими оперативно-розыскную деятельность или обеспечивающими безопасность Российской Федерации.

Еще одной немаловажной проблемой, с которой сталкиваются следователи и дознаватели при расследовании преступлений, совершенных с применением цифровых технологий, является долгое ожидание ответа (от нескольких недель до нескольких месяцев, а иногда и его отсутствие) на запрос, который был направлен в соответствии с ч. 4 ст. 21 УПК РФ, различными кредитными организациями, организациями,

[9] О связи : Федер. закон № 126-ФЗ : послед. ред. : принят Гос. Думой 18 июня 2003 года : одобрен Советом Федерации 25 июня 2003 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.04.2023). Режим доступа: свободный.

[10] В соответствии с п. 12 ст. 2 ФЗ «О связи», оператор связи – юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

предоставляющими услуги IP-телефонии и VPN, а также операторами сотовой связи о предоставлении интересующих предварительное расследование сведений, которые могут оказать значительное влияние на формирование доказательств стороной обвинения. Данные организации при получении в свой адрес подобного запроса не торопятся с ответом на него, поскольку самым серьезным неблагоприятным юридическим последствием в результате затягивания сроков ответа на подобные запросы для них является административная ответственность, предусмотренная ст. 17.7 Кодекса об административных правонарушениях Российской Федерации[11], то есть умышленное невыполнение требований следователя и дознавателя. Помимо перечисленного чаще всего преступники совершают преступления в отношении потенциальных потерпевших из других, отдаленных, субъектов Российской Федерации, а иногда и вовсе из иностранных государств.

Таким образом, длительные сроки ответов на запросы следователей и дознавателей, особенно тех подразделений, которые отдалены от головных офисов организаций, предоставляющих услуги IP-телефонии, операторов сотовой связи и организаторов распространения сети Интернет, также обусловлены большим расстоянием от места нахождения органов предварительного расследования.

Выводы и заключение

Представляется, что решением обозначенных проблем будут являться следующие меры правового характера:

– заключение договоров с кредитными организациями, операторами сотовой связи, организациями, предоставляющими услуги IP-телефонии, VPN и Proxy-сервисов, организаторами сервиса обмена мгновенными сообщениями, организаторами распространения инфор-мации в сети Интернет и иными коммерческими и некоммерческими организациями о взаимном сотрудничестве в области электронного документооборота с органами внутренних дел по направлению запросов, поручений и требований в соответствии с ч. 4 ст. 21 УПК РФ и получению на них ответов в виде электронных документов, в том числе с по-мощью сервиса электронного документооборота МВД России;

– рассмотрение вопроса о внесении в ч. 4 ст. 21 УПК РФ, ст. 10.1 Федерального закона от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и ст. 46 Федерального закона от 07.09.2003 г. № 126-ФЗ «О связи» строго установленных сроков для всех организаций в части направления ответов на запросы следователей и дознавателей – в течение 10 суток, если они были направлены посредством сервиса электронного документооборота (в случае нарушения данных сроков, на наш взгляд, такие действия следует квалифицировать как воспрепятствование осуществлению предварительного расследования);

– дополнение ст. 10.1 ФЗ «Об информации» и ст. 46 ФЗ «О связи» нормативными положениями, которые предусматривают в качестве субъектов направления запроса следователей и дознавателей по согласованию с руководителем следственного ор-

[11] Кодекс Российской Федерации об административных правонарушениях : КоАП : послед. ред. : принят Гос. Думой 20 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=le23jk9zsy155578243 (дата обращения: 13.04.2023). Режим доступа: свободный.

гана и прокурора соответственно для получения голосовой и иной информации, предусмотренной Постановлением Правительства № 1526, организаторам распространения информации в сети Интернет и операторам связи.

Перечень рассмотренных в нашем исследовании вопросов, касающихся расследования преступлений с использованием цифровых средств анонимизации, SIP-телефонии, IP-телефонии, мобильной связи, не является исчерпывающим. Модернизация нормативных правовых актов в области цифровых технологий, в том числе совершенствование уголовно-процессуального законодательства в части получения следователями и дознавателями значимой для доказывания голосовой информации, которая хранится на серверах операторов связи и организаторов распространения информации в сети Интернет, значительно повысят уровень противодействия цифровой преступности, эффективность, быстроту и качество предварительного расследования.

СПИСОК ИСТОЧНИКОВ

1. Особенности расследования преступлений, совершаемых в сети Интернет с использованием средств анонимизации : метод. рекомендации // А. И. Гайдин, Е. А. Пидусов, А. В. Головчанский. Воронеж : Воронежский институт МВД России, 2021. 41 с.

2. *Гаврилин, Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практич. пособие. М. : Академия управления МВД России, 2021. 71 с.

3. *Гаврилин, Ю. В., Бедеров, И. С.* Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учеб. пособие. М. : Академия управления МВД России, 2022. 76 с.

4. *Гаврилин, Ю. В., Бедеров, И. С.* Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России : науч.-практич. журн. М. : Академия управления МВД России. 2021. № 4(60). С. 101–108.

5. *Вехов, В. Б., Васюков, В. Ф.* Получение компьютерной информации от организаторов ее распространения в сети Интернет при расследовании преступлений // Российский следователь : науч.-практич. журн. М. : ООО ИГ «Юрист». 2018. № 3. С. 11–15.

6. Особенности расследования дознавателями мошенничеств, совершенных с использованием электронных средств платежа : метод. рекомендации. М. : УОД МВД России ФГКУ «ВНИИ МВД России», 2021. 21 с.

7. *Гончар, В. В., Горач, Н. Н., Галиев, Д. В. Гусев, Д. В.* Направление запросов при расследовании уголовных дел о преступлениях, совершаемых с использованием IT-технологий: организации и располагаемые ими сведения : метод. рекомендации. М. : Следственный департамент МВД России, Московский университет МВД России им. В. Я. Кикотя, 2021. 44 с.

REFERENCES

1. *Gaidin, A. I., Pidusov, E. A., Golovchansky, A. V.* Osobennosti rassledovanija prestuplenij, sovershaemyh v seti Internet s ispol'zovaniem sredstv anonimizacii [Features of the investigation of crimes committed on the Internet using means of anonymization]. Voronezh, 2021, 41 p. (in Russian).

2. *Gavrilin, Yu. V.* O nauchnyh podhodah k probleme ispol'zovanija informacionno-telekommunikacionnyh tehnologij v prestupnyh celjah [On scientific approaches to the problem of using information and telecommunication technologies for criminal purposes: a scientific and practical guide]. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2021, 71 p. (in Russian).

3. *Gavrilin, Yu. V., Bederov, I. S.* Establishing the owners of cryptocurrency wallets in the investigation of crimes in the field of illicit drug trafficking. [Ustanovlenie vladel'cev kriptovaljutnyh koshel'kov pri rassledovanii prestuplenij v sfere nezakonnogo oborota narkoticheskih sredstv]. Moscow, 2022, 76 p. (in Russian).

4. *Gavrilin, Yu. V.* Establishing the identity of the owners of digital currency: methodological foundations [Ustanovlenie lichnosti vladel'cev cifrovoj valjuty: metodologicheskie osnovy]. Trudy Akademii upravlenija MVD Rossii – Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2021, no. 4(60), pp. 101-108. (in Russian).

5. *Vekhov, V. B., Vasyukov, V. F.* Poluchenie komp'juternoj informacii ot organizatorov ee rasprostranenija v seti Internet pri rassledovanii prestuplenij [Obtaining computer information from the organizers of its dissemination on the Internet during the investigation of crimes]. Rossijskij sledovatel' – Russian investigator. 2018, no. 3, pp. 11-15. (in Russian).

6. Methodological recommendations "Features of investigation by investigators of fraud committed using electronic means of payment" UOD of the Ministry of Internal Affairs of Russia FGKU "Research Institute of the Ministry of Internal Affairs of Russia", 2021, 21 p. (in Russian).

7. *Gonchar, V.V., Gorach, N.N., Galiev, D.V. Gusev, D.V.* Sbornik Napravlenie zaprosov pri rassledovanii ugolovnyh del o prestuplenijah, sovershaemyh s ispol'zovaniem IT-tehnologij: organizacii i raspolagaemye imi svedenija. [Collection. Sending requests in the investigation of criminal cases about crimes committed using IT technologies: organizations and the information they have]. Moscow, Sledstvennyj departament MVD Rossii, Moskovskij universitet MVD Rossii imeni V.Ja. Kikotja – Investigative Department of the Ministry of Internal Affairs of Russia. 2021, 44 p. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Гольцов Степан Евгеньевич, адъюнкт. Академия управления МВД России. 125171, Российская Федерация, г. Москва, ул. Зои и Александра Космодемьянских, 8.

INFORMATION ABOUT THE AUTHOR

Stepan E. Goltsov, postgraduate student. Academy of Management of the MIA of Russia. 8, st., Zoya and Alexander Kosmodemyanskikh, Moscow, Russian Federation, 125171.