Научная статья
УДК 343.9
https://doi.org/10.36511/2078-5356-2022-2-70-76

Типичные следственные ситуации и алгоритмы выявления незаконной банковской деятельности с помощью мониторинга интернет-ресурсов

Гармаев Юрий Петрович[1], Поляков Николай Владиславович[2]
[1]Восточно-Сибирский филиал Российского государственного университета правосудия, Иркутск, Россия, garmaeff1@mail.ru, https://orcid.org/0000-0001-5431-8063
[2]Сибирский юридический институт МВД России, Красноярск, Россия, polyakov.nikolay.1987@mail.ru, https://orcid.org/0000-0002-7966-5755

Аннотация. В статье констатируется, что незаконная банковская деятельность, совершаемая способами преступного обналичивания денежных средств, — это лишь звено в цепи целого ряда высокоорганизованных налоговых преступлений, мошенничества (преступного возмещение НДС и т. п.), отмывания «грязных» денег, коррупционных преступных посягательств и ряда других. Их выявление и расследование наиболее эффективно в типичных следственных ситуациях, складывающихся в процессе инициативного мониторинга интернет-ресурсов оперативными сотрудниками и следователями. В статье раскрываются 5 типичных следственных ситуаций такого рода и ряд алгоритмов идентификации, а значит и последующего изобличения исполнителей незаконного обналичивания. Анализируются возможности специализированных программных комплексов, позволяющих производить поиск и систематизацию информации из онлайн-источников. Резюмируется, что эффективность выявления, раскрытия и расследования анализируемых преступлений неразрывно связана с инициативным использованием следователями и оперативными сотрудниками современных информационных технологий.

Ключевые слова: незаконная банковская деятельность, незаконное обналичивание денежных средств, следственные ситуации, алгоритмы расследования, компьютерная криминалистика, выявление и расследование экономических преступлений
Для цитирования: Гармаев Ю. П., Поляков Н. В. Типичные следственные ситуации и алгоритмы выявления незаконной банковской деятельности с помощью мониторинга интернет-ресурсов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 2 (58). С. 70—76. https://doi.org/10.36511/2078-5356-2022-2-70-76.

Original article

Typical investigation situations and detection algorithms illegal banking with the help of monitoring internet resources

Yury P. Garmaev[1], Nikolay V. Polyakov[2]
[1]East Siberian Branch Russian state University of Justice, Irkutsk, Russian Federation, garmaeff1@mail.ru, https://orcid.org/0000-0001-5431-8063
[2]Siberian Law Institute of the Ministry of Internal Affairs of Russia, Krasnoyarsk, Russian Federation, polyakov.nikolay.1987@mail.ru, https://orcid.org/0000-0002-7966-5755

Abstract. The article states that illegal banking activity, committed by means of criminal cashing out of funds, is only a link in the chain of a number of highly organized tax crimes, fraud (criminal VAT refunds, etc.), laundering of “dirty” money, corruption criminal attacks and a number of others. Their identification and investigation is most effective in typical investigative situations that develop in the process of proactive monitoring of Internet resources by operational officers and investigators. The article reveals 5 typical investigative situations of this kind and a number of identification algorithms, and hence the subsequent exposure of the perpetrators of illegal cashing. For example, in an investigative situation,

when the subscriber number of the perpetrator of the criminal cashing out of funds was obtained during the monitoring of an Internet resource, the algorithm of the work of an operative officer should include an initiative search for personal data in instant messengers, the use of photo identification applications on the Internet, establishing an account in social networks and etc. The possibilities of specialized software systems that allow searching and systematizing information from online sources are analyzed. It is summarized that the efficiency of detecting, disclosing and investigating the analyzed crimes is inextricably linked with the proactive use of modern information technologies by investigators and operatives.

Keywords: illegal banking, illegal cashing out of funds, investigative situations, investigation algorithms, computer forensics, detection and investigation of economic crimes

For citation: Garmaev Y. P., Polyakov N. V. Typical investigation situations and detection algorithms illegal banking with the help of monitoring internet resources. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,*2022, no. 2 (58), pp. 70—76. (In Russ.). https://doi.org/10.36511/2078-5356-2022-2-70-76.

Незаконные обналичивание и транзитирование денежных средств сотрудники правоохранительных органов, как правило, квалифицируют по статье 172 УК РФ, которая предусматривает уголовную ответственность за незаконную банковскую деятельность. Такие преступные посягательства относятся к числу наиболее опасных экономических преступлений. Однако, как показали результаты специального исследования (здесь и далее в уточненном и дополненном виде приводятся выводы, которые изложил один из авторов в своей диссертации [1], научный руководитель — доктор юридических наук, профессор Ю. П. Гармаев), лишь в незначительном количестве уголовных дел выявляются и расследуются организованные формы этой преступной деятельности.

Между тем в действительности незаконное обналичивание и транзитирование денежных средств является, с одной стороны, самостоятельной преступной деятельностью, а с другой — может быть охарактеризовано как одно из звеньев целого ряда механизмов ее составляющих (уклонение от уплаты налогов и сборов, возмещение НДС с использованием мошеннических схем, вывоз капиталов за пределы Российской Федерации, отмывание денежных средств, коррупционные преступления). В результате подрывается экономическая безопасность нашей страны. Так, по данным Центрального банка Российской Федерации, в 2020 году объем незаконного обналичивания денежных средств составил 78 млрд рублей, объем незаконного транзитирования был определен в размере около 600 млрд рублей, из них примерно 52 млрд рублей было выведено в офшоры. Нельзя сказать, что наиболее опасные — организованные и коррумпированные — формы анализируемой преступной деятельности не выявляются, не расследуются совсем.

Ранее мы уже отмечали, что ключевым принципом расследования анализируемых преступлений должен быть принцип приоритета использования знаний цифровой криминалистики в выявлении, раскрытии и расследовании незаконного обналичивания и транзитирования денежных средств, сопутствующих им преступлений [1, с. 50, 138—140]. Согласимся с Е. П. Ищенко и Н. В. Кручининой, считающими, что термин «цифровая криминалистика» максимально полно отражает содержание особенностей расследования преступлений, совершаемых в сфере информационных и телекоммуникационных технологий [2, с. 742]. Многие ученые-криминалисты [3—6] говорят о необходимости использования современных технологий в раскрытии и расследовании преступлений, совершаемых в интернете.

«В настоящее время люди не только пользуются информацией в сети, они активно насыщают ей Всемирную паутину, зачастую оставляя в ней хронологию своей жизни (записи, фотографии, комментарии, документы и т. п.). И эта информация является общедоступной для всех, так как подчиняется изначальному принципу открытости, на котором и создавалась сеть Интернет» [7, с. 7].

Не являются исключением и участники незаконного обналичивания и транзитирования денежных средств, которые постоянно используют Всемирную паутину для совершения преступных посягательств. Результатом такой противоправной деятельности являются различные цифровые (виртуальные) следы. Они весьма эффективно могут использоваться в раскрытии и расследовании преступлений. Несмотря на это, только 1,9 % опрошенных оперативных сотрудников подразделений ЭБиПК МВД России назвали интернет в качестве источника получения необходимой информации.

Между тем для получения первичных сведений о противоправной деятельности оперативному сотруднику, следователю, как и любому иному лицу, достаточно войти в интернет, где через поисковые системы («Яндекс», «Google» и т. п.) можно легко найти сайты, сообщества, блоги, форумы и каналы, распространяющие информацию об оказании соответствующих услуг. При их мониторинге может быть получена ориентирующая криминалистически значимая информация, которая в дальнейшем будет способствовать выявлению и раскрытию преступления, а именно:

1) место преступной деятельности (город, субъект Российской Федерации);

2) данные исполнителя (имя/никнейм);

3) абонентские номера субъектов, имеющих отношение к противоправной деятельности организованных преступленных групп, организованных преступных сообществ (далее — ОПГ, ОПС). Речь идет об абонентских номерах, которые размещаются в сети для целей установления контактов с названными субъектами;

4) адрес электронной почты, которая используется при переписке, приеме и отправке документов;

5) данные расчетных счетов (банковских карт), которые используются для безналичных расчетов;

6) данные IP-адресов, с которых происходит авторизация.

При наличии указанной информации есть возможность установить исполнителей заказов на «обналичку» (далее — исполнители) при помощи современных информационных технологий, например, при помощи мобильных приложений и компьютерных программ открытого характера. Некоторые из обозначенных в настоящей статье мобильных приложений и компьютерных программ не являются лицензионными. Поэтому акцентируем внимание оперативных работников и следователей на потенциальной угрозе данным, хранящимся на их компьютерах и мобильных устройствах. Кроме того, информация, полученная таким образом, не должна нарушать прав человека и в дальнейшем в ходе расследования подлежит проверке и оценке в порядке, предусмотренном законом.

Далее рассмотрим алгоритмы идентификации исполнителей «обналички» исходя из типичных следственных ситуаций, складывающихся в процессе мониторинга интернет-ресурсов.

Следственная ситуация 1. При мониторинге интернет-ресурса, на котором размещается информация об оказании подобных услуг, получен абонентский номер исполнителя. В этой ситуации его можно установить с помощью следующих алгоритмов.

Алгоритм № 1. Оперативный сотрудник (следователь) добавляет абонентский номер исполнителя в качестве контакта в свой телефон. При этом иногда в мессенджерах (Telegram, Viber, WhatsApp и т. д.) можно получить его фото. Затем при помощи приложений и программ поиска по фотографии в интернете (например, «Поиск по фото», SearchFace, Tineye, Search4faces, FindmeVK, PhotoSherlock) иногда удается идентифицировать исполнителя, имеющего фотографии в социальных сетях («Одноклассники», «Вконтакте», Facebook (социальная сеть является продуктом компании «Meta», запрещенной в России), Twitter и т. д.) или отмеченного на фотографиях друзей.

При выявлении сотрудниками правоохранительных органов аккаунта исполнителя в той или иной социальной сети его следует детально изучить, проанализировать. Если страница открыта, зачастую можно сравнительно легко получить информацию, характеризующую личные данные исполнителя (ФИО, дата рождения, населенный пункт, где проживает субъект, место его учебы и/или работы, семейное положение, контактный номер телефона и т. д.). Дополнительную информацию об интересующем субъекте сотрудники правоохранительных органов могут получить, используя программы для наблюдения (например, для наблюдения за пользователями социальной сети «Вконтакте» можно использовать такие, как: vk-express.ru, 220vk.com, VK.FIT, «Шпион Вконтакте» и т. д.). С помощью таких программ может быть получена следующая информация (здесь и далее опять же при условии безусловного соблюдения требований Конституции РФ и иного законодательства, защищающего права человека и гражданина на тайну переписки, телефонных переговоров и т. п.): дата регистрации, а также дата рождения; числовой идентификатор пользователя (id); онлайн-активность; наличие общих, скрытых, закрытых и потенциальных друзей, места их проживания; наличие черного списка, субъектов, в него входящих; имеющиеся цепочки друзей между любыми пользователями; наличие пользователей с открытыми сохраненными фотографиями интересующего лица; наличие подписок; исходящие лайки; комментарии в группах и на стенах друзей, содержание таких комментариев; скрытые диалоги и информация о том, с кем исполнитель общается сейчас; наличие наблюдения за изучаемым субъектом со стороны иных лиц.

Описанный способ, как уже отмечалось, сравнительно легко позволяет получить информацию об исполнителе, лицах, с которыми он контактирует, содержании их общения, а также иные криминалистически значимые сведения.

Приведенные рекомендации достаточно успешно апробируются на практике. Как отмечает А. С. Шаталов, сотрудники Агентства финансовой и правовой безопасности при расследовании высокотехнологичных преступных посягательств наравне с использованием новейших информационных технологии занимаются анализом аккаунтов в социальных сетях (анализируя списки «друзей» на наличие общих признаков) [8].

Ю. В. Гаврилин и А. В. Шмонин обращают внимание на возможность использования и других (помимо вышеприведнных) алгоритмов получения и анализа информации в сети «Интернет» на основе специализированных программных комплексов, с помощью которых можно проводить поиск и систематизацию данных из онлайн-источников (социальные сети, форумы, блоги и т.п.), используя семантические фильтры. В качестве примеров авторы приводят программу «ЛКС Аналитика», а также программный комплекс «СПРУТ», которые способен устанавливать активных участников групп, выявлять их связи, определять потенциальных носителей информационных угроз, а также отношение пользователей к какой-либо теме, обсуждаемой в сети [9].

После получения сведений об исполнителе (ФИО, дата рождения) целесообразным видится установление иных его данных при помощи «интегрированного банка данных» МВД России (далее по тексту — ИБД). В нем аккумулируются разыскные, криминалистические и профилактические учеты Министерства внутренних дел России. С использованием названного банка данных можно получить следующую информацию:

а) место рождения;

б) выданные паспорта (российские, заграничные);

в) место регистрации;

г) зарегистрированные автотранспортные средства;

д) наличие судимости; привлечение за совершение административных правонарушений;

е) данные об абонентских номерах и проч.

Использование электронных сервисов, например, Федеральной налоговой службы России — «Сведения об ИНН физического лица» [10], «Прозрачный бизнес» [11] — позволяет получить информацию: о наличии зарегистрированных на исполнителя юридических лицах и ИП, их возможной аффиляции между собой и местонахождении; видах деятельности, что заявлены такими юридическими лицами и ИП; данные выписок из ЕГРЮЛ и ЕГРИП и т. д.

Некоторые из приведенных данных могут быть получены при использовании ИБД, вебресурса «fedresurs.ru» [12], а также и без применения каких-либо специальных программ путем использования обычных поисковиков — yandex, rambler и других. В ходе интервьюирования отдельные оперативные сотрудники подразделений ЭБиПК МВД России отметили, что целесообразно запрашивать из ФНС России сведения на начальной стадии проверки именно негласно. Такая рекомендация обусловлена тем, что у лиц, в отношении которых запрашиваются сведения, могут иметься коррупционные связи. Вышеназванные электронные ресурсы сети позволяют организовать получение такой информации в режиме реального времени, не направляя соответствующих запросов в ФНС России, что обеспечивает конспирацию.

Таким образом, получив ориентирующую информацию об исполнителях, можно заводить дело оперативного учета и проводить в отношении них негласные оперативно-разыскные мероприятия (далее — ОРМ), такие как: прослушивание телефонных переговоров, снятие информации с технических каналов связи, наблюдение. Кроме того, целесообразно направить запрос в Росфинмониторинг для проведения финансового расследования деятельности заподозренных. Как отмечают в рамках интервьюирования оперативные сотрудники ЭБиПК МВД России, реализация указанных оперативно-разыскных и иных действий позволяют без утечки информации выявить организации и лиц, причастных к совершению преступлений.

Алгоритм № 2. С помощью мобильных приложений и компьютерных программ определение владельцев абонентских номеров.

Зачастую абонентские номера оформляются на подставных лиц. Использование таких ресурсов, как numbuster.com, nomerzvonka.ru, beholder.pro, позволяет выявить реального владельца абонентского номера (исполнителя). С этой целью в приложение необходимо ввести интересующий сотрудников правоохранительных органов номер, после чего происходит поиск его владельца среди контактов других абонентов, пользующихся этими ресурсами.

Кроме того, целесообразно использовать некоторые Telegram-боты. Например, @getfb_bot

по абонентскому номеру позволяет получить ссылку на страницу интересующего субъекта-исполнителя в социальной сети Facebook (социальная сеть является продуктом компании «Meta», запрещенной в России).

Такие Telegram-боты, как @bmi_np_bot, @mnp_bot, способны по абонентскому номеру определить регион и оператора сотовой связи. Значимо, что боты могут искать новые и перенесенные абонентские номера тех или иных исполнителей от других операторов сотовой связи. С помощью сервиса smsc.ru/hlr можно определить доступность абонентов сотовой связи без совершения звонков.

А. А. Рудых описывает один из вероятных алгоритмов получения ориентирующей информации об исполнителе с помощью сервисов ДБО. «Используя смартфон с подключенной услугой мобильный банк, оперативный сотрудник либо следователь могут совершить попытки подачи команд о переводе денежных средств на номер телефона пользователя, личность которого подлежит установлению. Подавляющее большинство владельцев банковских карт используют абонентский номер для управления банковским счетом и получения информации о расходных операциях. Этот прием позволяет получить информацию о факте регистрации абонентского номера в качестве модуля управления счетом, имя и отчество владельца банковского счета, первую букву фамилии, последние цифры номера банковской карты» [13, с. 143].

После установления исполнителя проводится аналогичный поиск криминалистически значимой информации о нем. В дальнейшем реализуются ОРМ негласного характера, а после возбуждения уголовного дела производятся следственные и иные процессуальные действия.

Следственная ситуация 2. При мониторинге интернет-ресурса получены данные исполнителя (имя, никнейм, аккаунт в социальной сети).

При установлении никнейма исполнителя для его идентификации можно использовать Telegram-боты типа @buzzim_alerts_bot, которые производит поиск упоминаний о нем в чатах, статьях и каналах в мессенджере Telegram. Данному боту присуще оповещение, которое срабатывает в случае, если происходит опубликование информации в мессенджере пользователем с аналогичным никнеймом.

Кроме того, личность, интересующего правоохранительные органы исполнителя можно определить с помощью таких программ поиска по социальным сетям, как www.yandex.ru/people, knowem.com и т. д.

Следственная ситуация 3. При мониторинге интернет-ресурса получены сведения об электронной почте исполнителя.

Почтовый ящик исполнителя можно установить при помощи веб-ресурса pipl.com, который ищет аккаунты на разных сервисах по имени, электронной почте или телефону.

Веб-сервис emailsherlock.com может быть использован для получения данных о владельце интересующей электронной почты (например, имя, возможные другие адреса электронной почты, адрес владельца, номер его телефона, имеющиеся фотографии и/или видео, наличие скрытых социальных профилей, наличие судимости/привлечения к уголовной ответственности, сведения о семейном положении, публичные записи, информацию о домене и т. д.).

Чтобы получить информацию о том, на каких еще известных почтовых сервисах, порталах, сайтах знакомств зарегистрирован исполнитель, можно использовать электронные сервисы типа poiskmail.com, com.lullar.com. Отметим, что, как показал анализ следственной практики, предполагаемые преступники зачастую для удобства используют один и тот же логин и никнейм для работы на разных сайтах. Также можно посмотреть результат поисковой выдачи и узнать, где встречается интересующий логин или e-mail.

Следственная ситуация 4. При мониторинге интернет-ресурса получены реквизиты расчетных счетов (банковских карт) фирм-однодневок (ИП), исполнителей.

Информацию о владельце той или иной банковской карты вполне возможно получить с помощью веб-ресурсов «покупной.рф», psm7.com/bin-card, karta-banka.ru, card2.ru/bank_po_karte. Данные ресурсы определяют принадлежность карты к тому или иному государству и банку, ее тип и категорию. Это облегчает отыскание банка-эмитента, который обсуживает карту. После установления кредитной организации туда необходимо направить запрос для получения выписки по счету, а после ее получения тщательно проанализировать и выявить места снятия наличных исполнителем.

Вышеобозначенные ресурсы поиска по фото и видео в сети «Интернет» позволяют оптимизировать деятельность сотрудников правоохранительных органов по установлению исполнителя, производящего снятие или внесение средств в банкоматах и/или платежных терминалах. Особенно при своевременном истребовании видеозаписей у обслуживающих организаций.

В результате повышается эффективность проведения ОРМ негласного характера, следственных, иных процессуальных действий в отношении предполагаемого преступника.

Следственная ситуация 5. При мониторинге интернет-ресурса получены сведения об IP-адресах домена или компьютера, с которого происходила авторизация исполнителя.

Веб-ресурсы r-cy.ru/whois, www.nic.ru/whois, www.reg.ru/whois в случае ввода IP-адреса или наименования ресурса дают возможность получить информацию о домене. Речь идет о выявлении сетевого имени, информации о стране, городе, организации, адресе, телефоне, дате создания, последних изменениях и т. д. Такой Telegram-бот, как @RknBlockBot, позволяет оперативно проверить домен или IP-адрес на блокировку Роскомнадзором РФ. После этого целесообразно направить в адрес провайдера запрос о предоставлении сведений.

Ресурсы myip.ms, ip-lookup.net, www.threatcrowd.org, 2ip.ru позволяют определить IP-адреса интересующих компьютерных и мобильных устройств.

В некоторых ситуациях могут быть полезны ресурсы системы «Платон» [14], контролирующей движение транспортных средств массой более 12 тонн через системы ГЛОНАСС и GPS. Через операторов системы «Платон» можно получить данные о движении транспортных средств. Такие данные могут быть использованы для опровержения версий исполнителей и заказчиков относительно реальности оказания транспортных услуг или доставки товаров фирмами-однодневками (ИП).

«Программное обеспечение глобальной системы координат (GPS), встроенное в системы смартфонов и спутниковой навигации, может помочь отслеживать местонахождение подозреваемого» [15, с. 45].

Резюмируя, отметим, что выявление, раскрытие и расследование анализируемых преступлений неразрывно связаны с использованием современных информационных технологий, возможности которых позволяют достаточно эффективно решать целый ряд задач, поставленных перед правоохранительными органами.

Список источников

1. Поляков Н. В. Особенности методики расследования незаконного обналичивания и транзитирования денежных средств: дис. … канд. юрид. наук: Красноярск. 2021. 241 с.

2. Ищенко Е. П., Кручинина Н. В. Преступления, совершаемые с использованием высоких технологий // Всероссийский криминологический журнал. 2019. № 5. С. 740—746.

3. Варданян А. В., Никитина Е. В. Расследование преступлений в сфере высоких технологий и компьютерной информации: монография. М., 2007. 307 с.

4. Белькова А. В., Дяблова Ю. Л. Информационные технологии криминалистической регистрации и правовой статистики: современное состояние и тенденции развития // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 169—176.

5. Прорвич В. А. Интегрированные криминалистические знания как основа современных информационных технологий для расследования преступлений в сфере экономики // Уголовное судопроизводство: проблемы теории и практики. 2018. № 3. С. 63—66.

6. Россинская Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 109—117.

7. Молоков В. В., Галушин П. В., Тугаринов Н. В. Использование информационно-телекоммуникационных технологий в противодействии незаконному обороту наркотиков: учебно-практическое пособие. Красноярск: СибЮИ МВД России, 2018. 84 с.

8. Шаталов А. С. Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 77—78.

9. Гаврилин Ю. В., Шмонин А. В. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности // Труды Академии управления МВД России. 2019. № 1 (49). С. 108—109.

10. Электронный сервис «Узнать ИНН». URL: https://service.nalog.ru/inn.do (дата обращения: 05.05.2022).

11. Электронный сервис «Прозрачный бизнес». URL: https://pb.nalog.ru (дата обращения: 05.05.2022).

12. Единый федеральный реестр юридически значимых сведений о фактах деятельности юридических лиц, ИП и иных субъектов экономической деятельности. URL: http://www.fedresurs.ru (дата обращения: 05.05.2022).

13. Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Иркутск, 2019. 239 с.

14. Система взимания платы «Платон». URL: http://platon.ru/ru (дата обращения: 05.05.2022).

15. Мальцагов И. Д. Современные технологии в расследовании преступлений: компьютерная криминалистика // Экономика. Бизнес. Право. 2018. № 4-6 (26). С. 44—48.

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 2 (58)

References

1. Polyakov N. V. Features of the methodology for investigating illegal cashing and transit of funds. Dissertation... candidate of legal sciences. Krasnoyarsk. 2021. 241 p. (In Russ.)

2. Ishchenko E. P., Kruchinina N. V. Crimes committed with the use of high technologies. *All-Russian journal of criminology,* 2019, no. 5, pp. 740—746. (In Russ.)

3. Vardanyan A. V., Nikitina E. V. Investigation of crimes in the sphere of high technologies and computer information: monograph. Moscoiw, 2007. 307 p. (In Russ.)

4. Belkova A. V., Dyablova Yu. L. Information technologies of forensic registration and legal statistics: current state and development trends. *Bulletin of the Tula State University. Economic and legal sciences,* 2016, no. 3-2, pp. 169—176. (In Russ.)

5. Prorvich V. A. Integrated forensic knowledge as the basis of modern information technologies for investigating crimes in the economic sphere. *Criminal Justice: Problems of Theory and Practice,* 2018, no. 3, pp. 63—66. (In Russ.)

6. Rossinskaya E. R. To the question of the private theory of information and computer support for criminalistic activity. *News of the Tula State University. Economic and legal sciences,* 2016, no. 3-2, pp. 109—117. (In Russ.)

7. Molokov V. V., Galushin P. V., Tugarinov N. V. The use of information and telecommunication technologies in countering drug trafficking: educational and practical guide. Krasnoyarsk: SibUI of the Ministry of Internal Affairs of Russia Publ., 2018. 84 p. (In Russ.)

8. Shatalov A. S. Phenomenology of crimes committed with the use of modern information technologies. *Law. Journal of the Higher School of Economics,* 2018, no. 2, pp. 77—78. (In Russ.)

9. Gavrilin Yu. V., Shmonin A. V. The use of information obtained from the Internet in the investigation of extremist crimes. *Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia,* 2019, no. 1 (49), pp. 108—109. (In Russ.)

10. Electronic service “Find TIN”. URL: https://service.nalog.ru/inn.do (accessed 05.05.2022). (In Russ.)

11. Electronic service “Transparent business”. URL: https://pb.nalog.ru (accessed 05.05.2022). (In Russ.)

12. The unified federal register of legally significant information about the facts of the activities of legal entities, individual entrepreneurs and other economic entities. URL: http://www.fedresurs.ru (accessed 05.05.2022). (In Russ.)

13. Rudykh A. A. Information and technological support of forensic activities in the investigation of crimes in the field of information technology. Dissertation... candidate of legal sciences. Irkutsk, 2019. 239 p. (In Russ.)

14. Payment system “Platon”. URL: http://platon.ru/ru (accessed 05.05.2022). (In Russ.)

15. Maltsagov I. D. Modern technologies in the investigation of crimes: computer forensics. *Economics. Business. Right,* 2018, no. 4-6 (26), pp. 44—48. (In Russ.)

Информация об авторах

Ю. П. Гармаев — доктор юридических наук, профессор;
Н. В. Поляков — кандидат юридических наук.

Information about the authors

Y. P. Garmaev — Doctor of Law, Professor;
N. V. Polyakov — Candidate of Sciences (Law).

Статья поступила в редакцию 06.05.2022; одобрена после рецензирования 05.06.2022; принята к публикации 09.06.2022.

The article was submitted 06.05.2022; approved after reviewing 05.06.2022; accepted for publication 09.06.2022.