DOI https://doi.org/10.34216/1998-0817-2020-26-3-199-203
УДК 343.2

Павлюков Виталий Владимирович
Луганская академия внутренних дел им. Э.А. Дидоренко

ПРАКТИЧЕСКИЕ СПОСОБЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В данной статье освещены возможности практического использования потенциала оперативно-розыскного мероприятия «Получение компьютерной информации». На основании анализа судебной практики охарактеризован механизм фиксации результатов такого ОРМ. Доказана целесообразность более четкого законодательного закрепления процессуальных и процедурных аспектов получения компьютерной информации в целях противодействия компьютерной преступности. Научная новизна статьи заключается также в обосновании необходимости наделения полномочиями должностных лиц правоохранительных органов требовать у владельцев интернет-ресурсов или отдельных приложений данные о пользователе того или иного аккаунта в сети Интернет в целях его авторизации. Предлагается обязать провайдеров и операторов связи блокировать доступ к аккаунту или всему интернет-ресурсу соответствующего пользователя, если с такой рекомендацией к ним обратились правоохранительные органы. В рекомендации должно быть указано на факты противоправной деятельности пользователя, что должно подтверждаться скриншотом экрана компьютера, мобильного телефона или соответствующими материалами ОРМ.

Ключевые слова: *оперативно-розыскное мероприятие, получение компьютерной информации, результаты оперативно-розыскной деятельности.*

Информация об авторе: Павлюков Виталий Владимирович, ORCID https://orcid.org/0000-0002-2860-2156, старший преподаватель кафедры экономико-правовых и социально-гуманитарных дисциплин, Луганская академия внутренних дел им. Э.А. Дидоренко, г. Луганск.
E-mail: ykc@mail.ru

Дата поступления статьи: 29.06.2020.
Для цитирования: Павлюков В.В. Практические способы получения и использования результатов оперативно-розыскного мероприятия «Получение компьютерной информации» // Вестник Костромского государственного университета. 2020. Т. 26, № 3. С. 199-203. DOI https://doi.org/10.34216/1998-0817-2020-26-3-199-203.

Vitaliy V. Pavlyukov
Didorenko Lugansk Academy of Internal Affairs

PRACTICAL METHODS OF OBTAINING AND USING THE RESULTS OF THE OPERATIONAL-SEARCH EVENT “OBTAINING COMPUTER INFORMATION”

This article highlights the possibilities of practical use of the potential of the operational search event «Obtaining computer information». Based on the analysis of judicial practice, the mechanism for fixing the results of such an operational search event is described. The expediency of a clearer legislative consolidation of procedural and procedural aspects of obtaining computer information in order to counter computer crime is proved. The scientific novelty of the article also lies in the justification of the need to empower law enforcement officials to demand from the owners of the Internet resources or individual applications data about the user of a particular account on the Internet in order to authorise it. It is proposed to oblige providers and Telecom operators to block access to the account or the entire Internet resource of the corresponding user, should the law enforcement agencies contact them with such a recommendation. The recommendation should indicate the facts of illegal activity of the user, which should be confirmed by a screenshot of the computer screen, mobile phone or relevant materials of the operational search event.

Keywords: *operational-search measures, obtaining computer information, results of operational-search activities.*

Information about the author: Vitaliy V. Pavlyukov, ORCID https://orcid.org/0000-0002-2860-2156, Senior Lecturer, Department of Economic, Legal and Social and Humanitarian Disciplines, Didorenko Lugansk Academy of Internal Affairs, Lugansk.
E-mail: ykc@mail.ru

Article received: June 29, 2020.
For citation: Pavlyukov V.V. Practical methods of obtaining and using the results of the operational-search event “Obtaining computer information”. Vestnik of Kostroma State University, 2020, vol. 26, № 3, pp. 199-203 (In Russ.). DOI https://doi.org/10.34216/1998-0817-2020-26-3-199-203.

Роль компьютерной информации в обществе возрастает с каждым годом. Сегодня любой доступный информационный ресурс помимо его развития нуждается в защите, безопасном использовании и контроле на государственном уровне. Автоматизация информации при помощи компьютерных технологий и ее передача посредством сети Интернет превращает такую информацию не только в социально полезный инструмент, но и средство совершения противоправных деяний.

Данные, зафиксированные в статистическом сборнике Генеральной прокуратуры РФ, указывают на существенный рост преступности в сфере компьютерной информации за последние годы. Так в 2016 году было совершено 65 949 преступлений, в 2017 году – 90 587, в 2018 – 174 674, в 2019 – 294 409. Примечательно также и то, что за 2019 год предварительно расследовано всего 65 238 преступных деяний указанной направленности[1].

На наш взгляд, это связано с тем, что на первый план выходит защита компьютерной информации, а именно обеспечение безопасного доступа к ней, создание условий для ее надежного хранения и передачи. С этой целью разработчики программного обеспечения постоянно выпускают различные обновления, устраняют имеющиеся уязвимости и предлагают механизмы защиты доступа к компьютерной информации. Каждая уважающая себя компания разрабатывает собственные алгоритмы шифрования и защиты данных, которые даже при наличии законных требований не всегда предоставляются сотрудникам правоохранительных органов. Все это только на руку лицам, склонным к занятию противоправной деятельностью при помощи компьютерных технологий.

А.С. Александин и С.И. Захарцев правомерно обращают внимание на то, что в компьютерах нередко содержатся сведения, доказывающие преступный характер конкретных лиц [Александин, Захарцев: 147], однако вопрос о том, как получить и процессуально оформить такие сведения, сегодня остается пока что неразрешенным.

Следует отметить, что в целях обеспечения доступа правоохранительных органов России к компьютерной информации, содержащей признаки противоправного характера, законодатель предпринимает определенные шаги. Так, например, ФЗ «Об оперативно-розыскной деятельности» был дополнен таким оперативно-розыскным мероприятием, как «Получение компьютерной информации» (далее – ОРМ ПКИ). По мнению руководства ФСБ России, последнее должно проводиться по решению суда соответствующими оперативно-техническими подразделениями и обеспечивать возможность копирования компьютерной информации, ее изъятие с жестких дисков сетевых компьютеров или серверов в информационно-телекоммуникационной сети Интернет, в том числе из «облачных» хранилищ. То есть такое ОРМ должно позволять получать оперативно значимую информацию путем удаленного доступа к компьютеру или серверу в сети Интернет [Баженов: 31].

Понимая важность ОРМ ПКИ в борьбе с преступностью в сфере компьютерной информации, ученые тоже обратили внимание на него и указали, что одним из общих признаков, характерных для проведения данного ОРМ, должна являться фиксация сведений, хранящихся на компьютерах, различных носителях машинной информации [Сенатов, Плужников: 31]. В то же время отдельные авторы отмечают, что любой способ получения компьютерной информации в ходе ОРД может рассматриваться как ОРМ ПКИ [Бакланов: 40]. Однако при детальном изучении открытой судебной практики нами была выявлена несколько иная ситуация, которая указывает на то, что результаты ОРМ ПКИ могут получаться путем:

1) мониторинга и фиксации компьютерной информации в социальных сетях[2], досках объявлений[3], специализированных (созданных для осуществления противоправной деятельности) сайтах[4];

2) физического осмотра содержимого различных компьютерных устройств, в первую очередь мобильных телефонов[5], где информация была получена в папке «Галерея» (видео и фотографии)[6], в папке «Диктофон» (аудиозаписи)[7];

3) получения от пользователя логина и пароля к программному обеспечению (мессенджеры Telegram[8], WhatsApp[9]), используемых для осуществления противоправной деятельности.

Известно, что доступ к программному обеспечению и к компьютерному устройству правонарушителя может быть закрыт им парольной защитой, в силу чего следователю приходится принимать решение об изъятии мобильного телефона и направлении его на компьютерно-техническую экспертизу. Вместе с тем практика отдельных судебных дел показывает, что обозначенная проблема может непосредственно разрешаться и сотрудниками оперативных подразделений. В частности, из справки по результатам проведения ОРМ «Получение компьютерной информации», которая зафиксирована в приговоре Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-244/2017 от 17 ноября 2017 г. по делу № 1-244/2017, видно, что у подозреваемого был изъят мобильный телефон, который мог содержать оперативно значимую информацию для расследования преступления. В частности, для выяснения данного факта оперативники при помощи мобильного телефона осуществили вход на сайт путем внесения полученных от подозреваемого данных в поле «имя» и «пароль». Так была получена компьютерная информация личного кабинета правонарушителя[5].

В соответствии с положениями п. 36.1 ст. 5 УПК РФ сведения, полученные в ходе ОРД, в том числе при проведении ОРМ ПКИ, носят название «результаты оперативно-розыскной деятельности»[10], порядок фиксации которых должен соответствовать определенным требованиям. Так, фиксация результатов ОРМ ПКИ зачастую заключается в снимке экрана смартфона или монитора компьютера (скриншоте)[11], который оперативный сотрудник прикрепляет к рапорту, протоколу или акту. Стоит указать, что скриншоты могут быть сделаны при помощи одновременного нажатия на клавиатуре клавиш Ctrl+Print Screen, после чего скриншот сохраняется в памяти компьютера. На мобильном телефоне также возможно сделать скриншот. В зависимости от марки телефона скриншот делается по-разному. Зачастую это нажатие нескольких клавиш, например, на мобильном телефоне фирмы Apple – одновременное нажатие кнопок «Домой» и «Питание». Сделанный снимок можно вставить как в графический редактор (Paint), так и в текстовый (Word), после чего полученный результат распечатать.

Судебная практика свидетельствует также и о том, что суды принимают скриншоты в качестве надлежащих доказательств, однако для использования их в этом качестве к ним должны предъявляться определенные требования, которые отражены в письме Федеральной налоговой службы от 31.03.2016 г. № СА-4-7/5589 «О понятии “скриншот”», а именно:

– на скриншоте необходимо проставить дату и время получения информации с сайта в сети Интернет;

– указать наименование сайта (полный URL-адрес интернет-страницы, с которой сделан скриншот);

– скриншот должен содержать данные о лице, которое произвело его выведение на экран и дальнейшую распечатку, а также сведения о программном обеспечении и об использованной компьютерной технике[12]. Фиксация скриншота, как и других результатов ОРД, регламентируется «Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд», где в п. 6 сказано, что результаты, полученные в ходе проведения ОРД, должны быть представлены в виде рапорта об обнаружении признаков преступления или сообщения о результатах оперативно-розыскной деятельности. Также в п. 16 Инструкции указано, что к рапорту могут прилагаться (при наличии) полученные (выполненные) при проведении ОРМ материалы фото- и киносъемки, аудио- и видеозаписи, иные носители информации и материальные объекты[13]. Считаем, что такими носителями информации могут быть, например, скриншоты, сделанные в ходе проведения ОРМ ПКИ. Последние необходимо признать полноценным доказательством, прописав соответствующие требования в п. 16 Инструкции.

Что касается удаленного доступа, то далеко не все владельцы интернет-ресурсов охотно идут на предоставление ответов на запросы правоохранительных органов РФ, не говоря уже о предоставлении удаленного доступа к «облачным» хранилищам. Так, в частности, компания Google с 2011 года начала публиковать статистику запросов правоохранительных органов касательно пользовательских данных со всего мира, где при определенных сортировках можно увидеть не только количество запросов к Google, но и процент одобренных ответов. Например, за июль – декабрь 2019 года компания Google одобрила всего 23 % запросов от правоохранительных органов РФ и 83 % – от правоохранительных органов США. Примечательно, что 23 % – это самый большой процент одобренных запросов от РФ за последнее время и, судя по статистике за предыдущие годы, процент таких запросов составлял от 5 до 15[14].

Подобная ситуация складывается и с отечественными интернет-компаниями. Например, поисковая компания «Яндекс» вообще отказалась предоставлять ФСБ ключи шифрования от «Яндекс.Почта» и «Яндекс.Диск», причем чуть ранее так же поступил и владелец мессенджера Telegram[15].

Как видим, в практике противодействия преступности по определенным причинам складывается такая ситуация, которая не соответствует идее получения удаленного доступа к данным. Она зачастую сводится только лишь к получению скриншотов информации с экрана монитора компьютера или же с мобильного телефона. Считаем, что указанная ситуация возникает по той причине, что законодатель и, следовательно, сами владельцы компьютерной информации ограничили возможности доступа к тем данным, которые указаны в запросе от сотрудника правоохранительных органов, при этом существенно ограничив эти действия необходимостью судебного решения.

Можно ли найти оптимальный вариант разрешения вышеуказанной проблемы? На наш взгляд, конечно же, можно, однако для этой цели необходимо будет в ст. 6 ФЗ «Об оперативно-розыскной деятельности» отдельным пунктом прописать, что «в ходе проведения оперативно-розыскного мероприятия “Получение компьютерной информации”, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, владелец интернет-ресурса или отдельного приложения обязан предоставлять данные для авторизации интересующего правоохранительные органы пользователя от его аккаунта в сети Интернет или приложения. В случае, если такие требования не будут выполнены, то на основании мотивированного постанов-

ления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, может быть затребовано от провайдеров и операторов связи заблокировать доступ к аккаунту или всему интернет-ресурсу, если есть основания полагать, что при помощи последнего осуществляется противоправная деятельность или в нем хранится информация, представляющая оперативный интерес, что должно подтверждаться скриншотом или материалами ОРМ».

Примечание

[1] Состояние преступности в России. URL: https://genproc.gov.ru/ (дата обращения: 25.06.2020).

[2] Постановление Карачаевского районного суда (Карачаево-Черкесская Республика) № 5-4/2019 от 15 января 2019 г. по делу № 5-4/2019. URL: https://sudact.ru/regular/doc/T5Do8RqhwAdO/ (дата обращения: 09.06.2020).

[3] Решение Абинского районного суд (Краснодарский край) № 12-40/2018 от 25 мая 2018 г. по делу № 12-40/2018. URL: https://sudact.ru/regular/doc/6YL6sesUHsHt/ (дата обращения: 09.06.2020).

[4] Приговор Приморского районного суда г. Новороссийска (Краснодарский край) № 1-16/2019 1-360/2018 от 9 января 2019 г. по делу № 1-16/2019. URL: https://sudact.ru/regular/doc/5FEHQ1WqirLl/ (дата обращения: 11.06.2020).

[5] Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-244/2017 от 17 ноября 2017 г. по делу № 1-244/2017. URL: https://sudact.ru/regular/doc/QODcLxpWm5dr/ (дата обращения: 11.06.2020).

[6] Приговор Приморского районного суда г. Новороссийска № 1-458/2017 1-63/2018 от 2 февраля 2018 г. по делу № 1-458/2017. URL: https://sudact.ru/regular/doc/gaRcTHh7C6dC/ (дата обращения: 10.06.2020).

[7] Приговор Приморского районного суда г. Новороссийска № 1-130/2017 от 17 мая 2017 г. по делу № 1-130/2017. URL: https://sudact.ru/regular/doc/GPSNpiTKsHYB/ (дата обращения: 10.06.2020).

[8] Приговор Лесосибирского городского суда № 1-275/2018 от 18 октября 2018 г. по делу № 1-275/2018. URL: https://sudact.ru/regular/doc/YXnsYURSnoJL/ (дата обращения: 11.06.2020).

[9] Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-164/2017 от 18 августа 2017 г. по делу № 1-164/2017. URL: https://sudact.ru/regular/doc/TweV9tbuut5Z/ (дата обращения: 11.06.2020).

[10] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 24.04.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 30.04.2019).

[11] Постановление Анапского городского суда (Краснодарский край) № 5-3613/2018 от 2 ноября 2018 г. по делу № 5-3613/2018. URL: https://sudact.ru/regular/doc/iD75SkvOV7by/ (дата обращения: 11.06.2020).

[12] Письмо Федеральной налоговой службы от 31 марта 2016 г. № СА-4-7/5589 О понятии «скриншот» («снимок экрана») и порядке его использования. URL: https://www.garant.ru/products/ipo/prime/doc/71284846/ (дата обращения: 05.01.2020).

[13] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013. URL: http://www.consultant.ru/document/cons_doc_LAW_155629/ (дата обращения: 19.04.2018).

[14] Запросы пользовательских данных со всего мира. URL: https://transparencyreport.google.com/user-data/overview?hl=ru (дата обращения: 24.06.2020).

[15] ФСБ потребовала ключи шифрования переписки пользователей у «Яндекса». За отказ их предоставить год назад был заблокирован Telegram. URL: https://www.rbc.ru/technology_and_media/04/06/2019/5cf50e139a79474f8ab5494b (дата обращения: 24.06.2020).

Список литературы

Алексанин А.С., Захарцев С.И. Введено новое оперативно-розыскное мероприятие: «Получение компьютерной информации» // Мир политики и социологии. 2019. № 5. С. 145–149.

Бакланов Л.А. Получение компьютерной информации в оперативно-розыскной деятельности // Научный вестник Омской академии МВД России. 2020. № 1 (76). С. 37–42.

Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. 2017. № 2 (65). С. 31–33.

Сенатов А.В., Плужников М.И. Проведение оперативно-розыскного мероприятия «Получение компьютерной информации»: понятие и особенности // Пенитенциарное право: юридическая теория и правоприменительная практика. 2019. № 2 (20). С. 59–63.

References

Aleksanin A.S., Zakhartsev S.I. *Vvedeno novoe operativno-rozysknoe meropriiatie: "Poluchenie komp'iuternoi informatsii"* [A new operational-search measure has been introduced: "Obtaining computer information"]. *Mir politiki i sotsiologii* [World of Politics and Sociology], 2019, № 5, pp. 145–149. (In Russ.)

Baklanov L.A. *Poluchenie komp'iuternoi informatsii v operativno-rozysknoi deiatel'nosti*

[Obtaining computer information in operational-search activity]. *Nauchnyi vestnik Omskoi akademii MVD Rossii* [Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia], 2020, № 1 (76), pp. 37–42. (In Russ.)

Bazhenov S.V. *Operativno-rozysknoe meropriiatie "Poluchenie komp'iuternoi informatsii"* [Operational-search action "Obtaining computer information"]. *Nauchnyi vestnik Omskoi akademii MVD Rossii* [Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia], 2017, № 2 (65), pp. 31–33. (In Russ.)

Senatov A.V., Pluzhnikov M.I. *Provedenie operativno-rozysknogo meropriiatiia "Poluchenie komp'iuternoi informatsii": poniatie i osobennosti* [Conducting an operational-search activity "Obtaining computer information": concept and features]. *Penitentsiarnoe pravo: iuridicheskaia teoriia i pravoprimenitel'naia praktika* [Penitentiary law: legal theory and law enforcement practice], 2019, № 2 (20), pp. 59–63. (In Russ.)