УДК 343.1

Вспомогательные возможности ОРМ «Получение компьютерной информации» в уголовно-процессуальном аспекте

Борисов Денис Вадимович

Старший лейтенант полиции,
оперуполномоченный ОЭБиПК УМВД России по ЗАТО Северск Томской области;
адъюнкт,
Нижегородская академия Министерства внутренних дел Российской Федерации,
603950, Российская Федерация, Нижний Новгород, Анкудиновское шоссе, 3;
e-mail: starig@sibmail.com

Аннотация

В данной статье рассматриваются вопросы, связанные с использованием ОРМ «Получение компьютерной информации» в качестве одного из предполагаемых важнейших аспектов доказательства при расследовании уголовных дел экономической и общеуголовной направленности. Анализируются преимущества применения данного ОРМ перед другими ОРМ и следственными действиями, а также раскрывается суть его назначения, прорабатываются основы его практического осуществления и роли в качестве предполагаемого самостоятельного доказательства, закрепленного в действующем уголовно-процессуальном законодательстве. Исследуются действующие законодательные нормы, регламентирующие проведение ОРМ и следственных дейтствий по получению компьютерной информации. Дополнительно в статье описываются полномочия сотрудников оперативных подразделений и сотрудников органов предварительного следствия при осуществлении мероприятий (действий), направленных на получение и закрепление в качестве доказательств электронной информации.

Для цитирования в научных исследованиях

Борисов Д.В. Вспомогательные возможности ОРМ «Получение компьютерной информации» в уголовно-процессуальном аспекте // Вопросы российского и международного права. 2018. Том 8. № 6А. С. 71-77.

Ключевые слова

Доказательства, ОРМ «Получение компьютерной информации», обыск, выемка, электронные носители.

Введение

Создание ЭВМ, в том числе компьютерной техники (планшетов, ноутбуков, нетбуков, смартфонов), а также электронно-переносных устройств (флешек, жестких дисков), иначе говоря, электронных носителей, можно назвать одним из главных технических рывков современности. Вышеуказанные устройства прежде всего предоставили большой спектр возможностей для получения, обработки (оценки) и передачи информации. Количество пользователей компьютерной техникой в мире с каждым часом растет, хоть и прошло менее 70 лет, так как первый компьютер был создан американской фирмой NCR в 1957 г.

Однако сфера компьютерных технологии и электронной информации не всегда имеет только учебный или развлекательный характер, иногда она служит способом совершения преступления, количество которых с каждым годом все возрастает, о чем может свидетельствовать дополнение главы 28 УК РФ «Преступления в сфере компьютерной информации» (ст.ст. 272-274) статьей «Мошенничество в сфере компьютерной информации» (введена Федеральным законом от 29 ноября 2012 г. № 207-ФЗ). Очень часто по уголовным делам экономической направленности органам предварительного расследования приходиться иметь дело с доказательствами, имеющими электронную направленность, в том числе и электронной перепиской, ведь не секрет, что в настоящее время электронная переписка набирает все больший оборот и постепенно заменяет консервативный вид общения, а именно «бумажный». Электронная переписка происходит с помощью смс- и ммс-сообщений, электронной почты, мессенджеров (Skype, Viber, WhatsApp, Jabber, ICQ) и социальных сетей (Одноклассники, ВКонтакте, Instagram).

В правовой же сфере компьютерная информация и компьютерные технологии находятся на начальной стадии регламентации, до сих пор нет четкого единообразного определения компьютерной информации. Существует множество определений понятия «компьютерная информация» как в социальной сети «Интернет», так и в напечатанных периодических изданиях, монографиях, авторефератах и диссертациях, кодексах.

Определение понятия «компьютерная информация» в юриспруденции

Так, в соответствии с «Соглашением о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», заключенным в г. Минске 1 июня 2001 г., под компьютерной информацией понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи. Согласно примечанию к ст. 272 УК РФ, компьютерная информация – это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В.Б. Вехов предложил понятие «компьютерная информация» рассматривать как «сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо переданные по каналам связи посредством электромагнитных сигналов» [Вехов, 2008, 71].

О.С. Кучин компьютерную информацию рассматривает как информацию коллективного пользования, доступную к использованию неопределенным числом пользователей. Характерные черты компьютерной информации допускают преобразование данной

информации из одной объективной формы реальности в другую форму, включая передачу указанной информации на значительные расстояния, что обеспечивается современными средствами связи [Кучин, 2017, 32-33].

Однако, по нашему мнению, наиболее полное и универсальное определение нового ОРМ отразили в своей статье А.Ф. Мицкевич и А.В. Суслопаров: под компьютерной информацией нужно понимать не какой-то особый вид информации, а специфическую форму ее представления, приспособленную для обработки в компьютерных устройствах, передачи по каналам связи и хранения на специализированных носителях [Мицкевич, Суслопаров, 2010].

Естественно, законодатель реагирует на появление новых способов (использование информационно-телекоммуникационных сетей) совершения преступления и вносит в УК РФ квалифицирующее обстоятельство в такие статьи, как 171.2, 185.3, 228.1, 242, 242.1, 242.2, 137, 146, 159.6, 183.

Использование компьютерной информации в качестве доказательства по уголовным делам

Остроугольным моментом включения компьютерной информации в уголовный процесс является возможность ее использования в качестве доказательства по уголовным делам. Остается вопрос: каким образом получить компьютерную информацию и приобщить ее к материалу проверки или уголовному делу, чтобы ее можно было рассматривать как доказательство способа совершения преступления?

При наличии возбужденного уголовного дела ответом на вышеуказанный вопрос будет являться самый простой и логичный способ процессуального получения содержащейся в компьютере информации как источника доказательства – осуществление выемки в соответствии со ст. 183 УПК РФ (в данном случае – электронного носителя). Проводить данное следственное действие необходимо на основании судебного решения в соответствии со ст. 165 УПК РФ, так как на электронном носителе могут содержаться персональные данные граждан, а также информация о вкладах и счетах граждан и организаций.

Дополнительно рамками УПК РФ регламентированы положения, при которых в выемке электронных носителей информации обязательно должны участвовать специалист в области компьютерных технологий (ч. 3.1 ст. 183 УПК РФ) и не менее двух понятых (ч. 1 ст. 170 УПК РФ). Также в рамках данного следственного действия законный владелец изымаемого электронного носителя имеет право заявить ходатайство о копировании информации с изымаемого электронного носителя на другие электронные носители. Таким образом, как мы видим, сторона, у которой изымается тот или иной электронный носитель, в должной мере защищена: во-первых, следователю необходимо наличие возбужденного уголовного дела, о чем он заранее обязан уведомить лицо, которое является подозреваемым, что предоставляет последнем фору в маневрировании и сокрытии того или иного доказательства, если уголовное дело возбужденно не по «факту»; во-вторых, получение судебной санкции на проведение данного следственного действия и вручение копии лицу, у которого изымается электронный носитель, также занимают определенное время; в-третьих, подозреваемый имеет возможность скопировать информацию, которая изымается, что позволит в дальнейшем в рамках судебных прений занять более устойчивую позицию и сыграть на вполне ожидаемых доводах следователя с учетом изученной в рамках изъятия информации.

Проведение такого следственного действия, как осмотр места происшествия для целей, указанных выше, по нашему мнению, является весьма некорректным и неэффективным, а также рискованным для стороны обвинения ввиду раскрытия истинных целей проводимого следственного действия. Во-первых, как мы указывали ранее, на изымаемом электронном носителе может содержаться информация, подпадающая под принципы обеспечения конституционных прав граждан, тогда изъятый в рамках осмотра места происшествия и приобщенный к уголовному делу в качестве доказательства электронный носитель в дальнейшем может быть признан недопустимым ввиду отсутствия судебного решения на изымаемый предмет. Во-вторых, проводя осмотр места происшествия, мы завуалированно, но все же определяем спектр нашей заинтересованности, тем самым раскрывая карты.

Есть и иной способ получения доказательств в виде компьютерной информации, проводимый оперативным аппаратом в рамках гласного ОРМ «Обследование помещений, зданий, сооружений, участков местности и транспортных средств», предусмотренного п. 8 ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Также проведение ОРМ регламентировано п. 10 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции», где указывается, что сотрудники полиции имеют право производить при осуществлении оперативно-розыскной деятельности изъятие документов, предметов, материалов и сообщений.

Однако при проведении данного ОРМ мы также, во-первых, ставим под угрозу истинную цель проводимого мероприятия, так как необходимо предоставить лицу, в отношении которого проводится ОРМ, распоряжение, подписанное руководителем УМВД, в котором указывается, на основании чего и в чем подозревается лицо, в отношении которого проводятся проверочные мероприятия, во-вторых, без получения судебной санкции рискуем получить доказательства, которые судебные органы в дальнейшем признают недопустимыми ввиду возможного наличия на электронном носителе персональных данных проверяемого лица. Во всех вышеперечисленных случаях результатом подобных ситуаций зачастую являлась потеря доказательств, что негативно сказывалось на всем процессе расследования. В связи с этим, по нашему мнению, Федеральным законом от 6 июля 2016 г. № 374-ФЗ было внесено изменение в Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», а именно – к имеющимся 14 ОРМ добавлено новое – получение компьютерной информации (ст. 6). В указанной статье делается акцент на том, что ОРМ, связанные с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов ФСБ и ОВД, тем самым определяется, что именно внутренний специалист участвует в проводимых мероприятиях, что снижает такое явление, как утечка информации.

Также важно отметить то, что для проведения ОРМ «Получение компьютерной информации» необходимо наличие судебной санкции, так как полученная в рамках ОРМ информация может касаться ограничения конституционных прав граждан, однако, в отличие от вышеуказанных случаев, при получения судебного решения на проведение ОРМ «Получение компьютерной информации» никто не уведомляется и не ознакамливается с судебной санкцией, лицу, в отношении которого проводятся мероприятия, не вручают копию судебного решения, что также имеет, на наш взгляд, положительный аспект.

Данный способ получения информации носит негласный характер и реализуется втайне от лица, которое использует тот или иной электронный носитель при совершении преступных деяний. Проведение данного мероприятия возможно как в рамках мероприятий, предусмотренных Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-

розыскной деятельности», так и в рамках поступившего поручения следователя по уголовному делу. Уголовно-процессуальные права следователя на дачу поручений закреплены в п. 11 ч. 2 ст. 37, п. 4 ч. 2 ст. 38 УПК РФ.

Заключение

Полученные результаты ОРМ помогут правоохранительным органам иметь скрытые от подозреваемого лица сведения о том, каким образом лицо совершает преступление, о наличии и количестве соучастников, способствующих совершению лицом преступления, а также более подготовленно строить линию нападения в судебных прениях и не оказаться в спектре рисков превращения добытых на досудебной стадии доказательств в недопустимые в рамках судебного следствия и прения, вследствие чего, на наш взгляд, проведение именно ОРМ «Получение компьютерной информации» для собирания электронных сведений является вспомогательные способом закрепления доказательств в уголовно-процессуальном аспекте, а также относится к наиболее защищенным со стороны обвинения способам собирания компьютерной информации. В связи с этим, по нашему мнению, необходимо внести изменения в действующее уголовно-процессуальное законодательство по вопросу закрепеления результатов ОРМ «Получение компьютерной информации» в качестве самостоятельного доказательства.

Библиография

1. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград: ВА МВД России, 2008. 408 с.
2. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. … канд. юрид. наук. М., 1997. 215 с.
3. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/
4. Кучерук Д.С. К вопросу об использовании в доказывании результатов гласных оперативно-розыскных мероприятий // Баранов В.М., Пшеничнов М.А. (ред.) Проблемы юридической науки в исследованиях докторантов, адъюнктов и соискателей. Нижний Новгород, 2009. Вып. 15. С. 48-51.
5. Кучин О.С. (ред.) Электронные носители информации в криминалистике. М.: Юрлитинформ, 2017. 304 с.
6. Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. 2010. № 2. С. 206-209.
7. О внесение изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российский Федерации: федер. закон Рос. Федерации от 29.11.2012 № 207-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 23.11.2012: одобр. Советом Федерации Федер. Собр. Рос. Федерации 28.11.2012. URL: http://www.consultant.ru/document/cons_doc_LAW_138322/
8. О полиции: федер. закон Рос. Федерации от 07.02.2011 № 3-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 28.01.2011: одобр. Советом Федерации Федер. Собр. Рос. Федерации 02.02.2011. URL: http://www.consultant.ru/document/cons_doc_LAW_110165/
9. Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12.08.1995 № 144-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 05.07.1995. URL: http://www.consultant.ru/document/cons_doc_LAW_7519/
10. Плахотнюк Ю.И. Взаимодействие органов предварительного следствия с оперативным и другими подразделениями при расследовании уголовных дел по преступлениям против семьи и несовершеннолетних // Материалы II международной научной конференции «Государство и право: теория и практика». Чита, 2013. URL: https://moluch.ru/conf/law/archive/83/3340/
11. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22.11.2001: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.12.2001. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/
12. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24.05.1996: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.06.1996. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

Additional capacities of the operational-search activity "Obtaining computer information" from the criminal procedural aspect

Denis V. Borisov

Police Senior Lieutenant,
Detective at the Department of economic security and counteraction to corruption of the Directorate of the Ministry of Internal Affairs of the Russian Federation in Seversk of the Tomsk region;
Postgraduate,
Nizhny Novgorod Academy of the Ministry of Internal Affairs of the Russian Federation,
603950, 3 Ankudinovskoe highway, Nizhny Novgorod, Russian Federation;
e-mail: starig@sibmail.com

Abstract

This article discusses issues related to the use of the operational-search activity "Obtaining computer information" as one of the most important types of evidence in the investigation of economic and general criminal cases. It analyses the advantages of using this operational-search activity over other operational-search activities and investigative actions, identifies the fundamentals of its practical implementation and role as prospective independent evidence, stipulated in the current legislation on criminal procedure. The author examines the powers of employees working in operational units and preliminary investigation bodies when they carry out activities (actions) aimed at obtaining and fixing electronic information as evidence. The results of the operational-search activity "Obtaining computer information" will help law enforcement agencies to obtain information about how a crime was committed, about the presence and number of accomplices without informing suspects, as well as to prepare for the court debate and ensure that the evidence, obtained as a result of operational-search activities, will not be viewed as inadmissible by the court. The author points out that carrying out the operational-search activity "Obtaining computer information" with a view to collecting electronic information is an additional way of gathering evidence in criminal procedure and also belongs to the most protected methods used for collecting computer information.

For citation

Borisov D.V. (2018) Vspomogatel'nye vozmozhnosti ORM “Poluchenie komp'yuternoi informatsii” v ugolovno-protsessual'nom aspekte [Additional capacities of the operational-search activity "Obtaining computer information" from the criminal procedural aspect]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 8 (6A), pp. 71-77.

Keywords

Evidence, special investigative activity "Obtaining computer information", search, seizure, electronic media.

References

1. Kasatkin A.B. (1997) *Taktika sobiraniya i ispol'zovaniya komp'yuternoi informatsii pri rassledovanii prestuplenii. Doct. Diss.* [The tactics of collecting and using computer information in the investigation of crimes. Dost. Diss.]. Moscow.

2. *Konstitutsiya Rossiiskoi Federatsii: prinyata vsenarodnym golosovaniem 12.12.1993* [Constitution of the Russian Federation: adopted by popular vote on December 12, 1993]. Available at: http://www.consultant.ru/document/cons_doc_LAW_28399/ [Accessed 24/05/18].
3. Kucheruk D.S. (2009) K voprosu ob ispol'zovanii v dokazyvanii rezul'tatov glasnykh operativno-rozysknykh meropriyatii [On the use of the results of public operational-search activities as evidence]. In: Baranov V.M., Pshenichnov M.A. (eds.) *Problemy yuridicheskoi nauki v issledovaniyakh doktorantov, ad"yunktov i soiskatelei* [Problems of legal science in research carried out by doctoral students and postgraduates], Vol. 15. Nizhny Novgorod, pp. 48-51.
4. Kuchin O.S. (ed.) (2017) *Elektronnye nositeli informatsii v kriminalistike* [Electronic media in forensic science]. Moscow: Yurlitinform Publ.
5. Mitskevich A.F., Susloparov A.V. (2010) Ponyatie komp'yuternoi informatsii po rossiiskomu i zarubezhnomu ugolovnomu pravu [The concept of computer information in Russian and foreign criminal law]. *Probely v rossiiskom zakonodatel'stve* [Gaps in Russian legislation], 2, pp. 206-209.
6. *O politsii: feder. zakon Ros. Federatsii ot 07.02.2011 № 3-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 28.01.2011: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 02.02.2011* [On the police: Federal Law of the Russian Federation No. 3-FZ of February 7, 2011]. Available at: http://www.consultant.ru/document/cons_doc_LAW_110165/ [Accessed 24/05/18].
7. *O vnesenie izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i otdel'nye zakonodatel'nye akty Rossiiskii Federatsii: feder. zakon Ros. Federatsii ot 29.11.2012 № 207-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 23.11.2012: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 28.11.2012* [On amending the Criminal Code of the Russian Federation and certain legislative acts of the Russian Federation: Federal Law of the Russian Federation No. 207-FZ of November 29, 2012]. Available at: http://www.consultant.ru/document/cons_doc_LAW_138322/ [Accessed 24/05/18].
8. *Ob operativno-rozysknoi deyatel'nosti: feder. zakon Ros. Federatsii ot 12.08.1995 № 144-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 05.07.1995* [On operational-search activities: Federal Law of the Russian Federation No. 144-FZ of August 12, 1995]. Available at: http://www.consultant.ru/document/cons_doc_LAW_7519/ [Accessed 24/05/18].
9. Plakhotnyuk Yu.I. (2013) Vzaimodeistvie organov predvaritel'nogo sledstviya s operativnym i drugimi podrazdeleniyami pri rassledovanii ugolovnykh del po prestupleniyam protiv sem'i i nesovershennoletnikh [The interaction of preliminary investigation bodies with operational and other units in the investigation of crimes against the family and minors]. *Materialy II mezhdunarodnoi nauchnoi konferentsii "Gosudarstvo i pravo: teoriya i praktika"* [Proc. 2nd Int. Conf. "State and law: theory and practice"]. Chita. Available at: https://moluch.ru/conf/law/archive/83/3340/ [Accessed 24/05/18].
10. *Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 18.12.2001 № 174-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 22.11.2001: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.12.2001* [Criminal Procedure Code of the Russian Federation: Federal Law of the Russian Federation No. 174-FZ of December 18, 2001]. Available at: http://www.consultant.ru/document/cons_doc_LAW_34481/ [Accessed 24/05/18].
11. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 24.05.1996: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.06.1996* [Criminal Code of the Russian Federation: Federal Law of the Russian Federation No. 63-FZ of June 13, 1996]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/ [Accessed 24/05/18].
12. Vekhov V.B. (2008) *Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoi informatsii i sredstv ee obrabotki* [The fundamentals of forensic doctrine of studying and using computer information and means of its processing]. Volgograd: Volgograd Academy of the Ministry of Internal Affairs.