Научная статья
УДК 343.132
https://doi.org/10.36511/2078-5356-2022-4-238-242

Выемка, осмотр и обыск в электронных сетях: понятие и разграничение

Телевицкая Юлия Андреевна
Нижегородская академия МВД России, Нижний Новгород, Россия, miss.umniagina@yandex.ru

Аннотация. Совершенствование уголовно-процессуального законодательства как одна из действенных форм противодействия преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий, не может обойтись без регулирования вопросов собирания доказательств на электронных носителях информации. Электронные сети являются одним из видов таких электронных носителей. В статье автор обращает внимание на актуальность исследования процессуальных особенностей собирания информации из электронных сетей, приходит к выводу о необходимости дополнения Уголовно-процессуального кодекса Российской Федерации такими следственными действиями, как осмотр электронных сетей, обыск в электронных сетях, выемка в электронных сетях. Приводится их разграничение между собой.

Ключевые слова: электронные сети, осмотр, обыск, выемка, собирание информации, изъятие, электронные носители информации

Для цитирования: Телевицкая Ю. А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 238—242. https://doi.org/10.36511/2078-5356-2022-4-238-242.

Original article

Seizure, inspection and search in electronic networks: the concept and differentiation

Yulia A. Televitskaya
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, miss.umniagina@yandex.ru

Abstract. The improvement of criminal procedure legislation as one of the effective forms of countering crimes committed in the field of information and telecommunication technologies cannot do without regulating the issues of collecting evidence on electronic media. Electronic networks are one of the types of electronic media. In the article, the author draws attention to the relevance of the study of the procedural features of collecting information from electronic networks, comes to the conclusion that it is necessary to supplement the Criminal Procedure Code of the Russian Federation with such investigative actions as inspection of electronic networks, search in electronic networks, seizure in electronic networks. Their differentiation among themselves is given.

Keywords: electronic networks, inspection, search, seizure, collection of information, seizure, electronic media

For citation: Televitskaya Yu. A. Seizure, inspection and search in electronic networks: concept and differentiation. *Legal Science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2022, no. 4 (60), pp. 238—242. (In Russ.). https://doi.org/10.36511/2078-5356-2022-4-238-242.

В современном мире возрастает значимость информации и информационных технологий. Информация, в свою очередь, в большом объеме содержится в информационно-телекоммуникационных сетях, которые в настоящее время получили широкое распространение.

В соответствии со статистическими данными, предоставленными *We Are Social и Hootsuite*, в 2021 году на 7,3 % увеличилось количество

пользователей сети «Интернет» по сравнению с прошлым годом. Уровень проникновения интернета составляет почти 60 % при количестве пользователей в 4,66 миллиарда человек [1].

Однако развитие информационного общества и информационных технологий приводит не только к дальнейшей глобализации современного общества, но и к появлению новых угроз для него. По данным ГИАЦ МВД России, за первое полугодие 2022 года преступления в сфере IT-технологий составили одну четвертую часть от общего уровня преступности в стране. За 2020—2021 годы почти на 100 % увеличилось количество преступлений, совершаемых через сеть «Интернет» [2]. Таким образом, расследование преступлений в сфере информационно-телекоммуникационных технологий должно стать приоритетным направлением деятельности правоохранительных органов.

Идею о введение в Уголовно-процессуальный кодекс Российской Федерации (далее — УПК РФ) удаленных (дистанционных) следственных действий высказывали многие отечественные ученые. А. Н. Иванов считает необходимым дополнить перечень следственных действий дистанционными осмотром и обыском, аргументируя это тем, что УПК РФ пора привести к состоянию, в котором его нормы будут учитывать все современные достижения в области электронной информации [3, с. 76]. А. А. Балашова, выступая сторонником введения удаленных следственных действий, предлагает закрепить в УПК РФ дистанционные осмотр и обыск, обосновывая необходимость удаленных следственных действий существующим в настоящее время пробелом в процессуальном законодательстве относительно регулирования вопросов получения доказательственной информации, содержащейся в информационной системе [4, с. 130—134]. Примечательно, что в литературе не рассматривался вопрос о возможности производства выемки с целью изъятия информации из электронных сетей.

Следует отметить, что на сегодняшний день уголовно-процессуальное законодательство не содержит правового регулирования собирания информации из сетевых инфраструктур. Изъятие информации из электронных сетей происходит путем производства следственного осмотра. Считаем, что осмотр в порядке статьи 176 УПК РФ не может в полной мере соответствовать всем особенностям, которые присущи электронным сетям и работе с электронной информации в целом. Именно поэтому мы предлагаем дополнить УПК РФ отдельной главой, которая будет регулировать процесс собирания информации из электронных сетей. В систему следственных действий, закрепляющих особенности изъятия информации из сетевых инфраструктур, предлагаем включить осмотр электронных сетей, обыск в электронных сетях, выемка в электронных сетях.

Чтобы понять сущность предлагаемых следственных действий, следует разграничить их между собой.

При разграничении дистанционного осмотра и обыска следует обратить внимание на тот факт, что оба следственных действия имеют поисково-познавательный характер, направлены на получение доказательственной информации, содержащейся в электронной сети, доступ к которой осуществляется с помощью технических устройств. Главное различие между ними состоит в возможности или невозможности собирания доказательственной информации, находящейся в закрытом доступе в электронной сети.

В рамках возбужденного уголовного дела по факту приобретения наркотических средств через сеть «Интернет» следователь произвел осмотр странички в социальной сети «ВКонтакте», используя в качестве технического средства рабочий компьютер. В результате осмотра был обнаружен сайт, с которого непосредственно были приобретены наркотики. Для подтверждения данного факта следователь сделал скриншоты осмотренного сайта [5].

В целях установления факта фальсификации доказательств следователь в присутствии специалиста произвел осмотр сетевой инфраструктуры "Lotus", подразумевающей обмен почтой между сотрудниками компании. Все необходимые для уголовного дела сведения были зафиксированы с помощью скриншотов и приложены к протоколу осмотра [6].

Как видно из представленных примеров, в настоящее время именно осмотром оформляется получение сведений из сетей любого масштаба, будь то локальных или глобальных. Однако возникает вопрос: «Как же должен поступить следователь, если информация в сетевых инфраструктурах находится не в свободном доступе: система требует пароль для входа, а лицо отказывается предоставлять такую информацию?». Преодоление преград в виде паролей и блокировок входа уже будет выходить за пределы действия осмотра.

Уголовно-процессуальное законодательство не содержит понятия осмотра. Однако в федеральном законодательстве Российской Федерации данное понятие все же закреплено.

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 4 (60)

Статья 76 Федерального закона от 31 июля 2020 года № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации предлагает считать осмотром визуальное обследование территории и иных объектов без их вскрытия и нарушения целостности [7]. Преодоление защиты в виде паролей можно приравнять к вскрытию помещения или иному нарушению целостности объекта исследования. Следовательно, под категорию «осмотр» обход паролей для получения доступа к закрытому аккаунту в информационной сети попадать не может.

В соответствии с частью 6 статьи 182 УПК РФ при обыске могут вскрываться любые помещения, если лицо отказывается открыть их добровольно. В виду отсутствия специальных норм предположим, что для получения информации из закрытых для общего доступа источников в сети следует применить аналогию части 6 статьи 182 УПК РФ и отдавать предпочтение такому следственному действию, как обыск, а не осмотр.

Однако в следственно-судебной практике дела обстоят совершенно иначе.

В. Ф. Васюкин и А. Н. Колычева приводят примеры получения доступа к закрытым web-ресурсам в рамках осмотра, указывая на то, что современные браузеры способны сохранять логины и пароли пользователя. Следовательно, с помощью программ для сохранения паролей можно легко получить доступ к необходимому сетевому ресурсу, если имеется изъятый электронный носитель информации владельца [8, с. 115—116]. Соглашаясь с тем, что рассмотренный способ, несомненно, наиболее благоприятен для органов предварительного расследования, нельзя оставить без внимания тот факт, что обход паролей, будь то получение доступа с помощью специальных программ или наличие данных, сохраненных в памяти браузера, не может позиционироваться как осмотр. По нашему мнению, данные действия подходят под определение обыска.

Следовательно, с целью изъятия общедоступной информации из электронных сетей следует применять нормы дистанционного осмотра, так как при нем не будет нарушено правило «исключительно визуального обследования». Получение информации, доступ к которой ограничен обладателем, может быть осуществлено исключительно при производстве обыска в сетевой инфраструктуре.

Таким образом, происходит отграничение осмотра от обыска на основании критерия «доступность информации для общего пользования».

В общей теории уголовного процесса обыск часто разграничивают с выемкой. Отсылочная норма в статье 183 УПК РФ также указывает на схожесть процессуального порядка производства следственных действий. Следует отметить, что вопрос выемки информации из сетевых инфраструктур еще не исследовался в отечественном уголовно-процессуальном праве.

По общим правилам выемка заключается в добровольном или принудительном изъятии у лица индивидуально-определенных предметов, документов и электронных носителей информации, имеющих значение для уголовного дела. Ключевым признаком рассматриваемого следственного действия является осведомленность правоохранительных органов о предмете, месте и субъекте, у которого находятся представляющие интерес объекты.

Однако ввиду специфики электронных сетей как объекта выемки следует обозначить процессуальные особенности изъятия информации из сетевых инфраструктур. Если в случае с обыском в электронных сетях ключевым критерием для его производства является закрытый доступ к интересующей информации, то в случае с выемкой следует обращать внимание на уже имеющиеся в деле сведения относительно того, какая именно информации находится в сети, на каком ресурсе она отображается и кто является ее обладателем. Категория «у кого находятся сведения» не применима к информации, хранящейся в электронной сети, так как в материальном воплощении она не существует. Поэтому при выемке электронной информации из сетевых инфраструктур необходимо обращать внимание на следующие критерии: определенность информации, место ее нахождения в сети и сведения об ее обладателе.

Как уже было отмечено выше, изъятие информации из электронных сетей, которая является общедоступной, по нашему мнению, следует осуществлять путем производства осмотра электронных сетей. Обыск производится в случае наличия препятствий в доступе к информации. Выемка занимает промежуточное положение. Изъятие информации путем производства выемки возможно и в случае с общедоступной информацией, и при необходимости в собирании сведений из закрытых источников в электронной сети при соблюдении особенностей производства выемки как следственного действия.

Если органы предварительного расследования владеют указанными сведениями, то производится выемка, а не обыск или осмотр, так как отпадает необходимость в поиске информации. В случае добровольной выдачи не имеет значения, находятся ли предоставляемые сведения в открытом или закрытом для третьих лиц доступе. Если обладатель информации отказывается добровольно предоставить необходимые для уголовного дела сведения, их выемка производится принудительно.

Таким образом, говоря о следственных действиях, направленных на изъятие информации из электронных сетей, нельзя ограничиваться исключительно осмотром. Необходимо также рассмотреть возможность производства дистанционного обыска и выемки.

На основании изложенного, считаем целесообразным определить категориальный аппарат рассматриваемых следственных действий.

Под осмотром электронных сетей следует понимать следственное действие, заключающееся в визуальном обследовании сетевой инфраструктуры, производимое с целью отыскания и собирания необходимой для уголовного дела информации, находящейся в свободном доступе для всех пользователей сети.

Под обыском в электронных сетях следует понимать следственное действие, заключающееся в принудительном обследовании сетевой инфраструктуры, с целью отыскания и собирания необходимой для уголовного дела информации, доступ к которой ограничен обладателем.

Под выемкой в электронных сетях следует понимать следственное действие, связанное с изъятием имеющей значение для дела определенной информации из электронной сети, если точно известно, где она находится.

Если с глобальной сетью проблем не возникает, то при изъятии информации из локальных сетей могут возникнуть определенные трудности при выборе следственного действия, направленного на сбор доказательственной информации. Общедоступные сведения в сети «Интернет» подлежат изъятию в ходе производства осмотра. Данные, доступ к которым ограничен обладателем, изымаются путем производства обыска. Локальные сети, в отличие от глобальных, имеют относительно небольшие масштабы, количество узлов в них жестко ограничено. Сети подобного рода можно представить как закрытую систему, доступ к которой предоставляется исключительно на определенной территории и ограниченному числу пользователей. К примеру, доступ к локальной вычислительной сети организации имеют только ее работники. Доступ к корпоративной вычислительной сети коммерческого банка имеют только работники банка, третьи лица не могут ознакомиться со сведениями, хранящимися в локальных сетях, тем более если они находятся за пределами зоны покрытия. Информация в локальных вычислительных сетях не является общедоступной. Доступ к сведениям ограничен. Следовательно, данные из локальных вычислительных сетей могут быть изъяты только путем производства обыска.

В случае если у органов предварительного расследования имеются сведения относительно того, какая именно информация находится в локальной сети, а также сведения о сети (к примеру, локальная сеть организации, городская сеть или локальная сеть в компьютерном классе и др.), то производится выемка.

Таким образом, изъятие общедоступной информации из электронных сетей может производиться путем производства специального вида осмотра —сетевого. Получение информации, доступ к которой ограничен обладателем, может быть осуществлен исключительно при производстве обыска в сетевой инфраструктуре. В том случае, если точно известно, где хранится определенная электронная информация, производится выемка. Если обладатель информации отказывается добровольно предоставить необходимые для уголовного дела сведения, их выемка производится принудительно.

Список источников

1. Digital 2021: the latest insights into the state of digital. URL: https://wearesocial.com/uk/blog/2021/01/digital-2021/ (дата обращения: 18.07.2022).

2. Министерство внутренних дел Российской Федерации. Краткая характеристика состояния преступности за январь—июнь 2022 года. URL: https://мвд.рф/reports/item/31209853/ (дата обращения: 08.07.2022).

3. Иванов А. Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. 2009. № 2. С. 77—77.

4. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. … канд. юрид. наук. М., 2020. 216 с.

5. Приговор Сургутского городского суда Ханты-Мансийского автономного округа — Югры № 1-1241/2018 1-170/2019 1-27/2020 от 18 мая 2020 года. URL: https://sudact.ru (дата обращения: 06.11.2021).

6. Приговор Центрального районного суда г. Читы № 1-1223/2019 1-43/2020 от 27 июля 2020 года. URL: https://sudact.ru (дата обращения: 06.11.2021).

7. О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации: федеральный закон от 31 июля 2020 года № 248-ФЗ (с изм. и доп., вступ. в силу с 1 января 2022 г.). Доступ из СПС «КонсультантПлюс» (дата обращения: 15.01.2022).

8. Васюков В. Ф., Колычева А. Н. Осмотр и фиксация страниц интернет сайта в сети «Интернет» // Вестник экономической безопасности. 2019. № 1. С. 115—118.

References

1. Digital 2021: the latest insights into the state of digital. URL: https://wearesocial.com/uk/blog/2021/01/digital-2021/ (accessed 18.07.2022). (In Russ.)

2. Ministry of Internal Affairs of the Russian Federation. A brief description of the state of crime in January—June 2022. URL: https://мвд.рф/reports/item/31209853/ (accessed 08.07.2022). (In Russ.)

3. Ivanov A. N. Remote study of computer information: criminal procedural and criminalistic problems. *Izvestiya Saratov University*, 2009, no. 2, pp. 77—77. (In Russ.)

4. Balashova A. A. Electronic media and their use in criminal procedural proof. Dissertation… candidate of legal sciences. Moscow. 2020. Pp. 130—137. (In Russ.)

5. Verdict of Surgut City Court of Khanty-Mansiysk Autonomous Okrug — Yugra Verdict no. 1-1241/2018, 1-170/2019, 1-27/2020 of May 18, 2020. URL: https://sudact.ru (accessed 06.11.2021). (In Russ.)

6. Verdict of the Central District Court of Chita no. 1-1223/2019, 1-43/2020 of July 27, 2020. URL: https://sudact.ru (accessed 06.11.2021). (In Russ.)

7. On State Control (Supervision) and Municipal Control in the Russian Federation: federal law no. 248-FZ of July 31, 2020 (with amendments and additions, intro. effective from January 1, 2022). Access from the reference legal system "ConsultantPlus" (accessed 15.01.2022). (In Russ.)

8. Vasyukov V. F., Kolycheva A. N. Inspection and fixation of the pages of the Internet site on the Internet. *Bulletin of Economic Security*, 2019, no. 1, pp. 115—118. (In Russ.)

Статья поступила в редакцию 15.10.2022; одобрена после рецензирования 20.11.2022; принята к публикации 01.12.2022.

The article was submitted 15.10.2022; approved after reviewing 20.11.2022; accepted for publication 01.12.2022.