

Научная статья
УДК 343.132
<https://doi.org/10.36511/2078-5356-2023-4-191-194>

Объект выемки, осмотра и обыска в электронных сетях

Телевицкая Юлия Андреевна

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

Аннотация. В рамках предварительного расследования по уголовному делу часто возникает необходимость в собирании сведений, хранящихся в информационно-телекоммуникационных сетях, в том числе в сети «Интернет». В представленном исследовании проанализированы различные подходы к объекту осмотра, обыска и выемки в электронных сетях. Приводится разграничение технического средства, применяемого при производстве следственного действия от объекта при собирании информации из электронных сетей, доступ к которой осуществляется через электронные носители. Предложено авторское видение понятия «электронная сеть» как специфической разновидности электронных носителей информации.

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

Для цитирования: Телевицкая Ю. А. Объект выемки, осмотра и обыска в электронных сетях // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 4 (64). С. 191–194. <https://doi.org/10.36511/2078-5356-2023-4-191-194>.

Original article

The object of seizure, inspection and search in electronic networks

Yulia A. Televitskaya

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

Abstract. As part of the preliminary investigation of a criminal case, it often becomes necessary to collect information stored in information and telecommunications networks, including the Internet. In the presented work, the author analyzes various approaches to the object of inspection, search and seizure in electronic networks. A distinction is made between the technical means used in the production of an investigative action and the object when collecting information from electronic networks, access to which is carried out through electronic media. The author's vision of the concept of "electronic network" as a specific kind of electronic media is proposed.

Keywords: electronic media, electronic network, inspection, search, seizure, seizure, collection

For citation: Televitskaya Yu. A. The object of seizure, inspection and search in electronic networks. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 4 (64), pp. 191–194. (In Russ.). <https://doi.org/10.36511/2078-5356-2023-4-191-194>.

Целью нашего исследования является разработка комплексного механизма собирания информации из электронных сетей. В работах, опубликованных ранее, мы обозначили круг следственных действий, которые будут направлены на сбор необходимой информации [1]. Однако открытым остался вопрос об объекте осмотра, обыска и выемки в электронных сетях.

Отличительной чертой следственных действий, направленных на собирание информации

из электронных сетей, является их объект. Именно специфика объекта отличает удаленные следственные действия от тех, которые уже закреплены в Уголовно-процессуальном кодексе Российской Федерации (далее — УПК РФ). Разница между видами осмотра / обыска / выемки, предусмотренными УПК РФ и осмотром / обыском / выемки в электронной сети существенна, следовательно, и объект дистанционного следственного действия должен быть отличным от

© Телевицкая Ю. А., 2023

классического. Если в первом случае границы и пределы осмотра / обыска / выемки можно увидеть, то во втором случае при собирании информации из электронной сети, тем более глобальной, границ попросту не существует.

Так, А. А. Балашова в своем исследовании отмечает, что осмотр сетевой инфраструктуры, в том числе страниц в сети «Интернет», происходит путем производства следственного осмотра, в котором объектом выступает электронный носитель информации, чаще всего в виде компьютера самого следователя [2, с. 121]. Получается, что объектом производства следственного действия признается компьютер как носитель информации, а не сам сетевой ресурс, на котором непосредственно находится необходимые для уголовного дела сведения. Однако следует понимать, что для уголовного дела представляет интерес не сам ноутбук или даже информация, находящаяся в его памяти, а данные из информационно-телекоммуникационной сети (далее — ИТС) либо любой сетевой инфраструктуры, доступ к которой невозможен без специального технического средства. Если отталкиваться от теории С. В. Зуева, согласно которой сам по себе сетевой ресурс является носителем электронных данных, целесообразнее признать объектом осмотра именно его. Соответственно, компьютер, с помощью которого осуществляется доступ к необходимым сведениям, находящимся за пределами его памяти, следует признавать техническим средством, а не объектом. Компьютер может быть объектом следственного действия только при производстве осмотра его внешних признаков и внутренней памяти. Осмотр данных в сетевой инфраструктуре не может входить в предмет осмотра компьютера, так как информация из электронных сетей находится за его пределами.

А. Н. Иванов считает, что объектом осмотра сетевых инфраструктур следует признавать документ, обнаруженный в сети, а результаты следственного действия необходимо оформлять протоколом осмотра документов [3, с. 75]. Кроме того, А. Л. Карлов придерживается аналогичного мнения, уточняя, что под объектом осмотра электронных сетей следует понимать не просто документ, а документ, информация в котором представлена в электронно-цифровом формате [4, с. 143]. Следовательно, результат осмотра, по мнению автора, следует оформлять протоколом осмотра электронного документа, под которым он предлагает считать страницу в сети «Интернет».

Не можем полностью согласиться с мнением А. Н. Иванова и А. Л. Карлова. Если под объектом дистанционного осмотра понимать страницу в сети «Интернет», то неурегулированным

по-прежнему останется осмотр в локальных, региональных, корпоративных сетях. Также документ как объект осмотра в полной мере не отражает всю специфику следственного действия, так как электронные сети представляют собой материю наиболее сложную. Следовательно, признавать документ объектом осмотра электронных сетей неправильно.

По нашему мнению, следует расширить закрепленный в УПК РФ перечень объектов осмотра / обыска / выемки, дополнив его электронной сетью.

Так, Л. Г. Литвяк утверждает, что «информационно-телекоммуникационная сеть» и «электронная сеть» — это синонимичные понятия [5, с. 95]. С. В. Зуев использует также понятие «компьютерная сеть», под которой он предлагает понимать программные, аппаратные и информационные ресурсы, связанные между собой и распределенные по определенной территории. К информационным ресурсам автор относит средства ввода-вывода, обработки и хранения информации, доступ к которой осуществляется с нескольких технических устройств [6, с. 31].

Другие ученые приравнивают к понятию электронной и ИТС информационную сеть, под которой понимают совокупность каналов связи, коммутирующей аппаратуры, электронно-вычислительных машин, объединенных средствами передачи данных [7, с. 214–215].

В декабре 2022 года Верховный Суд Российской Федерации закрепил, что понятия электронно-телекоммуникационных и электронных сетей не разграничиваются. При этом Верховный Суд Российской Федерации отметил, что сеть «Интернет» является одним из их видов [8].

Российское законодательство не содержит понятий электронной и компьютерной сети. Однако в Федеральном законе от 27 июня 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — ФЗ № 149) дано определение ИТС, под которой понимается предназначенная для передачи по линиям связи технологическая система, доступ к которой осуществляется с помощью средств вычислительной техники [9].

По нашему мнению, при обозначении характеристик сети следует обратить внимание на две основные составляющие: информационную и телекоммуникационную. Закон не раскрывает данные характеристики при обозначении дефиниции ИТС.

Под телекоммуникационной сетью понимается система каналов связи и коммутационного оборудования, осуществляющих обмен данными

между различными программами, задающими способ передачи данных и исправления ошибок. Следовательно, в основе телекоммуникации лежит дистанционный обмен информацией. В основе информационной составляющей ИТС — хранение информации [10, с. 8]. Определение, закрепленное в ФЗ № 149, содержит характеристику только коммуникационной составляющей, направленной на обмен информацией, упуская из внимания информационную — способность к хранению информации. Сохранность данных и их защита от искажений являются основными принципами работы электронных сетей. Данные хранятся на специальных серверах, специализированных устройствах с большим объемом памяти, представляющие собой хранилища информации. Хранение информации — неотъемлемая составляющая ИТС. Таким образом, считаем, что при обозначении понятия ИТС необходимо передачу информации заменить обменом информации, тем самым расширив ее коммуникационную составляющую, а также добавить формулировку, связанную с хранением, с целью указания на информационный характер сети.

Еще одним важным моментом при обозначении характеристики ИТС является ее классификация.

Сети делятся на три группы в зависимости от территориального признака и объема входящих в них данных. Локальные сети относятся к первой группе. Они обычно охватывают небольшие территории и ресурсы, расположенные в нескольких километрах друг от друга. Примером может служить локальная сеть вуза или школы. Вторая группа представлена региональными сетями, которые могут охватить район, город или даже целую республику. Третий элемент классификации — глобальные сети, которые могут охватить несколько стран и даже континентов. Самым ярким примером глобальной сети является сеть «Интернет».

Интернет представляет собой конгломерат глобальных систем, в результате чего в нем наиболее наглядно проявляются все особенности функционирования современных сетевых инфраструктур. Также в отдельную группу выделяют корпоративные сети, управляемые единой организацией, к примеру, сеть МВД РФ [6, с. 31].

В соответствии с результатами анкетирования 67 % опрошенных граждан утверждают, что под ИТС подразумевается исключительно сеть «Интернет». 21 % ответили, что данное понятие включает в себя и другие виды сетей.

12 % затруднились дать ответ на поставленный вопрос.

Следует отметить, что ИТС включает в себя локальные, региональные, корпоративные, а также глобальные сети, в том числе сеть «Интернет». Неосведомленность в обозначенном вопросе еще раз подчеркивает необходимость рассмотрения видов электронных сетей, обозначения категории «электронная сеть», а также отдельное изучение особенностей изъятия информации из локальных сетей.

Пятый кассационный суд общей юрисдикции в своем постановлении при упоминании корпоративной сети ссылается на определение ИТС, закрепленное в пункте 4 статьи 2 ФЗ № 149, тем самым указывая на ее принадлежность к ИТС [11]. Таким образом, корпоративная сеть является составной частью ИТС, что еще раз подтверждается решением кассационного суда.

Термины «компьютерная сеть», «электронная сеть», «информационно-телекоммуникационная сеть» являются синонимичными понятиями. Следовательно, характеристики, рассмотренные на примере ИТС, распространяются и на остальные понятия, применяемые авторами для обозначения технологических систем обмена и хранения данных, передаваемых по линиям связи. Под ИТС в сознании людей чаще всего понимается именно сеть «Интернет», именно поэтому с целью недопущения ограничительного толкования предлагаем взять за основу объекта дистанционного осмотра, обыска и выемки понятие «электронная сеть».

Под электронной сетью предлагаем понимать технологическую систему, функционирующую на локальном, региональном, корпоративном или глобальном уровнях, предназначенную для дистанционного обмена информацией и ее хранением, доступ к которой осуществляется с помощью средств вычислительной техники.

Следовательно, если брать во внимание тот факт, что объектом дистанционных следственных действий (осмотр, обыск и выемка в сетевых инфраструктурах) является электронная сеть, в которую входят все разновидности существующих сетей, то документом, отображающим ход производства следственного действия, должен быть протокол осмотра / обыска / выемки электронной сети. В протоколе должно быть обязательно указано техническое средство, при помощи которого производилось следственное действие, а также способ размещения данных в сети.

Список источников

1. 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.
2. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. Москва, 2020. 216 с.
3. Иванов А. Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. 2009. Т. 9. Вып. 2. С. 74–77.
4. Карлов А. Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети Интернет // Вестник сибирского юридического института ФСКН России. 2015. № 2 (19). С. 142–146.
5. Литвяк Л. Г. К вопросу о понятии электронных или информационно-телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. № 11-2. С. 93–96.
6. Зуев С. В. Основы теории электронных доказательств: монография / под ред. С. В. Зуева. Москва: Юрлитинформ, 2019. 398 с.
7. Головин Ю. А. Информационные сети: учебник для студентов высших учебных заведений, обучающихся по направлению подготовки «Информационные системы». Москва: Академия, 2013. 375 с.
8. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37. Доступ из СПС «КонсультантПлюс» (дата обращения: 27.05.2023).
9. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 года № 149-ФЗ. Доступ из СПС «КонсультантПлюс» (дата обращения: 11.05.2023).
10. Кошелев С. В. Информационные сети: учебное пособие. Муром: Телеком, 2004. 298 с.
11. Определение Пятого кассационного суда общей юрисдикции от 10 ноября 2020 года № 88-6460/2020 по делу № 2-195/2020. Доступ из СПС «КонсультантПлюс» (дата обращения: 27.05.2023).

Статья поступила в редакцию 15.08.2023, одобрена после рецензирования 03.11.2023; принята к публикации 12.12.2023.

The article was submitted 15.08.2023, approved after reviewing 03.11.2023; accepted for publication 12.12.2023.

References

1. Televitskaya Yu. A. Seizure, inspection and search in electronic networks: concept and differentiation. *Legal science and practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 4 (60), pp. 238–242. (In Russ.)
2. Balashova A. A. Electronic media and their use in criminal procedural proof. Dissertation... candidate of legal sciences. Moscow. 2020. 216 p. (In Russ.)
3. Ivanov A. N. Remote study of computer information: criminal procedural and criminalistic problems. *Izvestiya Saratov University*, 2009, vol. 9, issue 2, pp. 74–77. (In Russ.)
4. Karlov A. L. The use in proving criminal cases of information constituting the secret of communication located on the Internet. *Bulletin of the Siberian Law Institute of the Federal Drug Control Service of Russia*, 2015, no. 2 (19), pp. 142–146. (In Russ.)
5. Litvyak L. G. On the question of the concept of electronic or information and telecommunication networks for the purposes of criminal law. *Humanities, socio-economic and social sciences*, 2020, no. 11-2, pp. 93–96. (In Russ.)
6. Zuev S. V. Fundamentals of the theory of electronic evidence: monograph / ed. by S. V. Zuev. Moscow: Yurliinform Publ., 2019. 398 p. (In Russ.)
7. Golovin Yu. A. Information networks: textbook: for students of higher educational institutions studying in the field of training “Information systems”. Moscow: Academy Publ., 2013. 375 p. (In Russ.)
8. On some issues of judicial practice in criminal cases on crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet: resolution of the Plenum of the Supreme Court of the Russian Federation no. 37 of December 15, 2022. Access from the reference legal system “ConsultantPlus” (accessed 27.05.2023). (In Russ.)
9. On Information, Information Technologies and Information Protection: federal law no. 149-FZ of July 27, 2006. Access from the reference legal system “ConsultantPlus” (accessed 11.05.2023). (In Russ.)
10. Koshelev S. V. Information networks: a textbook. Murom: Telecom Publ., 2004. 298 p. (In Russ.)
11. The ruling of the Fifth Cassation Court of General Jurisdiction no. 88-6460/2020 of November 10, 2020 in the case no. 2-195/2020. Access from the reference legal system “ConsultantPlus” (accessed 27.05.2023). (In Russ.)