УДК 343.13 DOI: 10.17277/pravo.2020.01.pp.109-115

Показаны особенности производства осмотра по уголовным делам о преступлениях в сфере компьютерной информации. Отмечено, что задачами осмотра в расследовании данной категории преступлений являются обнаружение, фиксация и изъятие специфических электронно-цифровых следов. Обоснована необходимость внесения изменений в уголовно-процессуальное законодательство Российской Федерации в части расширения перечня полномочий следователя при производстве осмотра места происшествия по преступлениям, совершаемым в сфере компьютерной информации.

Ключевые слова: преступления в сфере компьютерной информации; осмотр места происшествия; осмотр предметов и документов; предварительное расследование; процесс доказывания.

Алексей Михайлович Попов, *канд. юрид. наук, доцент, заведующий кафедрой «Безопасность и правопорядок», ФГБОУ ВО «Тамбовский государственный технический университет», Тамбов, Россия; pamtambov@yandex.ru*

Андрей Иванович Дубовицкий, *научный сотрудник, управление организации научной и редакционно-издательской деятельности, ФГКОУ ВО «Московский университет МВД Российской Федерации имени В. Я. Кикотя», Москва, Россия; adubovitckii5@mvd.ru*

ОСОБЕННОСТИ ПРОИЗВОДСТВА ОСМОТРА ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ЭЛЕМЕНТ ДОКАЗЫВАНИЯ

Информационный прогресс является важнейшим способом развития государства и его экономического роста. Вместе с этим нечистые на руку субъекты научились использовать благо в своих корыстных целях, обманывая людей и чувствуя свою безнаказанность. Что такое компьютерное преступление известно многим, даже тем, кто никогда с ним не сталкивался. Все слышали про взломы почтовых ящиков, использование чужих личных данных и внедрение вирусов, которые уничтожают всю имеющуюся информацию на сервере.

Определять подобные злодеяния очень сложно, а найти и наказать злоумышленника еще сложнее. Киберпреступление направлено против безопасности информации, которая гарантируется на государственном уровне.

Понятие «киберпреступность» сравнительно новое, и еще не достаточно изучено правоохранительными органами.

Согласно статистическим данным, компьютерная преступность часто инициируется несовершеннолетними гражданами, которые желают заработать, используя мнимую конфиденциальность. Конечно, более серьез-

ные преступления по взлому банковских серверов и созданию вирусных программ, это дело рук профессионалов, но именно несовершеннолетние пользуются своим статусом «уголовно-ненаказуемых» и нередко обманывают пользователей социальных сетей, шантажируют и используют их личные данные.

Компьютерная преступность развивается во многих сферах, соответственно, нарушения разделяют на конкретные виды. На сегодняшний день различают следующие виды злодеяний.

Взлом − получение доступа к чужим данным. Осуществляется путем подбора пароля к нужному сайту и распоряжения имеющейся там информацией на свое усмотрение. Разновидностью взлома является использование данных IP-адресов для совершения преступлений под вымышленным адресом.

Фишинг − попытка завладеть личными данными пользователей. Создаются ложные сайты, требующие ввода номера кредиток или паспортных данных, через которые потом осуществляются несанкционированные операции с банковскими счетами и картами. Вирусы являют собой вредоносные программы, которые размножаются, попав в систему, и уничтожают важные данные, имеющиеся на компьютере. Злоумышленники создают набор специальных кодов и распространяют его через Сеть, через USB-накопители и компакт-диски.

Киберпреследование − суть преступления в том, что злоумышленники на всевозможных сайтах собирают информацию о своей жертве, а потом присылают письма с угрозами и оскорблениями. Целью подобных нарушений, как правило, выступает месть или личная неприязнь к жертве. Кража личности – одна из самых серьезных фальсификаций, ведь собрав достойное количество информации о потерпевшем, можно от его имени осуществлять ряд серьезных операций, таких как хищение денег и получение фальшивых удостоверений.

Кибервымогательство осуществляется в целях получения денег. Преступление может быть направлено на отдельных граждан или на коммерческие предприятия. Злоумышленник блокирует доступ компьютеров определенного предприятия к Сети или конкретным программам до получения выкупа. В случае с обычными гражданами злоумышленник может распространить слух о том, что частные фото жертвы имеются на порно сайте и будут там находиться, пока человек не выплатит конкретную сумму.

Кибервойны − самые серьезные преступления, ведь сторонами конфликта выступают разные страны. Хакеры одной страны взламывают серверы и сайты другой страны в целях дестабилизации экономической безопасности противника. Электронный спам – банальный тип преступлений. Каждый пользователь Сети неоднократно с ним сталкивался. На почту приходит письмо со ссылкой, которая отправляет на вредоносный сайт, после перехода слетает программное обеспечение или компьютер заражается вирусом. Вариантов осуществления преступлений подобного вида существует огромное множество, каждое имеет свои особенности и способ совершения. Особенности компьютерных преступлений в том, что совершаются они с разными мотивами, иногда они сопровождаются местью, иногда злоумышленниками руководит корысть, а иногда хулиганство, интерес или даже самоутверждение.

Общая характеристика преступлений в сфере компьютерной информации позволяет сделать вывод о высокой опасности подобных деяний. Законодатель относит этот вид преступлений к категории «средней тяжести», но при определенных обстоятельствах нарушение может переходить в категорию «тяжких» и «особо тяжких», если злодеяние связано с продажей государственной информации спецслужбам других стран.

В связи с вышесказанным, на сегодняшний день очень остро стоит вопрос по раскрытию и расследованию преступлений в сфере компьютерной информации. В полной мере это относится к таким действиям, как осмотр места происшествия, осмотр компьютерной техники и документов [3].

Изменение жизненных реалий, развитие научно-технического прогресса неизбежно приводят к совершенствованию криминалистической техники при проведении осмотра и выемки предметов. Появляются новые объекты осмотра: электронные носители информации, аппараты сотовой связи. Это влечет за собой разработку новых методик и введение новых норм в процессуальное законодательство.

Задачи осмотра места происшествия в расследовании данной категории преступлений заключается в том, что необходимо обнаружить, зафиксировать и изъять специфические электронно-цифровые следы. От качества проведения данного следственного действия будет зависеть дальнейший ход сбора доказательств и расследования преступления [1, с. 34].

Одни из видов материальных следов – электронно-цифровые. Одной из особенностей данной категории следов является то, что они находятся на электронных носителях информации или передаются по проводным каналам связи или радиоканалам в виде электромагнитных сигналов. Отметим, что они не обладают такими свойствами как геометрическая форма, цвет, масса, запах и т.д.

При проведении осмотра описываются выявленные электронно-цифровые следы преступления, что достигается за счет изучения содержания электронных документов, а не материального носителя. Мы поддерживаем точку зрения ряда ученых, работающих в области уголовно-процессуального законодательства, которая заключается в том, что электронно-цифровые следы следует рассматривать в качестве электронных документов. Необходимо также отметить, что особенности следообразования в виртуальной электронно-цифровой среде значительно усложняют получение доказательств, которые будут отвечать вышеназванным требованиям, таким как относимость, допустимость и достоверность.

Можно выделить следующие группы следов рассматриваемой категории преступлений, которые могут быть обнаружены в ходе производства осмотра места происшествия:

1) материальные следы: следы пальцев рук; следы, указывающие на применение различных инструментов; следы, указывающие на вмешательства в компьютерную технику (установка дополнительных микросхем, и т.д);

2) электронно-цифровые следы, важность которых заключается в том, что они содержат основную информацию о способе совершения преступного деяния.

К таким следам относятся различные электронные документы, например, лог-файлы журналов и отчетов операционной системы и иных программ; файлы программного обеспечения, используемого преступниками для осуществления сканирования, модификации, копирования; данные телекоммуникационных сервисов, мессенджеров и т.д.

В ходе осмотра места происшествия следователя интересует информация, как правило, хранящаяся на каком-либо материальном носителе информации (в смартфоне и др.). Из этого следует, один носитель, интересующий следователя, информации заключает в себе два вида следов, с одной стороны, это материальные следы, с другой – электронно-цифровые следы преступления.

В данном случае такое техническое устройство, исходя из норм уголовно-процессуального законодательства, будет являться вещественным доказательством, а электронная информация будет приобретать такой вид доказательства, как электронное, основанное на электронных документах.

В некоторых случаях при осмотре места происшествия перед следователем возникает вопрос о том, что лицу, у которого изымается необходимая для расследования преступления электронная информация, и которая необходима для продолжения его работы, и в этом случае законодатель предоставляет следователю право по осуществлению копирования данной информации (п. 9.1 ст. 182 УПК РФ).

Также следует отметить, что обращение с подобными устройствами должно отвечать требованиям, предъявляемым как к вещественным доказательствам [5].

Непосредственный осмотр данных объектов требует особых познаний и тактических приемов. Хотелось бы отметить, что для субъектов проведения осмотра места происшествия необходимо владение минимальными знаниями в области применения таких приемов, что определяет его компетенцию в расследовании данной категории преступлений. Выбор наиболее эффективного приема производства осмотра зависит от каждой конкретной ситуации, но традиционно выделяют три этапа: подготовительный, рабочий и заключительный.

Именно на каждом этапе существуют свои следственные ситуации и алгоритмы их разрешения, которые необходимо регулярно дополнять и адаптировать к изменяющимся обстоятельствам преступной деятельности. На практике зачастую перед следователем возникает вопрос, связанный с тем, что информация, необходимая для расследования преступления, является труднодоступной для производства осмотра, например, она может находиться на удаленном сервере в сети Интернет. По указаниям специалистов, доступ к такой информации осуществляется по идентификационным данным, получение которых вызывает ряд организационных и технических сложностей и, не имея определенных познаний в этой области, необходима помощь специалиста и консультанта. Однако полагаем, что осмотр и изъятие информации правильнее осуществлять в ходе выемки или обыска.

При производстве осмотра места происшествия в некоторых случаях следователь не просто описывает увиденное на экране монитора, но и осуществляет открытие и осмотр каталогов, файлов, программ и иной информации в компьютерном устройстве, а также может проводить простые

диагностические действия, если он обладает техническими познаниями, в противном случае, эти действия может выполнять участвующий в осмотре места происшествия специалист.

Но для принятия такого решения следователю необходимо подумать, ведь на сегодняшний день техника достигла высоких вершин, и следственной практики известны случаи, когда открывая один файл, вся информация автоматически стирается, также возможны пароли. Что касается пароля, то известно, что согласно ч. 6 ст. 177 УПК РФ при осмотре места происшествия в помещении организации обязан присутствовать администратор, который должен сообщить пароли в интересах расследования уголовного дела, в противном случае делается соответствующая запись в протоколе осмотра места происшествия.

Мы согласны с утверждением, что подробный осмотр информации, содержащейся в компьютере, внесение изменений в нее и тем самым в осматриваемый объект правильнее производить в ходе другого следственного действия – обыска [2]. Это связано с тем, что уголовно-процессуальное законодательство Российской Федерации разрешает при производстве обыска вносить необходимые изменения в техническое устройство, что при осмотре места происшествия делать запрещено. Отметим, что все действия должны быть сделаны специалистом либо под его руководством.

Работа с информацией, хранящейся на компьютере, – процесс, требующий много времени, тем самым в подобных ситуациях, исходя из эффективности и рациональности, следователь производит выемку данного технического устройства, о чем делается соответствующая запись в протоколе осмотра места происшествия (ч. 3 ст. 177 УПК РФ).

Также нельзя забывать о том, что во время производства осмотра места происшествия все действия подлежат фиксации и тем самым, должны быть зафиксированы все изменения, происходящие внутри технического устройства. Исходя из анализа следственной практики, распространены случаи, когда в ходе осмотра места происшествия имеющая интерес для уголовного дела информация, хранящаяся на технических устройствах, была удалена с помощью специальных программ, и вопрос по ее восстановлению весьма проблематичен.

Заниматься вопросом восстановления необходимо после осмотра места происшествия, фиксируя произошедшее в протоколе и изымая данное техническое устройство, соблюдая правила уголовно-процессуального законодательства Российской Федерации. В дальнейшем следователь назначает экспертизу. На сегодняшний день существует такое понятие, как облачное хранилище, которое хранит в себе различные файлы с интересующей следователя информацией. Осмотр такой компьютерной информации иногда оформляется как осмотр места происшествия, несмотря на то что происходит в служебном кабинете следователя с использованием служебной компьютерной техники [4].

При возникновении таких случаев, на наш взгляд, следователь не допускает процессуальной ошибки, осуществляя свои действия в рамках осмотра места происшествия, так как сетевое виртуальное пространство едино.

Как с теоретической, так и с практической стороны данное пространство является местом происшествия, осмотр которого будет производиться с привлечением специалиста и использованием специальных технических устройств. Особенность данного осмотра места происшествия заключается в том, что все действия и все явления должны быть зафиксированы, а для этого лучше использовать технические средства.

В заключение следует акцентировать внимание на необходимости внесения изменений в уголовно-процессуальное законодательство Российской Федерации, в части расширения перечня полномочий следователя при производстве осмотра места происшествия по преступлениям, совершаемым в сфере компьютерной информации ввиду всех рассмотренных в статье особенностей.

Список литературы

1. **Иванов Д. А.** Роль участников уголовного судопроизводства в реализации механизма возмещения вреда, причиненного преступлением, в досудебном производстве по уголовным делам // Вестник Московского университета им. С. Ю. Витте. Сер. 2: Юридические науки. 2015. № 1 (6). С. 33 – 36.
2. **Оконенко Р. И.** К вопросу о правомерности осмотра компьютера как следственного действия // Адвокат. 2015. № 1. С. 27 – 30.
3. **Протасевич А. А., Зверянская Л. П.** Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45 – 47.
4. **Стельмах В. Ю.** Современные проблемы фиксации хода и результатов производства следственных действий и возможные пути их решения // Актуальные проблемы российского права. 2016. № 7. С. 152 – 159.
5. **Хатунцев Н. А.** О специальных знаниях, необходимых при исследовании компьютерных средств и систем // Актуальные проблемы российского права. 2010. № 1. С. 332 – 339.

References

1. **Ivanov D.A.** [The role of participants in criminal proceedings in the implementation of the mechanism for compensation for harm caused by a crime in pre-trial criminal proceedings], *Vestnik Moskovskogo universiteta im. S.Yu. Vitte. Ser. 2: Yuridicheskiye nauki* [Bulletin of Moscow University. S. Yu. Witte. Ser. 2: Jurisprudence], 2015, no. 1(6), pp. 33-36. (In Russ.).
2. **Okonenko R.I.** [On the issue of the lawfulness of inspection of a computer as an investigative action], *Advokat* [Lawyer], 2015, no. 1, pp. 27-30. (In Russ.).
3. **Protasevich A.A., Zveryanskaya L.P.** [Forensic characteristics of computer crimes], *Rossiyskiy sledovatel'* [Russian investigator], 2013, no. 11, pp. 45-47. (In Russ.).
4. **Stel'makh V.Yu.** [Modern problems of fixing the course and results of investigative actions and possible ways to solve them], *Aktual'nyye problemy rossiyskogo prava* [Actual problems of Russian law], 2016, no. 7, pp. 152-159. (In Russ.).
5. **Khatuntsev N.A.** [On special knowledge required in the study of computer tools and systems], *Aktual'nyye problemy rossiyskogo prava* [Actual problems of Russian law], 2010, no. 1, pp. 332-339. (In Russ.).

Features of Inspection of the Scene of Cybercrime as an Element of Evidence

A. M. Popov, *Candidate of Law, Associate Professor, Head of Department of Security and Law and Order, Tambov State Technical University, Tambov, Russia; pamtambov@yandex.ru*

A. I. Dubovitsky, *Research Associate, Department of Organization of Scientific, Editorial and Publishing Work, V. Ya. Kikot Moscow University of the Ministry of internal Affairs of Russia, Moscow, Russia; adubovitckii5@mvd.ru*

The article focuses on the peculiarities of inspection in criminal cases of crimes in the field of computer information. It is noted that inspection in the investigation of this category of crimes aims at detection, recording and removal of specific electronic and digital evidence. The authors justify the need to make changes to the criminal procedure legislation of the Russian Federation, in terms of expanding the list of powers of the investigator during the inspection of the scene of the incident for crimes committed in the field of computer information.

Keywords: cybercrimes; inspection of the scene; inspection of items and documents; preliminary investigation; process of proof.

Статья поступила в редакцию 12.02.2020

При цитировании использовать:

Попов А. М., Дубовицкий А. И. Особенности производства осмотра по преступлениям в сфере компьютерной информации как элемент доказывания // Право: история и современность. 2020. № 1(10). С. 109 – 115. doi: 10.17277/pravo.2020.01.pp.109-115