УДК 343.140.02

С.*В. Зуев, Д.В. Овсянников**

КОПИРОВАНИЕ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ В ТЕОРИИ И ПРАКТИКЕ УГОЛОВНОГО ПРОЦЕССА

В статье рассматриваются проблемы копирования электронной информации в уголовном процессе. Такой познавательный прием может сегодня применяться в ходе обыска, выемки или осмотра, а также заслуживает признания в качестве самостоятельного следственного действия. К сожалению, действующее уголовно-процессуальное законодательство не отвечает требованиям развития современных телекоммуникационных отношений. Это в полной мере относится и к копированию электронной информации. Изъятие и копирование электронной информации – два относительно автономных познавательных приема, которые при определенных условиях могут быть последовательными и конкурентными относительно друг друга. При копировании электронной информации так же, как и при изъятии ее носителей, обязательно участвует специалист.

***Ключевые слова**:* информация, уголовный процесс, электронное копирование, теория, практика, обыск, выемка, осмотр.

Массовыми и наиболее прибыльными видами преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, являются мошенничества и кражи денежных средств со счетов физических лиц и организаций. Так, в 2012 году подразделениями «К» МВД России на всей территории страны зарегистрировано 3 645 подобных преступлений, тогда как в 2011 году их было 2123 [1]. Компьютерные системы становятся частью самых разнообразных сфер жизнедеятельности общества, а потому использование современных технологий с противоправными целями уже давно вышло за рамки составов компьютерных преступлений. Так, они используются для проектирования и изготовления фальсифицированных документов, денежных знаков, печатей, для создания и хранения баз данных при мошенничестве, лжепредпринимательстве и иных видах преступных деяний. Особому криминальному влиянию подвергнута финансово-кредитная система. Применение современных компьютерных технологий получает все большее распространение в качестве средств совершения и сокрытия различных видов преступлений.

Копирование электронной информации как познавательный прием используется в доказывании по уголовным делам. На сегодня оно проводится в рамках обыска, выемки или осмотра. Анализ следственной и судебной практики показывает, что во

Зуев Сергей Васильевич (zuevsergej@inbox.ru), кафедра уголовно-правовых дисциплин Южно-Уральский государственный университет, 454081, г. Челябинск, ул. Артиллерийская, 100.

Овсянников Дмитрий Васильевич (dvo-chel@mail.ru), представительство таможенной службы Российской Федерации в Республике Казахстан, 454021, Республика Казахстан, г. Челябинск.

многих случаях копирование такой информации может быть востребовано как самостоятельное средство уголовно-процессуального доказывания. Имеются в виду такие ситуации, когда следователя, дознавателя или суд интересует только электронная информация, и нет необходимости проводить полномасштабный обыск, выемку или осмотр будь то жилище, помещение или физическое лицо. При этом проверка допустимости использования доказательств по результатам электронного копирования требует особого внимания.

Так, например, 4 декабря 2008 года в вечернее время гр. В. и П. группой лиц совершили убийство гр. С. При этом гр. Д. оказал им в этом пособничество. Челябинский областной суд вынес обвинительный приговор. Помимо других доказательств в материалах уголовного дела имеется протокол осмотра предметов от 30 декабря 2008 года, согласно которому наряду с другими предметами был осмотрен сотовый телефон Самсунг SGH-D 840. В ходе просмотра и прослушивания содержащихся на данном телефоне файлов обнаружен файл SM-007. Данный файл содержит в себе фрагмент совершаемого в отношении С. преступления. Этот файл, согласно записи в протоколе, был изъят из осматриваемого телефона путем копирования на память жесткого диска персонального служебного компьютера. Из текста протокола следует, что осмотр предметов производился в присутствии понятых, протокол удостоверен их подписями. Сведений о том, что во время осмотра предметов воспроизводился скопированный с телефона файл SM-007, в протоколе не имеется. Вместе с тем к протоколу приобщена распечатка, согласно которой во время осмотра предметов на персональном компьютере следователем с помощью программы «ACDSee 8» был воспроизведен скопированный с телефона файл SM-007. Установлено, что данный файл представляет собой цифровую аудиозапись, на которой слышны мужские голоса. Приведено содержание аудиозаписи. Однако данное приложение не заверено подписями понятых, в связи с чем у суда возникли сомнения по поводу их участия при воспроизводстве вышеуказанной аудиозаписи. Кроме того, граждан с указанными фамилиями, значащихся в качестве понятых, в г. Челябинске установить не представилось возможным. В связи с чем на основании п. 3 ч.2 ст. 75 УПК РФ суд признал распечатку к протоколу осмотра предметов от 30 декабря 2008 года недопустимым доказательством [2].

Предложения об обособлении копирования электронной информации в качестве самостоятельного следственного действия поступали и ранее [3]. Такое заявление отдельные авторы основывали на различиях в фактической природе обыска, выемки, осмотра с одной стороны и электронного копирования информации – с другой. В.А. Семенцов, поддерживая эту идею в целом, пишет: «... в практике расследования возникает необходимость электронного копирования информации, и этот новый познавательный прием соответствует требованиям закона, морали и социальным закономерностям общественного развития. Необходимо только включить электронное копирование в систему процессуальных действий, предназначенных для собирания доказательств» [4, с. 36].

Действительно, развитие компьютерной и иной электронной техники, а также ее широкое внедрение в различные сферы человеческой деятельности вызвало рост числа противоправных действий, объектом и орудием совершения которых являются электронные носители информации. Прежде всего, это относится к компьютерной техники, однако спектр электронных носителей информации на сегодня гораздо шире.

Расследование таких преступлений имеет свои особенности. В обязательном порядке проводятся осмотры мест происшествия и обыски, направленные на обнаружение и изъятие следов преступления. Существует два способа получения такой информации: 1) изъятие всех обнаруженных средств компьютерной и иной техники с последующим изучением имеющейся на ней информации; 2) изучение всей информации

на электронных носителях непосредственно во время проведения осмотра или обыска. Последний вариант предполагает последующее копирование информации, представляющей интерес для уголовного дела и (или) изъятие магнитных носителей только с такой информацией.

Изъятие всех средств компьютерной техники ускоряет сам процесс расследования, дает возможность направить все силы на поиск иных материальных следов, имеющих отношение к преступлению (документы, технические средства и т. д.); снижает психологическую нагрузку на граждан; не требует привлечения высококвалифицированного специалиста в области компьютерных технологий к непосредственному участию в обыске, так как грамотное изъятие средств компьютерной техники вполне доступно и специалисту средней руки. К несомненным достоинствам такого подхода можно отнести и возможность в последующем более детально, привлекая необходимых специалистов, изучить всю информацию, имеющуюся в памяти компьютера. Это практически исключает возможность пропустить даже профессионально скрытую информацию. Однако с другой стороны, в ряде случаев существуют чисто технические сложности изъятия всех средств компьютерной техники (объединение в разнообразные сети, возможность потери информации при отключении и т. п.) или такое изъятие просто нецелесообразно. Также следует помнить, что выход из строя компьютерных систем банков и ряда предприятий может привести к полной дезорганизации их работы и значительным материальным убыткам, что грозит претензиями пострадавших организаций. Поэтому иногда рекомендуется применять второй способ: изъятие информации со средств компьютерной техники непосредственно в ходе проведения осмотра или обыска [5, с. 18]. И здесь не обойтись без электронного копирования информации с использованием переносного компьютера, накопители USB-флеш и т. п.

Копирование электронной информации может иметь место так же в случаях: 1) когда владелец электронного носителя информации является потерпевшим или свидетелем, который не заинтересован или возражает относительно изъятия у него видеорегистратора, видеокамеры и других средств личного пользования; 2) когда электронный носитель был изъят и его владелец ходатайствует о его возвращении.

Возникает вопрос, правомерно ли считать копирование электронной информации составной частью осмотра, обыска и выемки. Некоторые авторы считают, что можно выделить новый вид обыска – обыск средств компьютерной техники [6, с. 12]. Однако, представляется, что для ответа на поставленный вопрос, необходимо рассматривать не своеобразие тактики проводимых действий или применяемых технических средств, а природу копирования информации, находящейся в компьютере, и сравнивать ее со спецификой указанных следственных действий.

Новыми следственными действия, по мнению С.А. Шейфера, могут стать лишь приемы, которые соответствуют: а) общим принципам уголовного судопроизводства как системы более высокого уровня; б) общим принципам функционирования системы, т. е. являются оригинальными, приспособленными к достижению специфической цели приемами отображения следов [6, с. 90]. И это вполне справедливые требования.

Копирование – это процесс получения копий. Копирование электронной информации осуществляется с использованием магнитных лент, а также гибких и жестких дисков. Независимо от типа и емкости они используют один и тот же принцип долговременного хранения информации в виде намагниченных участков поверхности накопителя. При движении мимо них считывающего устройства в нем возбуждаются импульсы тока. Данные всегда записываются на магнитной поверхности в виде концентрических окружностей, называемых дорожками. Каждая дорожка в свою очередь состоит из нескольких секторов. Количество информации зависит от числа дорожек (называемого плотностью) и общего размера секторов на одной дорожке. Плотность

может существенно меняться от диска к диску. Высокая плотность достигается за счет особых свойств магнитного покрытия [8, с. 98, 102].

Таким образом, копирование электронной информации представляет собой процесс создания намагниченных участков поверхности накопителя за счет использования электромагнитного поля. Здесь нет момента передачи физических объектов, что так характерно для производства обыска или выемки (ст. 182-184 УПК РФ). Кроме того, процессу копирования информации, как правило, предшествует активный поиск информации, находящейся в базе данных персонального компьютера, что также вряд ли соответствует специфике осмотра.

Осмотр местности, жилища, предметов и документов производится в целях обнаружения следов преступления (ст. 176 УПК РФ). Такой осмотр предполагает собой поверхностный обзор указанных объектов и исключает активные внутрипоисковые мероприятия. Кроме того, согласно ч. 1 ст. 177 УПК РФ осмотр места происшествия предполагает лишь изъятие предметов, что, как было нами отмечено, не соответствует характеру производимых действий при электронном копировании информации. При осмотре же предметов законом не предусмотрено ни изъятие, ни копирование, ни производство других каких-либо подобных действий.

Кроме того, в настоящее время копирование электронной информации в организациях и учреждениях может повлечь за собой раскрытие тайны личной переписки и другой информации, касающейся частной жизни граждан. В такой ситуации потребуется судебное решение, тогда как обыск и выемка в помещении того не требует. Возникшее противоречие может привести к нарушению прав граждан, неуважению их чести и достоинства.

К обыску, выемки и осмотру наиболее близок такой познавательный прием, как изъятие электронных носителей информации, который наряду с копированием информации предусмотрен уголовно-процессуальным законом. Изъятие и копирование электронной информации – два относительно автономных познавательных приема, которые при определенных условиях могут быть последовательными и конкурентными относительно друг друга. Изъятие электронных носителей информации вряд ли может претендовать на самостоятельное следственное действие, так как по природе своей схоже с обыском и выемкой.

Однако на практике в некоторых случаях встречаются некорректные формулировки, например, *изъятие видеозаписи с видеорегистратора автомобиля* [9]. В данном случае должно было иметь место или копирование видеозаписи или изъятие видеорегистратора. В литературе также можно встретить предложение о введении в УПК РФ нормы, регламентирующей выемку компьютерной информации из компьютерной сети [10, с. 99], что также выглядит, по нашему мнению, как минимум некорректно. Информацию нельзя изъять, ее можно скопировать, а изъятию подлежит носитель информации.

Исходя из вышеизложенного, можно констатировать, что копирование электронной информации в силу специфики природы этого явления следует рассматривать как самостоятельное следственное действие, которое необходимо закрепить в УПК РФ. Предложение о придании самостоятельного следственного значения такого копирования информации не является единственным в этом роде. Многие исследователи сетуют по поводу отсутствия уголовно-процессуальной регламентации возможности, порядка и особенностей использования таких средств [11, с. 224; 12].

Копирование электронной информации может рассматриваться как познавательный прием, выполняемый в рамках проведения обыска, выемки или осмотра, а также заслуживает признания в качестве самостоятельного следственного действия и как элемент нового следственного действия. Для реализации этой идеи необходимо в действующий уголовно-процессуальный закон внести соответствующие дополнения.

Библиографический список

1. Материалы 15-го Национального форума информационной безопасности «Инновационные решения для безопасности России». URL: http://mvd.ru/news/item/830615 (дата обращения: 12.08.2014).

2. Уголовное дело № 2-25/2010. Архив Челябинского областного суда.

3. Зуев С.В., Сутягин К.И. Электронное копирование информации как самостоятельное следственное действие // Следователь. 2003. № 4. С. 14–15.

4. Семенцов В.А. Следственные действия в досудебном производстве (общие положения теории и практики): монография. Екатеринбург. 2006. С. 300 с.

5. Исаева Л. Обыск: роль специалиста // Законность. 2001. № 6. С. 17–21.

6. Комиссаров В., Гаврилов А., Иванов А. Обыск с извлечением компьютерной информации // Законность. 1999. № 3. С. 12–15.

7. Шейфер С.А. Проблемы развития системы следственных действий в УПК РФ // Уголовное право. 2002. № 3. С. 90–91.

8. Нортон П. Персональный компьютер фирмы IBM и операционная система MS-DOS: пер. с англ. М.: радио и связь, 1991. 415 с.

9. Уголовное дело № 10-368/2014. Архив Челябинского областного суда.

10. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. 416 с.

11. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.

12. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005. С. 18–20.

References

1. Proceedings of the 15th National forum of information security «Innovative solutions to Russia's security». Retrieved from: http://mvd.ru/news/item/830615/ (accessed 11.09.2014) [in Russian]

2. Criminal case № 2-25/2010. Archive of Chelyabinsk regional court [in Russian]

3. Zuev S.V., Sutyagin K.I. Electronic reproduction of information as an independent investigative action. *Sledovatel'* [*Investigator*], 2003, no. 4, pp. 14–15 [in Russian]

4. Sementsov V.A. Investigative actions in pre-trial proceedings (general provisions of theory and practice): monograph. Ekaterinburg, 2006, p. 36 [in Russian]

5. Isaeva L. The search: the role of specialist. *Zakonnost'* [Legality], 2001, no. 6, p. 17 – 21 [in Russian]

6. Commissarov V., Gavrilov A., Ivanov A. Search with the recovery of the computer information, *Zakonnost* [Legality], 1999, no. 3, p. 12–15 [in Russian]

7. Shafer S. Problems of development of the system of investigative actions in the Criminal Procedure Code of the Russian Federation. *Ugolovnoe pravo* [*Criminal Law*], 2002, no. 3, pp. 90-91 [in Russian]

8. Norton P. Personal computer of the IBM firm and the operating system MS-DOS. Translated from English. M., radio i sviaz', 1991, 415 p. [in Russian]

9. Criminal case № 10-368/2014. Archive of Chelyabinsk regional court [in Russian]

10. Rossinskaya E.R., Usov A.I. Trial computer forensic expertise. M., Pravo i zakon, 2001, 416 p. [in Russian]

11. Volevodz A.G. Countering cybercrime: legal foundations of international cooperation. M., Iurlitinform, 2002, 496 p. [in Russian]

12. Krasnova L.B. *Komp'iuternye ob»ekty v ugolovnom protsesse i kriminalistike: avtoref. dis. ...kand. iurid. nauk* [Computer objects in the criminal process and criminalistics: Extended abstract of Candidate's of Law thesis]. Voronezh, 2005, pp. 18-20 [in Russian]

S.V. Zuev, D.V. Ovsyannikov*

COPYING OF ELECTRONIC INFORMATION IN THE THEORY AND PRACTICE OF CRIMINAL PROCEDURE

The article deals with the problem of copying electronic information in criminal proceedings. This educational method can now be used in the process of search, seizure or inspection, and deserves to be recognized as an independent investigating action. Unfortunately, acting criminal procedure legislation does not meet the requirements of development of modern telecommunication relations. This is to the full extent refers to the copying of electronic information. Seizure and copying of electronic information are two relatively autonomous cognitive receptions, which under certain conditions may be consistent and competitive with respect to each other. When copying electronic information as well as when withdrawal of its carriers, a specialist is necessarily involved.

Key words: information, criminal process, electronic copying, theory, practice, search, seizure, inspection.

* *Zuev Sergey Vasilievich* (zuevsergej@inbox.ru), Department of Criminal and Legal disciplines, South Ural State University (National Research University), Chelyabinsk, 454081, Russian Federation.

Ovsyannikov Dmitry Vasilievich (dvo-chel@mail.ru), representative office of the customs office of the Russian Federation in the Republic of Kazakhstan, Chelyabinsk, 454021, Republic of Kazakhstan.