ЭЛЕКТРОННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

ELECTRONIC INFORMATION CARRIERS IN CRIMINAL PROCEEDINGS



УДК 343.3/.7

Васильков Егор Дмитриевич, магистрант, Крымский филиал Российского государственного университета правосудия, г.Симферополь

Vasilkov E. D. okumyra@gmail.com

Аннотация

Исследование посвящено рассмотрению значимости электронных носителей информации в уголовном судопроизводстве. Произведет всесторонний анализ нормативной базы регулирующей порядок использования и оценки электронных носителей информации в уголовном судопроизводстве. Установлена проблематика относительно темы исследования. Так же, Автором выдвинуты предложения по усовершенствованию законодательства, регулирующего электронные носителей информации в уголовном судопроизводстве.

Annotation

The study is devoted to the consideration of the importance of electronic media in criminal proceedings. Will make a comprehensive analysis of the regulatory framework governing the use and evaluation of electronic media in criminal proceedings. The problems concerning the research topic are established. The author also put forward proposals to improve the legislation regulating electronic media in criminal proceedings.

Ключевые слова: уголовное право; уголовное судопроизводство; электронные носители информации, цифровые доказательства, кибербезопасность.

Keywords: criminal law; criminal proceedings; electronic media, digital evidence, cybersecurity.

Электронные носители информации являются одни из первоочередных средств и инструментов, посредством которых совершаются преступления в интернете. Если обратиться к положениям норм федерального закона № 143-ФЗ[1], то можно увидеть, что в нем впервые на законодательном уровне были закреплены ключевые аспекты проведения следственных действий и мероприятий, в результате которых происходит изъятие электронных носителей информации. Так, в уголовно-процессуальном законодательстве[2] появилась возможность изъятия электронных носителей информации для проведения следственных действий.

К сожалению, до сих пор на законодательном уровне понятие электронного носителя информации не определено, Но в положениях п. 3.1.9. ГОСТ 2.051-2013[3] говорится о том, что под электронными носителями информации следует понимать определённый материальный носитель, с помощью которого может обрабатываться, храниться, передаваться и воспроизводится какая-либо информация.

Проблема данном случае заключается не только в том, что на федеральном уровне до сих пор не определено понятие электронного носителя информации, но и в том, что определение, данное в ГОСТ 2.051-2013 является чрезмерно широким, и под него логически обоснованно попадает практически

[1]О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 28 июля 2012 г. № 143-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 3 июля 2012 г. // Собр. законодательства Рос. Федерации. - 2012. - № 31, ст. 4332.

[2]Уголовно-процессуальный кодекс Российской Федерации от 18 дек 2001 г. № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г. // Собр. законодательства Рос. Федерации. - 2001. - № 52, ст. 4921.

[3]ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения. URL: http://www.consultant.ru (дата обращения: 20.04.2021).

любая микропроцессорная техника, в том числе, например, телевизор, стиральная машина, микроволновая печь и пр. По мнению Б. В. Вехова[4] данный подход законодателя является совершенно неприемлем, и в настоящий момент для целей более эффективного расследования преступлений с использованием информационных технологий требуется более точное и более детальное определение термина «электронный носитель информации».

Анализируя положения действующего российского уголовно-процессуального законодательства, можно прийти к выводу, что электронные носители информации признаются в качестве вещественных доказательств и могут быть приобщены к материалам уголовного дела в случае, когда они послужили орудием совершения преступления; в случае, если на них могли и (или) сохранилась следы преступления; в случае, если электронный носительинформации являлся предметом преступного посягательства; при условии, что электронный носитель информации мог служить средством для обнаружения преступления; в случае, если электронный носитель информации мог служить средством установления обстоятельств уголовного дела.

Действующее российское процессуальное законодательство устанавливает в положениях норм п. 4 ст. 81.1 УПК РФ максимальные сроки изъятия электронных носителей информации для проведения следственных мероприятий, которые равны пяти суткам.

Если обратиться к положениям норм абз «а» пп. 5 п. 2 ст. 82 УПК РФ, то можно увидеть, что электронные носители информации должны храниться в правоохранительных органах в опечатанном виде; с соблюдением условий, при которых должна быть исключена возможность ознакомления посторонних лиц с содержащейся на них информацией; а также с соблюдением условий, при которых должна быть обеспечена сохранность, как самих электронных носителей, так и содержащейся на них информации.

Заметим, что по общему правилу положений норм абз. «б» пп. 5 п. 2 ст. 82 УПК РФ, послеосмотра и осуществления представителями

[4]Вехов Б. В. Электронные носители информации в криминалистике: монография. М., 2017. С. 139.

правоохранительных органов всех необходимых следственных действий электронные носители информации должны быть возвращены их законному владельцу. При этом, так же существуют и случаи исключения, когда такой возраст не происходит, поскольку это может привести к сложностям расследования преступления.

Если обратиться к положениям норм п. 2.1 ст. 82, то можно увидеть, что при соблюдении определенного перечня условий владелец электронного носителя информации, при невозврате ему данного носителя от правоохранительных органов, может ходатайствовать о копировании информации, находящейся на носителе.

Правомерность действий, связанных с копированием информации, должна подтверждаться наличием определённых условий, к которым в частности относятся[5]:

- наличие ходатайства владельца электронных носителей, которые были изъяты, о том, что данное лицо изъявляет желание скопировать имеющуюся на данных носителях информацию;

- следователем, ведущим соответствующее дело, должно быть принято уполномоченное решение по данному указанному выше ходатайству;

- копирование информации сэлектронных носителей, которые были изъяты, должно происходить уполномоченным сотрудником правоохранительных органов;

- копирование информации с электронных носителей, которые были изъяты, ни в коем случае не должно препятствовать расследованию преступления, совершаемого при помощи информационных технологий;

- копирование информации с электронных носителей, которые были изъяты, должно осуществляться с участием понятых.

[5]Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. М.: Академия управления МВД России, 2019. С. 85.

К сожалению, в практической деятельности при реализации указанных выше положений действующего российского уголовно-процессуального законодательства, могут возникать определенные трудности.

Во-первых, при осуществлении следственных действий и мероприятий, связанных с осмотром, обыском места происшествия, а также связанных с изъятием электронных носителей для целей расследованияпреступлений, совершаемых при помощи информационных технологий, достаточно сложно оценить объективность правомерности копируемой законным владельцем электронных носителей информации. В данном случае речь идет о том, что на этапе обыска и изъятия все обстоятельства совершенного преступления могут быть еще полностью не определены и не определенным может быть содержание копируемой информации в той части, насколько данная информация правомерна. Ведь, действительно, может сложиться ситуация, при которой скопированная владельцем электронного носителя информация на этапе обыска и изъятия данного носителя, может в дальнейшем использоваться данным владельцем для продолжения преступления. Например, речь может идти о распространении неправомерной информации другим участникам преступной группировки, об использовании данной скопированной информации для перевода денежных средств в оффшорные юрисдикции и тому подобное.

Помимо всего прочего, всегда существует риск того, что информация в процессе её копирования может быть испорчена, утрачена или стерта, что, безусловно, самым неблагоприятным образом отразиться на расследовании преступления совершаемого при помощи информационных технологий.

Из всего вышесказанного становится понятным, что на этапе производства следственных действий в процессе обыска и изъятия электронных носителей, копирование информации законным владельцем носителей с данных носителей является весьма сомнительным действием, как минимум препятствующим расследованию преступлений, а как максимум – способствующему дальнейшему совершению преступного деяния (речь идет о

случаях, когда скопированная информация и дальше используется для продолжения преступления или для совершения новых преступлений).

Во-вторых, на этапе производства следственных действий в процессе обыска и изъятия электронных носителей, копирование информации законным владельцем носителей с данных носителей, может занимать довольно длительные промежутки времени (речь идет об объемах информации, например, в 1 терабайт, когда копирование может длиться 7 часов). Как известно, для эффективного расследования преступлений особенно важна оперативность, чего нельзя сказать о данном варианте развития событий. В длительные промежутки времени при копировании информации, злоумышленники могут успеть совершить другие преступления, могут успеть скрыться, изменить IP-адреса или совершить какие-либо другие действия, которые усложнят поиск преступников.

В-третьих, на этапе производства следственных действий в процессе обыска и изъятия электронных носителей, не всегда представляется возможным определить действительного владельца данных носителей, в связи с чем правомерность копирования может оставаться под вопросом, поскольку копирование информации с изымаемых носителей разрешение может дать только владелец данных электронных носителей.

Перечисленные выше обстоятельства ставят под сомнение положения норм п. 2 ст. 164.1 УПК РФдействующего российского федерального уголовного законодательства, регламентирующего применение мер уголовной ответственности в сфере совершения преступлений с использованием информационных технологий. В частности речь идет об указанном в данной статье праве законного владельца изымаемых электронных носителей на получение копии изымаемой информации непосредственно в процессе следственных действий, что также находит отражение во взглядах некоторых видных исследователей в рассматриваемой области[6].

[6]Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. М.: Академия управления МВД России, 2019. С. 81.

Таким образом, исследование электронных носителей информации в уголовном судопроизводстве позволяет сделать следующие выводы.

Во-первых, до сих пор в законодательстве отсутствует легальное определение термину электронный носитель информации, а формулировка данного термина в ГОСТ 2.051-2013 является чрезмерно широкой, и под него попадает практически любая микропроцессорная техника. В связи с этим, рекомендуется пп. 5 п. 2 ст. 82 УПК РФ от 18.12.2001 № 174-ФЗ, посвящённый электронным носителям информации, дополнить новым абзацем следующего содержания:

- «электронный носитель информации – это материальное устройство, конструкция которого непосредственно предназначена для получения, хранения, обработки, передачи или копирования информации в таком виде, в котором данную информацию можно было бы использовать в вычислительных машинах, в информационно-телекоммуникационных сетях(включая сеть «Интернет») и информационных системах».

Во-вторых, рекомендуется исключить п. 2 (о возможности копирования информации владельцем электронного носителя информации при проведении следственных мероприятий) из текста ст. 164.1 УКПК РФ.

Литература

1. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 28 июля 2012 г. № 143-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 3 июля 2012 г. // Собр. законодательства Рос. Федерации. - 2012. - № 31, ст. 4332.
2. Уголовно-процессуальный кодекс Российской Федерации от 18 дек 2001 г. № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г. // Собр. законодательства Рос. Федерации. - 2001. - № 52, ст. 4921.
3. ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения. URL: http://www.consultant.ru (дата обращения: 20.04.2021).

4. Вехов Б. В. Электронные носители информации в криминалистике: монография. М., 2017. С. 139.
5. Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. М.: Академия управления МВД России, 2019. С. 85.

Literature

1. On Amendments to the Criminal Procedure Code of the Russian Federation: Feder. the law grew. Federal Law No. 143-FZ of July 28, 2012: adopted by the State Duma of the Russian Federation. Sobr. Ros. Of the Russian Federation on July 3, 2012 / / Sobr. zakonodatelstva Ros. The Federation. - 2012. - No. 31, article 4332.
2. Criminal Procedure Code of the Russian Federation of December 18, 2001 No. 174-FZ: adopted by the State Duma of the Federal Assembly of the Russian Federation. Sobr. Ros. Federation on November 22. 2001 / / Sobr. zakonodatelstva Ros. The Federation. - 2001. - No. 52, article 4921.
3. GOST 2.051-2013 Unified system of design documentation. Electronic documents. General provisions. URL: http://www.consultant.ru (date accessed: 20.04.2021).
4. Vekhov B. V. Electronic media in forensic science: monograph. M., 2017. P. 139.
5. Anosov A. B. the activity of the bodies of internal Affairs to combat crimes committed using information, communication and high technologies: textbook. M.: Akademiya upravleniya MVD Rossii, 2019. P. 85.