

Министерство науки и высшего образования Российской Федерации

**Федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт–Петербургский политехнический университет Петра
Великого»**

**Гуманитарный институт
Высшая школа «Юриспруденции и судебно–технической экспертизы»**

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

БАКАЛАВРА

**Проблемы электронной переписки в уголовно-процессуальном
доказывании**

Направление подготовки 40.03.01 «Юриспруденция»

Студент гр. 43821/8

Попов Евгений Михайлович

Санкт–Петербург

2018

Министерство науки и высшего образования Российской Федерации

**Федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт–Петербургский политехнический университет Петра
Великого»**

**Гуманитарный институт
Высшая школа «Юриспруденции и судебно–технической экспертизы»**

Работа допущена к защите
И.о. директора Высшей
школы «Юриспруденции и
судебно–технической
экспертизы»

_____ Д.А. Мохоров
_____ 2018 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
БАКАЛАВРА**

**ПРОБЛЕМЫ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ В УГОЛОВНО-
ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ**

по направлению 40.03.01 «Юриспруденция»

Выполнил
студент гр. 43821/8

Е.М. Попов

Научный руководитель
к.ю.н., доц. ВШ «ЮиСТЭ»

Н.А. Липский

Санкт–Петербург

2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1. ЭЛЕКТРОННАЯ ПЕРЕПИСКА КАК ДОКАЗАТЕЛЬСТВО В УГОЛОВНОМ ПРОЦЕССЕ	7
1.1. Понятие, сущность и правовой режим электронной переписки в уголовном процессе	7
1.2. Примеры использования в судебной-следственной практики по уголовным делам электронных переписок в качестве доказательств	18
2. СОБИРАНИЕ, ПРОВЕРКА, ОЦЕНКА И ЗАКРЕПЛЕНИЕ НОСИТЕЛЯ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ, КАК ДОКАЗАТЕЛЬСТВА	23
2.1. Следственные действия, направленные на сбор и проверку носителя электронной переписки для последующего закрепления и признания его вещественным доказательством	23
2.2 Особенности использования специальной криминалистической техники для извлечения и закрепления информации из электронных устройств	31
2.3. Получение электронных переписок посредством проведения оперативно-розыскных мероприятий	37
2.4. Правовые аспекты действий защитника, связанных с уголовно-процессуальным доказыванием в контексте работы с электронными переписками и ее носителями	47
3. ВАРИАНТЫ РАЗРЕШЕНИЯ ПРАВОВОГО ПРОБЕЛА, СВЯЗАННОГО С ЭЛЕКТРОННОЙ ПЕРЕПИСКОЙ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ.....	53
3.1. Применение аналогии закона	53
3.2. Внесение изменений в Уголовно-процессуальный кодекс Российской Федерации	58
ЗАКЛЮЧЕНИЕ	62
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	66
АННОТАЦИЯ. КЛЮЧЕВЫЕ СЛОВА	72

ВВЕДЕНИЕ

На сегодняшний день тема, связанная с электронной перепиской в уголовно-процессуальном доказывании, является актуальной, поскольку в связи с научно-техническим прогрессом и развитием техники сильно возросла роль электронных переписок в сфере межличностной коммуникации. Из этого следует, что люди, общаясь между собой, могут выбирать в качестве альтернативы электронную форму общения в виде электронных сообщений, которая в некоторых ситуациях более удобная чем словесная. Следует отметить, что при этом информационное содержание общения между людьми не изменилось, а именно, люди пишут электронные сообщения, передавая ту информацию, которую они хотят передать другому лицу, но в данный момент времени не могут или не хотят делать это в словесной форме. При этом в определенных ситуациях передача информации одним лицом другому лицу может являться подготовкой к совершению преступления, одним из действий объективной стороны совершенного преступления или же окончанным преступлением.

Вышеуказанное означает, что люди способны совершать преступления и готовиться к ним посредством написания и отправления электронных сообщений, а также рассказывать другим лицам о своих преступных намерениях в прямой или косвенной формах. Однако в Уголовно-процессуальном кодексе Российской Федерации содержится недостаточное правовое регулирование процесса доказывания в рамках работы с электронной формой сообщений.

Объектом исследования настоящей выпускной квалификационной работы является весь комплекс общественных отношений, связанных с уголовно-процессуальным доказыванием посредством использования электронной переписки.

Предметом исследования настоящей выпускной квалификационной работы являются проблемы, связанные с электронной перепиской в уголовно-процессуальном доказывании, судебная, следственная и

адвокатская практика, криминалистическая техника, оперативно-розыскная деятельность и результаты оперативно-розыскных мероприятий, научная литература, статьи и суждения практических работников.

Целью исследования настоящей выпускной квалификационной работы является анализ роли электронной переписки в уголовно-процессуальном доказывании и выбор решений, направленных на устранение проблем, вызванных несовершенством уголовно-процессуального законодательства Российской Федерации в контексте использования электронных переписок в доказывании.

Для достижения поставленной цели автор ставит перед собой ряд следующих задач:

- 1) Проанализировать доказательственное значение электронной переписки в уголовно-процессуальном доказывании, на примере анализа судебной практики по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их аналогов, мошенничеством, доведением до самоубийства;
- 2) Рассмотреть следственные действия, направленные на собирание и проверку носителя электронной переписки для последующего закрепления и признания его вещественным доказательством;
- 3) Проанализировать особенности использования специальной криминалистической техники для работы с электронными носителями, содержащими электронные переписки;
- 4) Проанализировать особенности уголовно-процессуального доказывания и сбора информации в результате оперативно-розыскной деятельности, связанной с электронными переписками;
- 5) Проанализировать правовые аспекты действий защитника, связанных с уголовно-процессуальным доказыванием в контексте работы с электронными переписками и ее носителями;
- 6) Выявить правовые проблемы, связанные с электронной перепиской в уголовно-процессуальном доказывании;

7) Определить возможные пути разрешения правовых проблем, связанных с электронной перепиской в уголовно-процессуальном доказывании.

Раскрытием данной темы в общем аспекте в своих научных статьях и монографиях занимаются Россинская Е.Р., Безлепкин Б.Т., Гармаев Ю.П., Галяшина Е.И., Багмет А.П. и другие.

Методологическую основу исследования составляет диалектический подход, позволяющий раскрыть проблему электронной переписки. В качестве основных научных методов в работе применялись сравнительно-правовой, социологический, логический, метод системного анализа, уголовно-процессуального изучения и обобщения, статистический и другие методы научного познания. В работе использовались как общий – диалектический метод познания, так и специальные методы: логический, сравнительно-правовой, а также системно-структурные методы и метод функционального анализа.

Нормативную базу исследования составили Конституция России, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, информационное законодательство и иные нормативные правовые акты.

Эмпирической базой исследования являются материалы судебной практики и статистические данные.

Теоретическая значимость исследования заключается в обосновании совокупности научно-практических предположений по совершенствованию законодательства.

Научная новизна исследования состоит в том, что данная выпускная квалификационная работа представляет собой комплексное исследование проблем теоретических и практических вопросов института электронной переписки в российском уголовно-процессуальном праве. Выводы и предложения могут быть использованы в практической деятельности следственных органов и органов дознания.

1. ЭЛЕКТРОННАЯ ПЕРЕПИСКА КАК ДОКАЗАТЕЛЬСТВО В УГОЛОВНОМ ПРОЦЕССЕ

1.1 Понятие, сущность и правовой режим электронной переписки в уголовном процессе

Электронная переписка и электронные сообщения являются разновидностью переписок, как формы межличностной коммуникации, осуществляемой посредством обмена текстовыми сообщениями. От классических писем они отличаются своей формой, а именно, электронные сообщения могут содержаться в памяти электронных устройств. Доступ к указанным сообщениям (перепискам) может быть организован посредством специального программного обеспечения, установленного на компьютеры и иные аналогичные мобильные устройства, к примеру, планшеты, или посредством сети Интернет через программу-браузер.

Согласно пункту 28 части 1 статьи 2 Федерального закона Российской Федерации «О связи», средствами связи являются технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи. Пункт 35 части 1 статьи 2 Федерального закона Российской Федерации «О связи» гласит, что любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам является электросвязью¹.

Под электронной связью, основанной на использовании электронных приборов и устройств, понимается технология передачи информации из одного места в другое в виде электрических сигналов, посылаемых по

¹ Собрание законодательства Российской Федерации. – 14.07.2003. - №28. - Ст. 2895.

проводам, кабелю, оптоволоконным линиям или без направляющих линий¹. Согласно части 2 статьи 2 Федерального закона Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» и пункту 2 раздела 1 Постановления Правительства Российской Федерации от 10 сентября 2007 г. N 575 «Об утверждении правил оказания телематических услуг связи» информационно-телекоммуникационная сеть — это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники^{2,3}. В указанном Постановлении Правительства России под телематическим электронным сообщением понимается одно или несколько сообщений электросвязи. Соответственно электронной или информационно-телекоммуникационной является сеть, предназначенная для передачи и получения информации посредством проводных и сотовых телефонов, компьютеров.

Таким образом, все компьютерные программы, компьютеры и мобильные устройства, которые будут упоминаться далее в настоящей работе являются средствами связи в контексте данного исследования. Все электронные сообщения и объекты, которые приложены к указанным сообщениям в цифровом виде относятся к вышеуказанному понятию электросвязи. К электронному сообщению может быть приложена любая видеозапись, аудиозапись, гипертекст, фотография и иной файл.

Учитывая важность сохранения информации, передаваемой по каналам электросвязи, для обеспечения безопасности государства был принят Федеральный закон Российской Федерации № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части

¹ Мальков С., Винокуров В. Квалификация сбыта наркотических средств, психотропных веществ или их аналогов с использованием электронных или информационно-телекоммуникационных сетей. // журнал «Уголовное право». М: Право. – 2014. - №4. С. 25

² Собрание Законодательства Российской Федерации. – 31.07.2006. - №31 (ч. №1). - Ст. 3448.

³ Там же. – 17.09.2007. - №38. - Ст. 4552.

установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». Данный законодательный акт предусматривает обязанность с 1 июля 2018 года операторов связи хранить в течение срока 6 месяцев на территории России текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео, иные сообщения¹.

По мнению доктора юридических наук, профессора, полковника полиции А.Л. Осипенко компьютерной информацией является информация, содержащаяся в особой форме и приспособленная к воспроизведению посредством компьютерной техники, передачи по каналам связи и хранения на специальных носителях. Здесь правильнее говорить не об информации, а о данных, которые становятся информацией только при их осмыслении путем помещения их в определенный контекст².

Рассматривая компьютерные программы и их компоненты, как средства связи, следует отметить, что прежде всего пойдет речь о программах-клиентах, таких как «Mail.ru Агент», «Skype», «WhatsApp» (мобильный мессенджер, который может быть установлен на портативный компьютер) и интернет-сайтах различных электронных почт, к примеру, «@mail.ru», «yandex.ru», «gmail.com», данные которых хранятся на специальных серверах. Большая часть современных программ мессенджеров позволяет хранить в постоянной памяти устройства электронные сообщения (кэш файлы). Там, где это невозможно, доступ к электронным сообщениям может быть получен только посредством сети Интернет, а в обычном режиме сообщения хранятся только в оперативной памяти компьютера, на котором открыта данная программа или интернет-страница и на серверах организаций, предоставляющих услуги электронной почты.

¹ Собрание законодательства Российской Федерации. – 11.07.2016. - №28. - Ст. 4558.

² Осипенко А.Л. Новое оперативно-розыскное мероприятий «Получение компьютерной информации»: содержание и основы осуществления. // Вестник Воронежского института МВД России. Воронеж: Издательство ВИ МВД России. – 2016. – №3 С. 83-90.

В пункте 2 Постановления Правительства Российской Федерации от 26.09.2000 «Об утверждении Правил оказания услуг почтовой связи» содержится определение отправления посредством электронной почты: «Сообщение, принимаемое от отправителя на бумажном или магнитном носителе, передаваемое электронным путем на расстояние, определяемое структурой и возможностями технических и сетевых средств, и доставляемое адресату воспроизведенным в физической или электронной форме»¹.

М.В. Гаврилов в своей статье «Наложение ареста на электронную почту, ее осмотр и выемка» поясняет, что классическая почта является одним из видов связи. По аналогии можно определить электронную почту, как вид электросвязи, перемещающий сообщения, пересылаемые в цифровой форме с помощью компьютерных устройств, программных средств, сетевых технологий и предприятий по оказанию сетевых услуг (провайдеров сети)².

Также согласно Постановлению Правительства Российской Федерации от 26.09.2000 «Об утверждении Правил оказания услуг почтовой связи» электронные переписки являются электросвязью¹.

Отдельного внимания стоит уделить «гигантам» межличностной коммуникации в сети Интернет – социальным сетям. Социальные сети представляют собой веб-сайты, которые предназначены для построения, отражения и организации социальных взаимоотношений в сети Интернет. Переписки в социальных сетях можно разделить на 2 вида: открытые (размещение комментариев под отдельными записями в группах (сообществах) социальных сетей) и закрытые (переписки, построенные путем обмена сообщениями между аккаунтами пользователей социальной сети в режиме личных сообщений, которые недоступны иным пользователям социальной сети). На сегодняшний день крупнейшими социальными сетями являются «facebook», «twitter», «ВКонтакте», «Одноклассники». В контексте данного исследования переписки открытого типа не представляют интерес,

¹ Собрание законодательства Российской Федерации. – 09.10.2000. - №41. - Ст. 4076.

² Гаврилов М.В., Иванов А.Н. Наложение ареста на электронную почту, ее осмотр и выемка. // журнал «Правоведение. Политология». М: Наука. – 2014. – №5 С. 105.

так как в данном случае люди, общающиеся между собой, осознанно и целенаправленно выставляют на показ не ограниченному кругу лиц сообщения в комментариях, которые адресуют друг другу.

В настоящее время имеется большой выбор различных мессенджеров и клиентских приложений социальных сетей (программ, позволяющих открывать доступ к социальным сетям напрямую, минуя загрузку интернет-браузера) для различных электронных мобильных устройств (смартфонов, планшетов) и персональных компьютеров. Электронные сообщения, содержащиеся в «мессенджерах», хранятся в постоянной памяти мобильного устройства среди файлов соответствующей программы. Электронные сообщения, отправляемые посредством клиентских приложений (программ), установленных на мобильные устройства в основном хранятся в оперативной памяти этих мобильных устройств (в момент доступа) и на серверах социальных сетей¹.

Все вышеизложенное свидетельствует о том, что электронные сообщения, пересылаемые между абонентами посредством электронных средств связи, являются такими же переписками, как письма, пересылаемые посредством классической почты (ФГУП «Почта России»), а значит на них также распространяется правило о тайне переписки. Согласно части 2 статьи 23 Конституции Российской Федерации каждый гражданин имеет право на тайну переписки, почтовых, телеграфных и иных сообщений, ограничение указанного права допускается только на основании решения суда².

В уголовно-процессуальном законодательстве, иных законах и нормативных правовых актах содержатся правовые нормы аналогичные по содержанию вышеуказанным конституционно-правовым нормам. Часть 1 статьи 13 Уголовно-процессуального кодекса Российской Федерации гласит, что нарушение тайны переписки возможно лишь по решению суда.

¹ Шудрова. К. Интернет-мессенджеры: какое приложение обеспечит безопасность вашей переписки. Сайт газеты «Росконтроль». URK: <https://roscontrol.com/community/article/internet-messengeri-kakoe-prilogenie-obespechit-bezopasnost-vashey-perepiski/> (дата обращения 10.03.2018).

² Собрание законодательства Российской Федерации. – 04.08.2014. – №31. - Ст. 4398.

Часть 1 статьи 1 Уголовно-процессуального кодекса Российской Федерации предусматривает, что Уголовно-процессуальный кодекс Российской Федерации основывается на Конституции России, часть 7 статьи 185 Уголовно-процессуального кодекса России предусматривает, что осмотр и выемка электронных сообщений могут быть произведены следователем на основании решения суда¹. Согласно части 1 статьи 63 Федерального закона Российской Федерации «О связи», на территории России гарантируется тайна переписки, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами².

В соответствии с частью 1 статьи 73 Уголовно-процессуального кодекса России доказательствами являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела³.

По мнению Ю.М. Новолодского, подход законодателя к определению доказательства не выдерживает критики, поскольку «любые сведения» не должны являться доказательствами по уголовному делу. Доказательствами по уголовному делу должны являться сведения, объективно связанные с событием преступления, поскольку самыми плохими доказательствами являются те, в ходе исследования которых сложно проверить эту объективную связанность⁴. Поскольку без объективной связанности между доказательствами и фактами, устанавливаемыми с их помощью, тяжело проверить доказательства на достоверность.

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

² Там же. – 14.07.2003. - №28. - Ст. 2895

³ Там же. – 24.12.2001. - №52. - Ст. 4921.

⁴ Новолодский Ю.М. Школа уголовной защиты Юрия Новолаского. Путь к мастерству, первые стадии. // Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2017. – С.27.

Также Ю.М. Новолодский поясняет, что в указанной выше правовой норме отсутствует указание на участников уголовного судопроизводства со стороны защиты, несмотря на то, что уголовный закон предусматривает право последних на участие в доказывании. Данный недостаток применения законодательной техники пагубно сказался на практическом представлении концепции уголовно-процессуального доказывания в целом, так как некоторые ученые стали придерживаться мнения о том, что адвокат-защитник не может быть субъектом доказывания, а он только участвует в следственных действиях вместе с доверителем¹.

Анализируя электронные переписки в уголовно-процессуальном доказывании, следует определить в какой вид доказательств будет входить электронная переписка, поскольку статья 74 Уголовно-процессуального кодекса Российской Федерации содержит исчерпывающий перечень доказательств, куда не входит электронная переписка или электронное сообщение¹. В связи с этим электронная переписка может быть составной частью следующих доказательств: вещественных доказательств, протоколов следственных действий (протокол осмотра предметов или документов), иных документов. В качестве вещественного доказательства может быть любая электронная техника, позволяющая просмотреть электронную переписку и (или) на котором она сохранена в постоянной памяти или в оперативной памяти. Также возможен бумажный носитель с распечаткой, полученной от оператора связи или электронный носитель (магнитные накопитель или флэшка).

С практической точки зрения содержание электронной переписки в уголовном деле в качестве иного документа вряд ли возможно, так как согласно пункту 3 части 1 статьи 81 Уголовно-процессуального кодекса России вещественными доказательствами могут быть, в том числе, иные предметы и документы, которые могут служить средствами для обнаружения

¹ Новолодский Ю.М. Доказывание в практической деятельности адвоката-защитника. // Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2016. – С. 36

преступления и установления обстоятельств уголовного дела. Чтобы предмет или документ стал вещественным доказательством в соответствии с частью 2 статьи 81 Уголовно-процессуального кодекса России он должен быть изъят, осмотрен и признан вещественным доказательством на основании постановления следователя (дознавателя)¹. Данный аспект будет более подробно рассмотрен в следующем разделе настоящей работы.

В частях 1-6 статьи 185 Уголовно-процессуального кодекса Российской Федерации содержатся правовые нормы, которые посвящены наложению ареста, осмотру и выемке почтово-телеграфных отправлений, и только в 7 части содержится норма, посвященная электронным сообщениям: «При наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка». Таким образом, в указанной статье имеется группа специальных правовых норм, регулирующих указанные следственные действия с почтово-телеграфными отправлениями (относительно всех особенностей почтово-телеграфных отправлений) и одна специальная норма, которая относится к электронным сообщениям (не содержит никаких особенностей и нюансов, связанных с электронной формой сообщения). Такое правовое регулирование следственных действий с электронными сообщениями не совсем полное, поскольку данная норма не содержит никаких указаний на особенности ареста, если таковой возможен, изъятия и осмотра электронных переписок (сообщений), только обязывает получать судебное решение.

В судебно-следственной практике на сегодняшний день существует двоякое понимание электронных переписок (сообщений). Бывает их воспринимают, как некую составную часть, осматриваемого электронного устройства, например, мобильного телефона, и при таком подходе в ходе осмотра указанных электронных устройств обходятся без решения суда. Есть

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

обратный подход, согласно которому для использования электронных переписок и сведений, содержащихся в них в уголовно-процессуальном доказывании необходимо решение суда, поскольку это ограничивает право на тайну переписки¹. Второй подход следует считать наиболее правомерным.

Возможно это двоякое понимание держится на том, что в частях 1-6 статьи 185 Уголовно-процессуального кодекса России говорится про почтово-телеграфные отправления, а в части 7, указанной статьи, говорится только, что для наложения ареста, выемки и осмотра электронных сообщений нужно решение суда². Применительно к почтово-телеграфным отправлениям данная позиция законодателя грамотная и судебно-следственной практикой ее не исказить, поскольку почтово-телеграфные отправления действительно могут быть самостоятельными материальными объектами, которые нельзя подменить осмотром ноутбука или мобильного телефона. Однако электронные сообщения (переписки) могут быть самостоятельным объектом производства следственного действия только в определенных случаях. К примеру, изъятие распечаток электронных сообщений или копирование их на пустой магнитный носитель в организации, оказывающей услуги электронной почты или социальной сети. В остальных случаях электронные сообщения могут содержаться на электронном носителе, который скорее всего будет являться самостоятельным объектом следственного действия. В последней ситуации как раз наиболее вероятно подмена одного следственного действия другим, и, чтобы ликвидировать такую возможность, необходимо указание на прямой запрет, к примеру, на производство осмотра электронной переписки без решения суда, как составной части ее электронного носителя, то есть в рамках осмотра самого электронного носителя.

К примеру, Ленинский районный суд города Владивостока Приморского края в своем постановлении от 27.11.2014 отказал в

¹ Видеоблог адвоката Колегова А.В. «Адвокатские тайны»: «Исключение недопустимых доказательств». URL: <https://www.youtube.com/watch?v=HCX3IG5TyY4> (дата обращения 02.03.2018).

² Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

удовлетворении ходатайства следователя Следственного управления Следственного комитета Российской Федерации по Приморскому краю о разрешении производства осмотра электронных переписок, которые могли находиться на мобильных телефонах, изъятых в ходе обыска. Свое решение суд мотивировал тем, что уголовно-процессуальный закон не содержит правовых норм, предписывающих получение судебного разрешения на производство осмотра предметов (мобильных телефонов, планшетов, ноутбуков и иных), также указывает, что данные мобильные телефоны могли быть осмотрены и в ходе обыска. Далее суд сослался на смысл части 2 статьи 23 Конституции Российской Федерации и уголовно-процессуального закона пояснив, что судебное решение необходимо при производстве следственных действий для истребования информации, находящейся у оператора связи в целях обеспечения законности ее появления у соответствующего органа, осуществляющего уголовное преследование¹.

В данном примере содержится не правильное толкование судом правовых норм, которые были рассмотрены в данном параграфе. Возможно это вызвано указанием в части 5 статьи 185 Уголовно-процессуального кодекса Российской Федерации на то, что осмотр, выемка почтово-телеграфных отправлений осуществляются в соответствующем учреждении связи, так как суд в описательно-мотивировочной части указал на этот факт. Как уже говорилось выше эта правовая норма является специальной по характеру для почтово-телеграфных отправлений. К следственным действиям, объектом которых являются электронные переписки она может быть применена не непосредственно, а только посредством применения аналогии закона.

Конституционный Суд Российской Федерации в Постановлении от 26.10.2017 N 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о

¹ Постановление Ленинского районного суда города Владивостока № 22-455/14 от 27.11.2014 // РосПравосудие. - URL: <https://rospravosudie.com> (дата обращения 02.03.2018).

защите информации" в связи с жалобой гражданина А.И. Сушкова» указал, что на электронные переписки в полной мере распространяются правовые нормы о праве гражданина на тайну переписки¹.

По смыслу вышеприведенных правовых норм в настоящем подразделе следует считать необходимым решение суда для использования в доказывании электронных переписок наравне с классическими переписками (письмами), содержащимися на бумажном носителе. При отсутствии решения суда, разрешающего доступ к электронной переписки, доказательства, закрепляющие ее, должны быть признаны недопустимыми доказательствами полностью или в части (в случае, если в электронном устройстве содержится иная информация, которая представляет интерес для следствия и может быть использована без решения суда)¹. Данными доказательствами будут являться электронное устройство, к примеру, мобильный телефон, и протокол осмотра указанного устройства. К примеру, мобильный телефон, на котором в программе «WhatsApp» была обнаружена электронная переписка двух абонентов и ее содержание процитировано в указанном протоколе осмотра предметов. Данная проблема и пути ее решения будут всесторонне проанализированы в третьем разделе настоящей работы.

Таким образом, в настоящем подразделе была рассмотрена электронная переписка в уголовно-процессуальном доказывании, проанализирован ее правовой режим и формы, в виде которых она может содержаться (электронная техника, бумажные и электронные носители в виде флэшек, карт памяти и дисков).

¹ По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова: постановление Конституционного Суда России от 26.10.2017 N 25-П: офиц. текст по состоянию на 02.03.2018 // Российская газета. - № 259. – 16.11.

1.2 Примеры использования в судебно-следственной практике по уголовным делам электронных переписок в качестве доказательств

С практической точки зрения необходимо доказательственное закрепление связей и информации, которую передают друг другу лица, в том числе, посредством электронных сообщений, прежде всего, где имеются составы преступления, охватывающие собой, социальные связи, или, когда речь идет о таких признаках отягчающих уголовную ответственность, как совершение преступления группой лиц по предварительному сговору, организованной группы или в составе преступного сообщества, совершение преступления в целях пропаганды, оправдания и поддержки терроризма (пункты «в» или «р» части 1 статьи 63 Уголовного кодекса Российской Федерации). Следует подчеркнуть, что важным является также доказывание подготовки к совершению тяжкого или особо тяжкого преступления или покушение на совершение преступления в порядке частей 2 и 3 статьи 30 Уголовного кодекса Российской Федерации¹.

Стоит отметить, что законодатель посчитал использование средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») квалифицирующим признаком состава преступления, предусмотренного статьей 228.1 Уголовного кодекса Российской Федерации - незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества. Указанным признаком была дополнена часть 2 статьи 228.1 Уголовного кодекса Российской Федерации на основании Федеральным законом от 1 марта 2012 г. N 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»².

¹ Собрание законодательства Российской Федерации. – 17.06.1994. – №25. - Ст. 2954.

² Там же. – 05.03.2012. - №10. - Ст. 1166.

В настоящей работе будут рассмотрены примеры практического применения электронной переписки, как доказательства в уголовном процессе, на примере судебно-следственной практики по категориям уголовных дел, связанных с незаконным оборотом наркотических средств, психотропных вещества и их аналогов, мошенничеством, незаконного сбыта сильнодействующих веществ, доведением до самоубийства.

Согласно Апелляционному определению Судебной коллегии по уголовным делам Верховного Суда России от 17 октября 2013 г. N 50-АПУ 13-26 гражданка Сажина была признана виновной в совершении приготовления к сбыту наркотических средств с использованием информационно-телекоммуникационной системы «Интернет» по части 2 статьи 30 пункту «б» части 2 статьи 228.1 Уголовного кодекса Российской Федерации. Из указанного Апелляционного определения следует, что у гражданки Сажиной, не употреблявшей наркотические средства и задержанной во время ночной поездки на такси по городу, были изъяты наркотические средства в удобной для сбыта расфасовке, а в операционных системах системного блока ее компьютера, который был изъят в ходе обыска в ее квартире, обнаружены переписки Сажиной, содержащие информацию о распространении наркотических средств, в том числе адреса закладок¹.

В соответствии с приговором Северского районного суда Краснодарского края Makeev E.V. был признан виновным в совершении преступлений, предусмотренных частью 4 статьи 159 (мошенничество, совершенное лицом с использованием своего служебного положения в особо крупном размере), пунктом «а» частью 2 статьи 174.1 (сделки с иным имуществом, приобретённым лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанным иным имуществом, совершённые в крупном размере, группой лиц по предварительному сговору) и частью 3 статьи 159

¹ Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда России от 17 октября 2013 г. N 50-АПУ13-26 // РосПравосудие. - URL: <https://rospravosudie.com> (дата обращения 02.03.2018).

Уголовного кодекса Российской Федерации (мошенничество, совершенное в крупном размере). В указанном приговоре содержится ссылка на результаты производства выемки в помещениях, занимаемых компанией поставщиком услуг ООО «МЕЙЛ.РУ», в результате которой был изъят съемный электронный носитель компьютерной информации (CD-диск) с копией электронной переписки электронной почты аккаунта, которым пользовался Макеев Е.В. с третьими лицами. Это доказательство позволило доказать вину Макеева Е.В. в инкриминируемых ему преступлениях и привлечь его к уголовной ответственности¹.

Согласно приговору Вахитовского районного суда города Казани республики Татарстан по уголовному делу № 1-184/2014 от 06.05.2014 Бадриев А.Х. был признан виновным в совершении преступления, предусмотренного частью 3 статьи 234 Уголовного кодекса Российской Федерации - незаконный сбыт сильнодействующего вещества метандиенон в крупном размере. По данному уголовному делу судом было установлено, что гражданин Бадриев А.В. в ходе переписки в одной из социальных сетей с гражданином В., являющимся сотрудником УФСКН России по республике Татарстан, договорился о сбыте последнему сильнодействующего вещества. Впоследствии Бадриев А.В. сбыл указанное вещество сотруднику УФСКН России по республике Татарстан, участвующему в оперативно-розыскном мероприятии «проверочная закупка», и был задержан. Письменным доказательством по настоящему уголовному делу послужил протокол осмотра документов и скриншотов страниц социальной сети, в которых имеется переписка указанных лиц и обговариваются условия продажи сильнодействующего вещества. Это доказательство позволило доказать вину Бадриева А.В. в инкриминируемых ему преступлениях².

¹ Приговор Северского районного суда Краснодарского края от 24.06.2014 по уголовному делу № 1-175/10 // РосПравосудие. - URL: <https://rospravosudie.com/court-severskij-rajonnyj-sud-krasnodarskij-kraj-s/act-468893421> (дата обращения 03.03.2018)

² Приговор Вахитовского районного суда города Казани республики Татарстан от 06.05.2014 по уголовному делу № 1-184/2014 // РосПравосудие. - URL: <http://sudact.ru/regular/doc/WyavwZ7DR958/> (дата обращения 03.03.2018).

17.07.2017 Тобольским районным судом Тюменской области был вынесен обвинительный приговор по уголовному делу №1-51/2017 в отношении Филиппа Будейкина, известного в социальной сети «ВКонтакте» под никнэймом «Филипп Лис», по двум эпизодам признаков преступления, предусмотренного частью 3 статьей 30 статьи 110 Уголовного кодекса Российской Федерации, покушение на доведение до самоубийства двух несовершеннолетних девушек 16 и 17 лет¹.

Указанный приговор не был опубликован на сайте «РосПравосудие» и «ГАС правосудие», так как по данному уголовному делу потерпевшими являются несовершеннолетние лица. В соответствии с частью 2 пункта 5 статьи 15 Федерального закона России от 22.12.2008 N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» судебные акты по делам, затрагивающим права несовершеннолетних, не подлежат опубликованию в сети «Интернет»².

По информации органов Следственного комитета России Ф. Будейкин, используя свой аккаунт в социальной сети «ВКонтакте», посредством группы-смерти «Синий кит» в указанной социальной сети знакомился с несовершеннолетними лицами, которым давал различные задания, направленные на склонение несовершеннолетних к совершению суицида. В настоящее время органами Следственного комитета России многих субъектов Российской Федерации ведутся расследования по аналогичным уголовным делам. Данную информацию сообщают официальные представители Следственного комитета России³.

В настоящем параграфе были рассмотрены примеры из судебно-следственной практики по уголовным делам, в которых электронные сообщения являлись одними из основных доказательств стороны обвинения,

¹ Справка по приговору № 1-51/2017 от 17.07.2017 // Картотека судебного делопроизводства Тобольского районного суда URL: <https://tobolsky--tum.sudrf.ru/modules.php> (дата обращения 04.03.2018)

² Собрание законодательства Российской Федерации. – 29.12.2008. - №52 ст. (ч. 1). - Ст. 6217.

³ Официальный сайт «Вести.ру. ГТРК Санкт-Петербург»: СК завершил расследование уголовного дела администратора одной из «групп смерти». URL: <http://www.vesti.ru/doc.html> (дата обращения 04.03.2018).

так как они в полной мере отражали информацию, передаваемую путем межличностной коммуникации посредством электронных сообщений.

2. СОБИРАНИЕ, ПРОВЕРКА, ОЦЕНКА И ЗАКРЕПЛЕНИЕ НОСИТЕЛЯ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ, КАК ДОКАЗАТЕЛЬСТВА

2.1 Следственные действия, направленные на собирание и проверку носителя электронной переписки для последующего закрепления и признания его вещественным доказательством

В соответствии с частью 2 статьи 81 Уголовно-процессуального кодекса России в основе уголовно-процессуального доказывания лежат три обязательных стадии: собирание, проверка, оценка доказательств. Рассмотрим данные этапы в логической последовательности.

Необходимо отметить, что согласно части 2 статьи 50 Конституции Российской Федерации использование доказательств, полученных с нарушением федерального закона, при осуществлении правосудия не допускается¹. Часть 1 статьи 1 Уголовно-процессуального кодекса Российской Федерации гласит, что порядок уголовного судопроизводства на территории России урегулирован настоящим кодексом, основанным на Конституции России. В соответствии с частью 1 статьи 75 Уголовно-процессуального кодекса Российской Федерации доказательства, полученные с нарушением требований Уголовно-процессуального кодекса признаются недопустимыми, а значит не могут быть положены в основу обвинения и использоваться для доказывания любого из обстоятельств, предусмотренных статьей 73 Уголовно-процессуального кодекса Российской Федерации².

По смыслу Постановления Пленума Верховного Суда России «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением Конституционных прав граждан (статья 165 Уголовно-процессуального кодекса Российской Федерации)» для получения доступа к электронным перепискам и отдельным электронным

¹ Собрание законодательства Российской Федерации. – 04.08.2014. – №31. - Ст. 4398.

² Там же. – 24.12.2001. - №52. - Ст. 4921.

сообщениям органам предварительного расследования необходимо получить разрешение суда¹.

Статьями 182 и 183 Уголовно-процессуального кодекса Российской Федерации предусмотрены два однородных по правовому регулированию следственных действия – обыск и выемка. Их отличие состоит лишь в том, что обыск направлен на отыскание и изъятие любых предметов и документов, представляющих интерес для следствия, а выемка направлена на изъятие конкретного предмета или документа, когда известно, что указанный предмет или документ в данный момент времени находится в конкретном месте и (или) у конкретного лица. Обыск также может быть произведен с целью обнаружения разыскиваемых лиц, заложников и трупов, но эти аспекты не относятся к предмету настоящего исследования².

Важным моментом при обыске и выемке, которые проводятся с целью изъятия электронных носителей и иной компьютерной информации обязательно участие специалиста согласно части 9.1 статьи 182 Уголовно-процессуального кодекса Российской Федерации².

А.М. Багмет и С.Ю. Скобелин в своей статье «Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств» поясняют, что для большей эффективности обыск можно проводить с привлечением оперативного работника из Управления «К» МВД Российской Федерации, криминалистов из экспертно-криминалистического центра Министерства внутренних дел Российской Федерации или Управления криминалистики Следственного комитета России с использованием специальных криминалистических средств, позволяющих обнаружить спрятанные электронные носители. Такими средствами являются

¹ О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением Конституционных прав граждан: постановление Пленума Верховного Суда России от 01.06.2017 №19: офиц. текст по состоянию на 03.03.2018 // Бюллетень Верховного Суда России. – 01.07.2017. - №19.

² Собрание Законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

приборы криминалистической техники следующих марок: «Лорнет-24», «Лорнет-36», «NR-900S», «Люкс», «ORION HGO-4000»¹.

Согласно части 2 статьи 182 и части 2 статьи 183 Уголовно-процессуального кодекса Российской Федерации по общему правилу обыск производится на основании постановления следователя (дознателя). Однако, если местом производства обыска является жилище, то есть помещение, которое используется для постоянного или временного проживания, необходимо решение суда. Также исключительно на основании судебного решения может быть произведен обыск в служебном помещении адвоката².

Согласно части 11 статьи 182 Уголовно-процессуального кодекса Российской Федерации при производстве обыска должно участвовать лицо, в помещении которого проводится обыск, либо совершеннолетние члены его семьи². Также желательно, чтобы в помещении, где производится обыск присутствовало лицо «в отношении которого» проводится обыск, то есть лицо в чьем владении возможно находятся предметы или документы, представляющие интерес для следствия, поскольку в этой ситуации данное лицо вправе добровольно выдать те или иные предметы или документы, после чего обыск может быть прекращен³.

Носители, на которых содержатся электронные переписки могут быть также изъяты в ходе выемки. Выемка представляет собой родственное следственное действие по отношению к обыску, так как у них практически идентичное правовое регулирование. Отличием выемки от обыска является то, что она проводится с целью изъятия определенных предметов и документов, имеющих значение для уголовного дела, когда точно известно,

¹ Багмет А.М., Скобелин С.Ю. Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств. // Сборник статей «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях». – Тюмень: Издательство «ТГАМЭУП». – 2013. – №10 (ч. 2) С. 107.

² Собрание законодательства Российской Федерации. – 10.06.2002. - №23. - Ст. 2102.

³ Бюллетень Верховного Суда России. - 2003. - №8. – С.18, 19.

где и у кого они находятся. Выемке посвящена статья 183 Уголовно-процессуального кодекса Российской Федерации.¹

По мнению Б.Т. Безлепкина, в судебно-следственной практике выемка получила наибольшее распространение по уголовными делам, связанным с экономическими преступлениями, а также по уголовным делам, по которым необходимо изъять компьютерную технику, электронные носители².

Последний тезис подтверждает А.Н. Иванов в своей статье «Выемка электронной почты в сети Интернет», аргументируя свою позицию тем, что любое электронное сообщение, отправленное посредством технологий электронной почты или через социальные сети, прodelывает следующий путь: 1) компьютер лица, отправляющего электронную почту; 2) сервер-отправитель; 3) сервер, получающий сообщения электронной почты; 4) компьютер лица, которому адресована электронная корреспонденция. Это означает, что, если известен отправитель или получатель, то при желании установить путь сообщения будет несложно и будет понятно, где можно изъять носитель, содержащий электронное сообщение или его следы³.

А.Н. Иванов предлагает пользоваться следующим алгоритмом, который направлен на выемку самих файлов электронной почты, содержащих электронные сообщения: «а) искать электронные сообщения через бесплатный сервер электронной почты; б) через программы работы с электронной почтой (Microsoft Outlook Express, Netscape Messenger - как правило, названия папок хранения электронной почты этих программ совпадают, в папках этих программ: Inbox - папка хранения входящий почтовой корреспонденции, то есть, когда конкретный компьютер подключается к серверу провайдера и эта программа работы с электронной почтой перекачивает оттуда всю почту, то она помещается именно в этой папке и хранится там до момента удаления ее пользователем, однако можно

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

² Безлепкин Б.Т. Настольная книга следователя и дознавателя // Б.Т. Безлепкин. — М.: Проспект. – 2016. — С. 101.

³ Иванов А.Н., Силантьев Д.Н. Выемка электронной почты в сети Интернет. Журнал «Законность» №05/2015 URL: <http://www.crime-research.org/library/Removing.html> (дата обращения 05.03.2018).

попытаться ее восстановить). Outbox - в эту папку помещаются сообщения, созданные самим пользователем и подготовленные к отправлению (обычно сообщения электронной почты создаются в автономном режиме (т.е. когда компьютер не подключен к Интернету), а потом при подключении отправляются). Отправленные сообщения удаляются из папки Outbox. Sent Items - в этой папке хранятся копии отправленных с данного компьютера сообщений электронной почты (их оттуда можно удалить). Все удаленные сообщения хранятся в папке Deleted items (однако и оттуда можно все удалить). Это может сделать как сам пользователь, так и режим автоматического удаления, например, по истечении определенного времени. Однако пользователем могут создаваться и другие папки практически под любыми именами». В случае отсутствия файлов электронной почты на компьютере, но, когда имеются установленные по уголовному делу факты отправления (приема) электронного сообщения именно на этот компьютер, то компьютер подлежит изъятию и направлению на экспертизу для поиска следов электронных писем¹.

А.Н. Иванов поясняет, что согласно части 2 статьи 23 Конституции России, переписка может быть изъята только на основании решения суда, а значит необходимо руководствоваться не статьей 183 Уголовно-процессуального кодекса России, а применять по аналогии части 1-6, часть 7 применять непосредственно статьи 185 Уголовно-процессуального кодекса России «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», так как данная статья предусматривает обязательное решение суда¹.

Возможно более простым способом является выемка файлов электронной почты, содержащих электронные сообщения, непосредственно в организации оператора связи или в организации, представляющей услуги электронной почты, почтового сервера отправителя или получателя

¹ Иванов А.Н., Силантьев Д.Н. Выемка электронной почты в сети Интернет. Журнал «Законность» №05/2015 URL: <http://www.crime-research.org/library/Removing.html> (дата обращения 05.03.2018).

сообщений. Такой вывод можно сделать из того, что все файлы электронной почты хранятся на серверах, указанных организаций, и даже, если они стерты, то следы файлов точно должны остаться, так как данным организациям нет интереса удалять следы преступления. Данный вариант также является более простым с точки зрения правоприменения, поскольку часть 5 статьи 185 Уголовно-процессуального кодекса России предусматривает производство выемки и осмотра только в учреждении связи¹. Как уже отмечалось в предыдущей главе такой подход законодателя стоит считать не совсем верным.

Е.Р. Россинская и А.И. Усов указывают, что применение статьи 185 Уголовно-процессуального кодекса Российской Федерации при выемке электронной почты в учреждении связи или ином месте нахождения электронного носителя - это единственное правомерное решение по действующей редакции Уголовно-процессуального кодекса России².

Согласно части 3 статьи 185 Уголовно-процессуального кодекса Российской Федерации в постановлении следователя о возбуждении перед судом ходатайства о производстве изъятия и осмотра переписки необходимо указывать следующие сведения: 1) фамилию, имя, отчество и адрес лица, почтово-телеграфные отправления которого должны задерживаться; 2) основания наложения ареста, производства осмотра и выемки; 3) виды почтово-телеграфных отправок, подлежащих аресту (отправления электронной почты); 4) наименование учреждения связи (провайдера или владельца бесплатного почтового веб-сервера), на которое возлагается обязанность задерживать соответствующие почтово-телеграфные отправления³.

Электронные носители, содержащие электронные переписки или доступ к последним, могут также быть изъяты в ходе личного обыска в

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

² Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. // Е.Р. Россинская, А.И. Усов – М: Аст-Пресс. - 2011. - С.99.

³ Там же– 24.12.2001. - №52. - Ст. 4921.

порядке, предусмотренном статьей 184 Уголовно-процессуального кодекса России. Основанием для личного обыска является достаточное основание полагать, что предметы или документы, имеющие значение для уголовного дела, находятся у определенного лица. Личный обыск производится на основании судебного решения.

Для изъятия в ходе обыска у лица носителей электронных переписок, с целью последующего доступа к ним, необходимо судебное решение, в котором, во-первых, будет разрешено проведение личного обыска, во-вторых, будет разрешено получение доступа к электронным перепискам. Это предусмотрено в части 2 статьи 23 Конституции Российской Федерации, части 1 статьи 13, 184, 185 Уголовно-процессуального кодекса Российской Федерации^{1, 2}.

Исключением являются ситуации, предусмотренные частью 3 статьи 184 Уголовно-процессуального кодекса Российской Федерации, когда личный обыск проводится при задержании лица по подозрению в совершении преступления, есть основание полагать, что лицо, находясь в помещении, где производится обыск, скрывает предметы и документы, представляющие интерес для уголовного дела. Затем в случае, если в ходе осмотра, к примеру, мобильного телефона на нем будут обнаружены электронные переписки, то следует обратиться в суд за разрешением на проведение осмотра переписки и в случае положительного исхода провести дополнительный осмотр мобильного телефона, в ходе которого в протоколе осмотра предметов процитировать содержимое переписок. Это основано на применении аналогии частей 1-6 и непосредственном применении части 7 статьи 185 Уголовно-процессуального кодекса России².

Электронные носители могут быть также изъяты в ходе осмотра места происшествия, однако легальный доступ к электронным перепискам

¹ Собрание законодательства Российской Федерации. – 04.08.2014. – №31. - Ст. 4398

² Там же. – 24.12.2001. - №52. - Ст. 4921.

посредством последних может быть получен только на основании решения суда в соответствии с вышеуказанными правовыми нормами.

Электронная переписка также может быть изъята в ходе осмотра сайта социальной сети в порядке, предусмотренном частью 3 статьи 177 Уголовно-процессуального кодекса России, когда имеется доступ к аккаунту и разрешение суда на получение доступа органам предварительного расследования к электронной переписки¹.

В ходе осмотра в протоколе осмотра предметов (документов) необходимо указать с использованием какого персонального компьютера и каких компонентов (клавиатура, мышь, программное обеспечение) открыт сайт социальной сети, получен доступ к конкретному аккаунту (учетной записи) и соответствующей папки сообщений. Далее указываются аккаунты, с которыми велась переписка с обязательным указанием URL адреса их страниц и никнеймов аккаунтов, абонентского номера, если осматривается аккаунт мессенджера, далее в протоколе цитируются сообщения с указанием даты и времени отправления. В случае, если к сообщениям прикреплены отдельные файлы, к примеру, фотография или схема места предполагаемого совершения разбоя, нахождения «закладки» с наркотическим средством, указанный файл описывается в протоколе. Далее в протоколе можно написать, что указанные сообщения выделяются компьютерной мышью (наименование устройства) и направляются на печать (указывается название принтера) или записываются на CD-R диск. Это будет являться приложением к протоколу осмотра предметов (документов). Прикрепленные к сообщению иные файлы, которые могут быть распечатаны, также рекомендуется распечатать.

Анализируя вышеизложенное можно прийти к выводу о том, что после изъятия электронного носителя, содержащего переписку или доступ к ней, необходимо получить судебное решение на доступ к содержащейся в нем электронной переписки, если оно не было получено заранее, из-за того, что

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

следователь мог не знать о том, что на данном электронном носителе могут содержаться электронные сообщения, представляющее интерес для следствия. Затем производится осмотр предмета, в ходе которого цитируются сообщения, также может быть обеспечен перенос некоторых файлов, прикрепленных к сообщению на персональный компьютер путем копирования файлов, посредством которого они должны быть распечатаны. Указанные распечатки будут являться приложением к протоколу осмотра предметов. После этого следователь (дознатель) выносит постановление о признании и приобщении к уголовному делу вещественного доказательства в порядке, предусмотренном статьей 81 Уголовно-процессуального кодекса России¹. Указанное следственное действие желательно производить с участием специалиста в области компьютерной техники или хотя бы с участием следователя-криминалиста.

В ситуациях, когда электронное устройство находится под паролем и владелец не желает сообщать пароль или необходимо сделать наиболее качественный осмотр с закреплением большого количества файлов необходимо поручить проведение такого осмотра экспертно-криминалистическому управлению Следственного комитета России, Управлению «К» или экспертно-криминалистическому центру Управления Министерства внутренних дел России. Поскольку в указанных подразделениях имеется специальная криминалистическая техника.

2.2 Особенности использования специальной криминалистической техники для извлечения и закрепления информации из электронных устройств

В настоящее время для эффективной работы с электронными носителями информации существует комплекс криминалистического аппаратного обеспечения, в который входят специальные устройства и программное обеспечение для проведения осмотров электронной техники.

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

Для проведения наиболее эффективного осмотра электронной техники (компьютеров, ноутбуков, мобильных телефонов, планшетов и иных цифровых устройств) в Управлении криминалистики Следственного комитета России, Управлении «К» и экспертно-криминалистических центрах Управлений Министерства внутренних дел Российской Федерации имеется программное обеспечение «Мобильный криминалист» и специальные мобильные криминалистические устройства UFED и XRY¹.

Программа «Мобильный криминалист» разработана компанией «Оксиджен Софтвер». «Мобильный криминалист» - это универсальный программный комплекс для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи. Это программное обеспечение устанавливается на персональный компьютер. Данная программа позволяет извлекать данные из всех популярных моделей мобильных устройств на операционных системах iOS, Android, BlackBerry, Windows Phone и аппаратов на китайских чипсетах. Импортировать резервные копии устройств, а также их физические образы (JTAG, Chip-off). Получать данные из облачных хранилищ по логину/паролю или токenu: iCloud, Google, Microsoft, Email сервер и из других популярных облачных сервисов. Загружать и анализировать биллинги операторов сотовой связи. Извлекать весь набор данных из устройств: контакты, сообщения, звонки, файловую систему, местоположения и удаленную информацию. Находить общие места пребывания нескольких лиц и строить маршруты их передвижения на встроенной оффлайн карте. Выявлять общие связи между несколькими устройствами и устанавливать близкий круг общения пользователя. Просматривать все события в хронологическом порядке и выявлять периоды активности пользователя. Создавать отчеты в различных форматах (PDF, RTF, XLS, XML). Кроме того, ООО «Оксиджен Софтвер»

¹ Багмет А.М., Скобелин С.Ю. Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств. // Сборник статей «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях». – Тюмень: Издательство «ТГАМЭУП». – 2013. – №10 (ч. 2) С. 107.

предлагает к своему программному обеспечению следующие устройства, которые делают работу криминалиста более мобильной: планшет, на который установлено программное обеспечение «Мобильный криминалист»; набор кабелей и драйверов; защищенный кейс¹.

Программа «MobilEdit» работает по принципу программы «Мобильный криминалист» и содержит аналогичные функции. Ее разрабатывает компания «COMPELSON Labs». Единственное отличие в том, что «MobilEdit» не содержит никакого оборудования, а просто является программным обеспечением².

UFED представляет собой комплекс переносного оборудования, который способен выполнять следующие задачи. Физическое извлечение данных из устройств BlackBerry. Эксклюзивная расшифровка: данные мессенджера, приложений, электронной почты, Bluetooth, и иные. Широкая поддержка устройств Apple с операционными системами iOS3+. Физическое извлечение данных и расшифровка путем обхода блокировки из устройств на операционной системе Android. Извлечение файловой системы устройства на операционной системе Windows phone. Расшифровка журнала регистрации поездки TomTom, а также извлечение данных из других портативных устройств GPS. Получение существующих и удаленных данных: приложения, паспорта, сообщения электронной почты, история звонков, смс, контракты, календарь, файлы медиа, географические теги, информация о местонахождении, привязки GPS, и иные. Разработкой UFED занимается компания «Cellebrite Mobile Synchronization LTD». Также комплект UFED содержит специальный мешок, блокирующий сигналы связи, в который можно поместить изъятое упакованное мобильное устройство, это делается

¹ Официальный сайт ООО «Оксиджен Софтвр»: ПО «Мобильный криминалист». URL: <https://www.oxygensoftware.ru/ru/company/target/police> (дата обращения 06.03.2018).

² Официальный сайт организации «COMPELSON Labs». URL: <http://www.mobiledit.com/company/> (дата обращения 06.03.2018).

для того, чтобы через учетную запись, к примеру, через iCloud.com, нельзя было удалить данные¹.

Для более тщательной и всесторонней работы с электронными устройствами возможно направление последних на судебную компьютерно-техническую и иные экспертизы. По данной теме Е.Р. Россинская и Е.И. Галяшина приводят виды судебных компьютерных экспертиз и примерные перечни вопросов, задаваемых эксперту. Относительно исследования, проводимого в настоящей работе, представляют интерес следующие виды судебных компьютерно-технических экспертиз: «классическая» судебная компьютерно-техническая экспертиза; судебная аппаратно-компьютерная экспертиза; судебная информационно-компьютерная экспертиза; судебная компьютерно-сетевая экспертиза. Можно предположить, что проведение данных экспертиз актуально, когда речь идет о нестандартных носителях и устройствах-отправителях электронных сообщений.

Судебная компьютерно-техническая экспертиза направлена на установление фактов закономерностей эксплуатации аппаратных средств компьютерной системы. Возможен следующий перечень вопросов эксперту: «Относится ли представленное устройство к аппаратным компьютерным средствам? К какому типу (марке, модели) относится аппаратное средство? Какова роль и функциональные возможности данного аппаратного средства в конкретной компьютерной системе? Возможна ли отправка с данного аппаратного средства электронных сообщений и вложения в них формата файла (указать формат)? Каково фактическое состояние (исправное, неисправное) представленного аппаратного средства? Является ли представленное аппаратное средство носителем информации? Каков вид (тип, модель, марка) представленного носителя информации? Какое запоминающее устройство предназначено для работы с данным накопителем информации? Имеется ли в составе представленной компьютерной системы

¹ Официальный сайт организации «Cellebrite Mobile Synchronization» LTD. URL: <http://lang.cellebrite.com/ru/mobile-forensics/products/standalone/ufed-touch-ultimate> (дата обращения 07.03.2018).

запоминающее устройство для работы с этим носителем информации? Каковы параметры (емкость, среднее время доступа к данным, скорость передачи) носителя информации? Какой метод хранения данных реализован на представленном носителе? Доступен ли для чтения представленный носитель информации?»¹.

Судебная аппаратно-компьютерная экспертиза направлена на исследования программного обеспечения компьютерной системы и ее использования. Возможен следующий перечень вопросов эксперту: «Какова общая характеристика представленного программного обеспечения, из каких компонентов (программных средств) оно состоит? Каковы реквизиты разработчика и владельца данного программного средства? Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)? Какое общее функциональное предназначение имеет указанное программное средство? Имеются ли на носителях информации программные средства для реализации определенной функциональной задачи (в данном случае отправления и приема электронных сообщений)? Используется ли данное программное средство для решения определенной функциональной задачи? Каково фактическое состояние программного средства, его работоспособность по реализации отдельных (конкретных) функций? Каким образом организован ввод и вывод данных в представленном программном средстве? Имеются ли в программном средстве отклонения от нормальных параметров типовых программных продуктов (например, свойства инфицирования, недокументированных функций)? Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования? Каковы хронология и порядок использования программного средства (начиная с ее инсталляции или за определенный период)?»¹.

¹ Россинская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. / Е.Р. Россинская, Е.И. Галяшина. – М: Проспект. – 2013. – С. 178-188.

Судебная информационно-компьютерная экспертиза направлена на поиск, обнаружение, анализ и оценку информации. Возможен следующий перечень вопросов эксперту: «Как отформатирован носитель информации и в каком виде на него записаны данные? К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и другие) и какими программными средствами они обеспечиваются? Каким образом организован доступ (свободный, ограниченный) к данным на носителе информации и каковы его характеристики? Какие свойства, характеристики имеют выявленные средства защиты данных и какие пути ее преодоления возможны? Какие данные с фактами и обстоятельствами конкретного дела находятся на представленном носителе информации? Какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа) имеются на носителях информации? Какие данные с представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации? Каково содержание указанных файлов? Какая хронологическая последовательность действий (операций) с выявленными данными имела место при решении конкретной задачи? Какая причинная связь имеется между действиями с данными и имевшим место событием?»¹. В связи с тем, что ряд вышеуказанных вопросов, поставленных перед экспертом может быть связан с изъятием файлов электронной переписки и их осмотром, то необходимо вместе с постановлением о назначении судебной информационно-компьютерной экспертизы и копиями материалов уголовного дела направить в экспертное учреждение разрешение суда на доступ к электронным перепискам.

Судебная компьютерно-сетевая экспертиза направлена на выявление свойств и характеристик работы компьютерной техники в сети. Возможен следующий перечень вопросов эксперту: «Имеются ли признаки работы данного компьютерного средства в сети Интернет? Какие аппаратные

средства использовались для подключения к Интернету? Имеются ли заготовленные соединения с узлом сети Интернет и каковы их свойства (номера телефонов провайдера, имена и пароли пользователя, даты создания)? Каково содержание установок программы удаленного доступа к сети Интернет и протоколов соединений? Какие имеются адреса Интернета, по которым осуществлялся доступ с данного компьютерного средства? Имеются ли почтовые сообщения, полученные (а также отправленные) по электронной почте? Имеются ли сообщения, полученные (отправленные) посредством использования программ персональной связи через Интернет и каково их содержание?»¹.

Таким образом, в настоящем подразделе были рассмотрены особенности использования современной криминалистической техники для извлечения и закрепления информации, записанной на различные электронные устройства, и проанализированы возможности современных судебных компьютерно-технических экспертиз.

2.3 Получение электронных переписок посредством проведения оперативно-розыскных мероприятий

Оперативно-розыскная деятельность в соответствии со статьей 1 Федерального закона России «Об оперативно-розыскной деятельности» - это деятельность, которая осуществляется гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то Федеральным законом России «Об оперативно-розыскной деятельности», в пределах их полномочий посредством проведения оперативно-розыскных мероприятий².

Оперативно-розыскная деятельность осуществляется органами, указанными в статье 13 Федерального закона России «Об оперативно-розыскной деятельности»: Министерством внутренних дел, Федеральной

¹ Россинская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. / Е.Р. Россинская, Е.И. Галяшина. – М: Проспект. – 2013. – С. 178-188.

² Собрание законодательства Российской Федерации. – 14.08.1995. - №33. - Ст. 3349.

службой безопасности, Федеральной службы охраны, Федеральной службы исполнения наказаний, Службой внешней разведки, Федеральной таможенной службой¹.

Указанные органы осуществляют данный вид деятельности посредством проведения оперативно-розыскных мероприятий. Перечень оперативно-розыскных мероприятий является исчерпывающим и содержится в статье 6 Федерального закона России «Об оперативно-розыскной деятельности»¹.

Для работы с электронными и бумажными носителями, на которых могут отображаться электронные сообщения, не все из 15 оперативно-розыскных мероприятий будут считаться актуальными, а только следующие: контроль почтовых отправлений, телеграфных и иных сообщений; снятие информации с технических каналов связи; контролируемая поставка; оперативный эксперимент (в ходе контролируемой поставки и оперативного эксперимента возможен выход на связь с потенциальным подозреваемым посредством электронных сообщений); получение компьютерной информации. Такой подход обусловлен тем, что наиболее вероятно в ходе именно этих оперативно-розыскных мероприятий могут быть получены электронные или бумажные носители, содержащие электронные переписки.

В соответствии со статьей 8 Федерального закона России «Об оперативно-розыскной деятельности» проведение любого оперативно-розыскного мероприятия, ограничивающего конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи допускается на основании решения суда и при наличии информации: о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому обязательно производство предварительного следствия; о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; о событиях или

действиях, создающих угрозу государственной, военной, экономической и иной безопасности России. В случаях не терпящих отлагательств, допускается получение судебного решения не позднее 48 часов с момента начала проведения оперативно-розыскного мероприятия.

Часть 1 статьи 15 Федерального закона России «Об оперативно-розыскной деятельности» предусматривает, что органы, осуществляющие оперативно-розыскную деятельность, вправе в ходе проведения оперативно-розыскных мероприятий изымать предметы, документы, материалы и сообщения, прерывать в предусмотренных случаях услуги связи. Если изымаются электронные носители, то изготавливаются копии, если это не воспрепятствует осуществлению оперативно-розыскной деятельности¹.

Согласно статье 89 Уголовно-процессуального кодекса Российской Федерации в доказывании можно использовать результаты оперативно-розыскной деятельности только в том случае, если эти результаты будут в полной мере соответствовать требованиям Уголовно-процессуального кодекса Российской Федерации².

Среди перечня оперативно-розыскных мероприятий, в ходе которых наиболее вероятно изъятие носителя, содержащего электронную переписку или сведения о последней, стоит обратить отдельное внимание на новое оперативно-розыскное мероприятие - получение компьютерной информации.

Полковник полиции А.Л. Осипенко отмечает, что в ходе данного оперативно-розыскного мероприятия с компьютерных данных снимается обычно копия или делается распечатка, чтобы владелец информации не знал о проводимом оперативно-розыскном мероприятии. По его мнению, в качестве компьютеров сейчас могут рассматриваться любые электронные носители информации способные воспроизводить файлы цифровых форматов. Он считает, что данное оперативно-розыскное мероприятие в рамках электронных сообщений следует считать специальным с позиции

¹ Собрание законодательства Российской Федерации. – 14.08.1995. - №33. - Ст. 3349.

² Там же. – 24.12.2001. - №52. - Ст. 4921.

подхода к компьютерной техники по отношению к контролю почтовых, телеграфных и иных сообщений. Осуществляя контроль за электронной почтой или чатами социальной сети оперативный работник связан пределами объекта и названия оперативно-розыскного мероприятия, а работа в рамках получения компьютерной информации может осуществляться одновременно и в рамках электронной почты или чатов социальной сети, сообществ социальной сети, видео канала «Youtube» и иных возможных вариантов¹. Создание данного оперативно-розыскного мероприятия направлено на унификацию деятельности оперативных работников.

А.Л. Осипенко поясняет, что в техническом плане действия оперативных работников по получению компьютерной информации могут осуществляться следующим образом: «а) При доступе (непосредственно или через компьютерную сеть) к устройствам памяти, установленным в компьютере и периферийном оборудовании; б) При копировании данных с внешних устройств хранения информации; в) При получении информации с технических каналов связи». Данное мероприятие следует проводить с участием специалиста. Оперативно значимая информация может быть получена в виде отдельных текстовых, графических, аудио, фото или видео файлов. Последние случаи актуальны в рамках электронных переписок, когда эти файлы вложены в электронное сообщение. Среди источников получения оперативно значимой компьютерной информации особое место занимают сетевые каналы коммуникации, задействованные преступниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и иные. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. При этом важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интернет,

¹ Осипенко А.Л. Новое оперативно-розыскное мероприятий «Получение компьютерной информации»: содержание и основы осуществления. // Вестник Воронежского института МВД России. Воронеж: Издательство ВИ МВД России. – 2016. – №3 С. 83-90.

постоянно увеличивается («ICQ», «Skype», «WhatsApp», «Viber», «Telegram»), причем многие из них предоставляют услуги шифрования передаваемых данных¹.

Е.С. Дубоносов отмечает, что техническими объектами оперативно-розыскного мероприятия получение компьютерной информации являются: «а) мобильные устройства, обеспечивающие доступ к сетевым ресурсам, носители компьютерной информации, устройства, фиксирующие компьютерные данные, сетевое оборудование; б) объекты сети Интернет; в) места сетевого общения криминальных структур в социальных сетях; г) сетевые каналы коммуникации (электронная почта, мессенджеры)» .

Старший советник юстиции в отставке, доктор юридических наук Ю.П. Гармаев в своей монографии «Использование результатов оперативно-розыскной деятельности при расследовании уголовных дел о взяточничестве» поясняет, что результаты оперативно-розыскной деятельности целесообразно использовать в уголовно-процессуальном доказывании, если они отвечают следующим требованиям: соответствуют Уголовно-процессуальному кодексу России и содержат сведения, входящие в предмет доказывания; содержат указание на источник получения доказательства или предмета, который может стать доказательством; содержат данные, позволяющие проверить в условиях судопроизводства доказательства, сформированные на их основе. Также Ю.П. Гармаев указывает на возможность последующего допроса в качестве свидетелей по уголовному делу оперативных работников и иных лиц, участвующих в проведении конкретных оперативно-розыскных мероприятий (в случае, если это не относится к охраняемой законом тайне), осмотра и последующего признания вещественными доказательствами предметов (документов),

изъятых (собранных) в ходе проведения оперативно-розыскных мероприятий¹.

Из этого можно сделать следующий вывод о технологии придания доказательственного значения в уголовном процессе результатам оперативно-розыскной деятельности: 1) результаты оперативно-розыскной деятельности должны быть получены и переданы надлежащим образом органу, осуществляющему предварительное расследования, или суду; 2) результаты оперативно-розыскной деятельности, поступившие в орган предварительного расследования должны быть надлежащим образом закреплены в рамках Уголовно-процессуального кодекса Российской Федерации, осмотрены, при необходимости направлены на экспертизу и признаны вещественными доказательствами по уголовному делу; 3) оперативные работники, представители общественности и иные лица, принимающие участие в ходе оперативно-розыскных мероприятий могут быть допрошены в качестве свидетелей.

Статья 7 Федерального закона России «Об оперативно-розыскной деятельности» содержит следующие основания для проведения оперативно-розыскных мероприятий: 1) наличие возбужденного уголовного дела; 2) ставшие известными сведения о: признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах его подготавливающих, совершающих или совершивших; событиях или действиях, создающих угрозу государственной, военной, экономической, информационной или экологической безопасности России; лицах скрывающихся от органов предварительного расследования и суда или уклоняющихся от уголовного наказания; лицах, без вести пропавших, и об обнаружении неопознанных трупов; 3) поручения следователя (дознавателя) и определения суда; 4) запросы других органов, осуществляющих оперативно-розыскную деятельность; 5) применение мер безопасности в

¹ Гармаев Ю.П. Использование результатов оперативно-розыскной деятельности при расследовании уголовных дел о взяточничестве. // Ю.П. Гармаев, – Иркутск: ИИПК ПР ГП Российской Федерации. - 2014. - С.33.

отношении защищаемых лиц; б) запросы международных организаций и правоохранительных органов иностранных государств. Данный перечень является исчерпывающим¹.

Если в ходе проведения оперативно-розыскного мероприятия в соответствии с частью 2 статьи 6 Федерального закона России «Об оперативно-розыскной деятельности» использовались технические и иные средства, в описательной части постановления о представлении результатов оперативно-розыскной деятельности необходимо точно указывать все технические и количественные характеристики используемых технических средств¹. Информация о времени, месте и обстоятельствах производства оперативно-розыскного мероприятия должна быть отражена в рапорте об обнаружении признаков преступления или в сообщении о результатах оперативно-розыскной деятельности². Указывать вымышленные характеристики или не указывать вовсе запрещается, так как впоследствии это приводит к признанию доказательств, сформированных на основе результатов оперативно-розыскной деятельности, недопустимыми³.

Статья 11 Федерального закона России «Об оперативно-розыскной деятельности» предусматривает, что результаты оперативно-розыскной деятельности должны направляться следователю (дознавателю) или в суд на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность⁴.

Приказ от 27 сентября 2013 г. N 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» в пунктах 7-15 содержит правила направления следователю (дознавателю) или в суд результатов оперативно-розыскной деятельности.

¹ Собрание законодательства Российской Федерации. – 14.08.1995. - №33. - Ст. 3349.

² Российская газета. – 13.12.2013. – №6258 С. 88-93.

³ Ларинков А.А. Проблемы представления результатов ОРД для использования в уголовном судопроизводстве (по инструкции от 27 сентября 2017). // журнал «Криминалист». М: ЮИ АГП Российской Федерации. – 2014. – №1 С. 34-40.

⁴ Собрание законодательства Российской Федерации. – 14.08.1995. - №33. - Ст. 3349.

Результаты оперативно-розыскной деятельности представляются в виде рапорта об обнаружении признаков преступления или сообщения о результатах оперативно-розыскной деятельности вместе с постановлением о представлении результатов оперативно-розыскной деятельности руководителя органа, осуществляющего оперативно-розыскную деятельность. В случае, если были произведены проверочная закупка или контролируемая поставка предметов и веществ, свободная реализация которых запрещена или ограничена, а также оперативный эксперимент или оперативное внедрение, к ним прилагается постановление, вынесенное оперативным работником и утвержденное руководителем органа, осуществляющего оперативно-розыскную деятельность, о проведении данного оперативно-розыскного мероприятия. Далее факультативно прилагаются документы, которые были непосредственно получены (составлены) в ходе проведения конкретного оперативно-розыскного мероприятия и иные сопутствующие документы (данная процедура ни в одном нормативном правовом акте строго не описана). К примеру, если производилась проверочная закупка и перед ее началом между лицами была связь посредством электронной переписки, то можно приложить к сообщению скриншот ее изображения с мобильного устройства, однако в этом случае необходимо получить разрешение суда или письменное согласие обоих лиц, или же в дальнейшем следователю будет необходимо получить разрешение суда перед производством осмотра предмета (документ)а. Все это направляется вместе с сопроводительным письмом и описью документов и предметов¹.

Ю.П. Гармаев отмечает, что уголовные дела, связанные с незаконным оборотом наркотических средств и психотропных веществ, в основном возбуждаются на основании сведений, полученных в результате оперативно-розыскной деятельности, которым в последующем придается процессуальная форма, и они признаются вещественными доказательствами по уголовному

¹ Российская газета. – 13.12.2013. – №6258 С. 88-93.

делу, а рапорта в порядке статьи 143 Уголовно-процессуального кодекса Российской Федерации являются поводами для возбуждения уголовного дела. При этом он указывает на серьезные проблемы, связанные с часто встречающимся ненадлежащим оформлением оперативными работниками результатов оперативно-розыскной деятельности при направлении последних к следователю (дознавателю) или в суд, а также проблемы, связанные с нарушением Федерального закона «Об оперативно-розыскной деятельности»¹.

Ю.П. Гармаев приводит примеры типичных ошибок, связанных с осуществлением оперативно-розыскной деятельности. Он разделяет примеры на ситуации, когда ошибка имеет неустранимый характер, а именно, результат оперативно-розыскной деятельности не может быть использован в доказывании, и устранимый, когда государственный обвинитель, следователи и оперативный работник смогут в суде доказать несущественный характер нарушения производства оперативно-розыскного мероприятия.

К нарушениям, носящим неустранимый характер, Ю.П. Гармаев относит: 1) Проведение оперативно-розыскного мероприятия без основания, или в постановлении о проведении проверочной закупки, оперативного эксперимента, оперативного внедрения, контролируемой поставки не указано основание проведения; 2) Проведение оперативного эксперимента на основании сведений о признаках преступления небольшой или средней тяжести; 3) Незаконные досмотр и изъятие, когда предмет (к примеру, электронный носитель) изымается и в акте идет ссылка на Федеральный закон «О полиции» и (или) Кодекс Российской Федерации об административных правонарушениях, хотя по данному поводу есть специально предусмотренная правовая норма в части 1 статьи 15 Федерального закона России «Об оперативно-розыскной деятельности»;

¹ Гармаев Ю.П. Лекция «Использование результатов оперативно-розыскной деятельности в расследовании уголовных дел о незаконном обороте наркотиков и о коррупционных преступлениях»: канал Ю.П. Гармаева на портале Youtube.com «Юрий Гармаев». URL: <https://www.youtube.com/watch?v=XCbVtg3MgqQ> (дата обращения 08.03.2018).

4) Перед проведением оперативно-розыскного мероприятия происходит подстрекательство лица к совершению преступления; 5) Не обеспечены гарантии неприкосновенности в отношении спецсубъектов и не получено судебное решение в случаях, когда проведением оперативно розыскного мероприятия ограничиваются или нарушаются конституционные права граждан.

К нарушениям, носящим устранимый характер Ю.П. Гармаев относит нарушения должностными лицами органов, осуществляющих оперативно-розыскную деятельность, правил производства оперативно-розыскных мероприятий, оформления, представления результатов оперативно-розыскной деятельности следователю (дознавателю).

Под нарушением правил оформления результатов оперативно-розыскной деятельности следует понимать ситуации, к примеру, когда в акте неправильно указано название оперативно-розыскного мероприятия, привлекаются к участию в последнем не представители общественности, а понятые, которые не предусмотрены, как участвующие лица при производстве оперативно-розыскных мероприятий Федеральным законом России «Об оперативно-розыскной деятельности». В подобной ситуации следует допросить в суде в качестве свидетелей оперативных работников и представителей общественности, если последние принимали участие в оперативно-розыском мероприятии.

Нарушение правил представления результатов оперативно-розыскной деятельности следователю имеет место быть, когда сопроводительное письмо, сообщение (рапорт), постановление о представлении результатов оперативно-розыскной деятельности следователю, постановление о производстве отдельного оперативно-розыскного мероприятия, опись отсутствуют или подписаны ненадлежащим лицом. Чтобы исправить указанные нарушения в суд следует предоставить копии указанных выше документов из дела оперативного учета, при этом пояснив, что данные

документы не были своевременно приобщены и вшиты в материалы уголовного дела¹.

Таким образом, в настоящем параграфе был проанализирован правовой режим результатов оперативно-розыскной деятельности, рассмотрен порядок и основания производства оперативно-розыскных мероприятий, типичные ошибки и способы их недопущения, устранения.

2.4 Правовые аспекты действий защитника, связанных с уголовно-процессуальным доказыванием в контексте работы с электронными переписками и ее носителями

Согласно пункту 2 части 1 статьи 53 Уголовно-процессуального кодекса Российской Федерации защитник вправе собирать и представлять доказательства, которые необходимы для оказания юридической помощи, по правилам части 3 статьи 86 Уголовно-процессуального кодекса Российской Федерации посредством: получения предметов, документов и иных сведений; опроса лиц с их согласия; истребования справок, характеристик, иных документов от органов государственной власти, органов местного самоуправления, общественных объединений и организаций, которые обязаны предоставлять запрашиваемые документы или их копии. Также пункт 11 части 1 статьи 53 Уголовно-процессуального кодекса Российской Федерации предусматривает, что защитник вправе использовать любые незапрещенные средства и способы защиты².

Аналогичная правовая норма содержится в статье 6 Федерального закона России №63-ФЗ от 31.05.2002 «Об адвокатской деятельности и адвокатуре в Российской Федерации»³.

¹ Гармаев Ю.П. Использование результатов оперативно-розыскной деятельности при расследовании уголовных дел о взяточничестве. // Ю.П. Гармаев, – Иркутск: ИИПК ПР ГП Российской Федерации. - 2014. - С.38-70.

² Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

³ Там же. – 10.06.2002. - №23. - Ст. 2102.

Анализируя вышеприведенные правовые нормы, можно прийти к выводу о том, что сторона защиты вправе собирать доказательства любым незапрещенным законом способом и не нарушая прав других лиц.

Ю.М. Новолодский приводит два вида целевого назначения доказывания актуального для стороны защиты: «1) Реконструкционное доказывание, целью которого является ретроспективное получение выгодных для стороны защиты знаний об исследуемом преступлении; 2) Контрольное доказывание, направленное на выявление существенных нарушений стороной обвинения уголовно-процессуального законодательства в процессе доказывания»¹.

Реконструкционное доказывание в исследуемой теме можно обозначить, прежде всего, как процесс, связанный с установлением наличия или отсутствия факта межличностной коммуникации посредством электронных сообщений. Это может быть установлено путем опроса лиц с их согласия или иным, незапрещенным законом способом. Далее защитник может самостоятельно снять скриншоты с компьютерной информации и (или) предоставить соответствующий электронный носитель правоприменительному органу, осуществляющему производство по уголовному делу, заявить соответствующее ходатайство о предоставлении носителя информации. Учитывая охраняемое конституцией и уголовно-процессуальным законом право на тайну переписки, при отсутствии письменного согласия лиц, осуществлявших переписку, использование в доказывании данных сведений без решения суда является недопустимым. Однако, когда данное доказательство представляется непосредственно в суд и с разрешением хотя бы одной стороны переписки, процедура во многом упрощается.

По мнению Ю.М. Новолодского процесс поиска и собирания доказательств адвокату-защитнику лучше производить совместно или

¹ Новолодский Ю.М. Доказывание в практической деятельности адвоката-защитника. // Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2016. – С. 40.

посредством какой-либо коммуникации со своим доверителем или третьими лицами (специалистами, представителями муниципальных органов и иными). Это обусловлено тем, что защитник, самостоятельно в одиночку получивший предмет, который потенциально может являться вещественным доказательством, и представивший его органу, у которого находится в производстве уголовное дело, может перейти в разряд свидетелей, в случае если обстоятельства получения данного доказательства известны только ему одному. Соответственно данный факт исключит его дальнейшее участие в уголовном деле в качестве защитника, так как получится, что адвокат может оказаться единственным человеком, который будет осведомлен об обстоятельствах сбора данного доказательства (где?, как?, когда?, кем? и при каких обстоятельствах доказательство было получено?)¹.

При работе адвоката-защитника с «электронными доказательствами» в ряде случаев может быть целесообразным привлечение специалиста, тем более пункт 13 Стандарта осуществления адвокатом защиты в уголовном судопроизводстве предусматривает возможность привлечения специалиста, когда возникает такая необходимость².

В идеале реконструктивное доказывание должно быть направлено на альтернативное видение исследуемых событий, как полного, так и частичного несоответствия версии, отстаиваемой стороной обвинения.

Ю.М. Новолодский подчеркивает, что поскольку сторона защиты вправе осуществлять доказательственную деятельность, то ей должна быть обеспечена практическая возможность автономного осуществления доказательственной деятельности, включающей в себя поиск выгодной для защиты доказательственной информации, ее вне процессуального закрепления, предварительную оценку этой информации, а также

¹ Новолодский Ю.М. Доказывание в практической деятельности адвоката-защитника. // Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2016. – С. 62.

² Вестник Федеральной палаты адвокатов Российской Федерации. – 2017. - №2.

определение тактически выгодного момента представления этой доказательственной информации правоприменительному органу¹.

Таким образом, на стороне защиты нет обязанности предоставлять доказательства сразу после обнаружения или получения.

Завершая анализ реконструкционного доказывания, стоит отметить, что в каждом отдельном случае стороне защиты следует отталкиваться от сформулированной тактики защиты по уголовному делу. К примеру, по мнению курганского адвоката А.В. Колегова, собирая адвокату доказательства по уголовному делу, следует воздерживаться от заявления большого количества ходатайств следователю (дознавателю), связанных с проведением следственных действий. Он поясняет, что, если следователь (дознаватель) окажутся недобросовестными, то они могут попытаться уничтожить или исказить доказательственную информацию, предав ей обвинительный характер. Также все ходатайства приобщаются к материалу уголовного дела, а значит тактические наработки стороны защиты станут известны следователю и прокурору-гособвинителю, даже в случаях, когда эти ходатайства не были удовлетворены².

Далее стоит рассмотреть контрольное доказывание защитника.

В случае, если следователь (дознаватель), проводя следственные действия, направленные на собирание, проверку и оценку доказательств, допускает нарушение правовых норм Уголовно-процессуального кодекса Российской Федерации подозреваемый, обвиняемый, подсудимый и его защитник вправе заявлять ходатайство о признании доказательств недопустимым в порядке, предусмотренном статьями 119-122, 217 и 271 Уголовно-процессуального кодекса России³.

Новосибирский адвокат М.В. Спиридонов в своей статье «Изъятие электронных носителей информации без участия специалиста как основание

¹ Новолодский Ю.М. Доказывание в практической деятельности адвоката-защитника. // Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2016. – С. 37.

² Videоблог адвоката Колегова А.В. «Адвокатские тайны»: «Как строить защиту по уголовному делу?». URL: <https://www.youtube.com/watch?v=> (дата обращения 03.03.2018).

³ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

для признания обыска незаконным» приводит следующий пример. Он осуществлял защиту обвиняемого по уголовному делу по признакам преступления, предусмотренного пунктом «в» части 3 статьи 146 Уголовного кодекса Российской Федерации – нарушение авторских и смежных прав, совершенное группой лиц по предварительному сговору. У его подзащитного в квартире был произведен обыск, при котором были следующие нарушения: 1) его подзащитному не позволили пригласить адвоката; 2) в ходе обыска были изъяты электронные носители информации (USB-устройства флеш-памяти - флешкарты), оптические диски, жесткие диски, а также ноутбук, с установленной программой-мессенджером «WhatsApp», однако специалист в этом следственном действии участия не принимал. Им было принято решение подать жалобу на имя прокурора в порядке, предусмотренном статьей 124 Уголовно-процессуального кодекса России. Данный способ обжалования он выбрал в связи с тем, что не за долго до производства обыска уголовное дело было возвращено из прокуратуры к следователю для проведения дополнительного расследования с указанием производства обыска. При подаче жалобы прокурору, сторона защиты не лишена возможности обжаловать его решение в суд, а соответственно в случае отказа в удовлетворении жалобы, можно реализовать право на судебное рассмотрение предмета жалобы. Если сразу подать жалобу в порядке статьи 125 Уголовно-процессуального кодекса России в суд, то в случае вынесения постановления об отказе в удовлетворении жалобы, это судебное постановление будет приобщено к материалам уголовного дела, тем самым признает производство следственного действия законным («засилит» производство следственного действия), поэтому в дальнейшем будет сложнее признать производство обыска незаконным и признать полученные в ходе обыска доказательства недопустимыми. В результате прокурором обыск был признан незаконным, а доказательства, изъятые в ходе его производства, были признаны недопустимыми¹.

¹ Спиридонов М.В. Изъятие электронных носителей информации без участия специалиста как основание для

В настоящем подразделе были рассмотрены аспекты уголовно-процессуального доказывания стороны защиты.

3. ВАРИАНТЫ РАЗРЕШЕНИЯ ПРАВОВОГО ПРОБЕЛА, СВЯЗАННОГО С ЭЛЕКТРОННОЙ ПЕРЕПИСКОЙ В УГОЛОВНО- ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

3.1 Применение аналогии закона

В действующей редакции Уголовно-процессуального кодекса Российской Федерации отсутствуют специальные правовые нормы, детально регламентирующие изъятие и осмотр электронных сообщений (переписок). В части 7 статьи 185 Уголовно-процессуального кодекса Российской Федерации содержится единственная правовая норма, применимая к электронным перепискам, согласно которой электронные и иные сообщения, передаваемые по каналам электросвязи могут быть на основании решения суда изъяты и осмотрены¹.

Это единственная правовая норма, регулирующая напрямую (без применения аналогии закона) доказательственную работу с электронными переписками. Такого правового регулирования недостаточно для надлежащего правоприменения.

Данный вывод следует как минимум из того, что все 6 частей статьи 185 Уголовно-процессуального кодекса России посвящены почтово-телеграфным корреспонденциям, которые не с позиции правового регулирования, а исходя из своей формы и существа значительно отличаются от электронных сообщений (переписок). Также в первом подразделе первого раздела настоящей работы отмечалось, что правовые нормы регулирующие следственные действия, производимые с почтово-телеграфными отправлениями, во-первых, обусловлены строго указанным объектом следственных действий, во-вторых указывают на обязательное получение судебного решения в случае их осмотра и выемки в учреждениях связи (в начале настоящей работы был приведен пример из судебной практики, когда суд отказал следователю в получении доступа к мессенджерам на мобильных телефонах, изъятых в ходе обыска, сославшись на то, что судебное решение

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

выносятся только для осмотра и выемки сообщений в учреждениях связи и больше нигде). На основании вышеизложенного следует, что имеется необходимость в применении частичной аналогии уголовно-процессуального закона, а именно, часть 7 статьи 185 Уголовно-процессуального кодекса Российской Федерации стоит применять непосредственно, а части 1-6 указанной статьи по аналогии.

Данный подход стоит считать единственным правомерным подходом до тех пор, пока в Уголовно-процессуальный кодекс Российской Федерации не будут внесены изменения, о которых пойдет речь в следующем подразделе (или иные аналогичные законодательные изменения).

Ю.В. Францифоров и Н.О. Овчиникова указывают, что аналогией закона является применение к отношениям, не урегулированным законом, положений закона, регулирующего сходные отношения. По их мнению, преодоление пробелов в уголовно-процессуальном законе путем применения аналогии закона допустимо, если это не нарушает ничьи права и законные интересы. Такой подход следует считать правильным, так как Уголовно-процессуальный кодекс Российской Федерации в отличие от Уголовного кодекса Российской Федерации не содержит запрета на применение аналогии.

Конституционный Суд Российской Федерации считает, что применение аналогии уголовно-процессуального закона возможно. Они указывают свои позиции по данному поводу в следующих решениях Конституционного суда России: Постановление от 02.07.1998 № 20-П; Постановление от 23.03.1999 № 5-П; Определение от 24.04.2002 №114-О¹.

Конституционный Суд Российской Федерации в своем Определении от 24.04.2002 № 144-О «По жалобе граждан Вахонина Александра Ивановича и Смердова Сергея Дмитриевича на нарушение их конституционных прав

¹ Францифоров Ю.В., Овчиникова Н.О. Аналогия закона и аналогия права в Российском уголовном процессе как способ преодоления пробелов в уголовно-процессуальном праве. // журнал «Процессуальное право: вопросы теории и правоприменения». Волгоград: Вестник Волгоградского государственного университета. – 2016. – №1 С. 156-167.

частью третьей статьи 220.2 УПК РСФСР», подтверждая обоснованность применения аналогии уголовно-процессуального закона, указывает на условие такого применения: «...при применении в порядке аналогии положений части третьей статьи 220.2 УПК РСФСР судам, рассматривающим жалобы на незаконность и необоснованность отказа в возбуждении уголовного дела, надлежит - исходя из закрепленных в Конституции Российской Федерации и уголовно - процессуальном законодательстве принципов судопроизводства»¹. В случае с электронной перепиской применение аналогии уголовно-процессуального закона следует считать обоснованным, так как, во-первых, тайна переписки, сформулированная в статье 13 Уголовно-процессуального кодекса Российской Федерации, является одним из принципов уголовного судопроизводства, во-вторых применение данной аналогии соответствует остальным принципам уголовного судопроизводства, которые перечислены в главе 2 Уголовно-процессуального кодекса Российской Федерации².

В данном случае сходными отношениями следует считать следственные действия, урегулированные частями 1-6 статьи 185 Уголовно-процессуального кодекса Российской Федерации «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка»². Этот подход разделяют кандидат юридических науки А.Н. Иванов и помощник прокурора Д.Н. Силантьев в своей статье «Выемка электронной почты в сети Интернет». В рассматриваемом случае нет принципиальной разницы между тем, посредством мобильного мессенджера или электронной почты происходила отправка электронного сообщения, в учреждении связи или у гражданина в помещении следственного кабинета в ходе выемки будет получено электронное устройство.

¹ По жалобе граждан Вахонина Александра Ивановича и Смердова Сергея Дмитриевича на нарушение их конституционных прав частью третьей статьи 220.2 УПК РСФСР: определение Конституционного Суда России от 24.04.2002 № 114-О: офиц. текст по состоянию на 10.03.2018 // Вестник Конституционного Суда Российской Федерации. - №6. - 2002.

² Собрание законодательства Российской Федерации. - 24.12.2001. - №52. - Ст. 4921.

В постановлении о возбуждении перед судом ходатайства необходимо сослаться на часть 2 статьи 23 Конституции Российской Федерации, предусматривающей право каждого на тайну переписки¹. Кроме того, важно указать следующие правовые нормы Уголовно-процессуального кодекса Российской Федерации: часть 1 статьи 13, предусматривающую обязательное получение судебного решения для проведения следственных действий, ограничивающих права граждан на тайну переписки, почтовых, телеграфных и иных сообщений; статью 165, содержащую общие правовые нормы о возбуждении перед судом ходатайств о проведении следственных действий, для которых необходимо судебное решение; статью 185, которая была рассмотрена выше. Также нужно указать, что в соответствии с частью 1 статьи 63 Федерального закона Российской Федерации «О связи» ограничение права на тайну переписки возможно только в случаях, предусмотренных федеральными законами².

Применяя указанную аналогию, можно в порядке статьи 185 Уголовно-процессуального кодекса Российской Федерации получить разрешение суда на изъятие и осмотр носителя, содержащего электронную переписку или доступ к ней (в случае, если последняя хранится не в постоянной памяти, а на серверах).

Если изымается такой носитель, но осмотр переписок не предполагается, тогда разрешение суда не нужно. В случае, когда электронный носитель был уже изъят, а доступ к электронной переписке потребовался позже, тогда в ходатайстве можно указать только необходимость осмотра этой переписки.

Уголовно-процессуальный кодекс Российской Федерации не содержит каких-либо запретов на применения аналогии закона, к тому же в данном случае речь идет о частичном применении аналогии закона, так как часть 7 статьи 185 Уголовно-процессуального кодекса России будет применяться

¹ Собрание законодательства Российской Федерации. – 04.08.2014. – №31. - Ст. 4398.

² Там же. – 14.07.2003. - №28. - Ст. 2895.

непосредственно. Стоит отметить, что данное применение аналогии закона направлено в первую очередь на улучшение положения и гарантию прав, законных интересов граждан. Также это позволит органам предварительного расследования и прокуратуре не опасаться того, что собранные ими по делу доказательства в суде будут под угрозой признания их недопустимыми из-за нарушения правовых норм Конституции России и Уголовно-процессуального кодекса Российской Федерации. Также стоит подчеркнуть, что это немного усложнит работу следователей (дознавателей), так как им придется тратить время на вынесение постановления о возбуждении перед судом соответствующих ходатайств, согласовывать данные постановления с руководителем следственного органа (дознавателю придется согласовывать с прокурором), ксерокопировать необходимые материалы уголовного дела и вести все это в суд. Работу суда это также усложнит, поскольку добавится дополнительная нагрузка.

С другой стороны, у органов предварительного расследования и суда работы меньше не станет, если уголовные дела будут возвращаться прокурору в порядке статьи 237 Уголовно-процессуального кодекса России¹.

Стоит учитывать, что применение аналогии уголовно-процессуального закона к анализируемой проблеме, не является ее идеальным решением. Такой вывод следует из того, что каждый правоприменитель использует аналогию закона относительно уровня своей правовой культуры, правосознания и толкования правовых норм. Францифоров Ю.В. и Овчиникова Н.О. поясняют, что применение аналогии закона или аналогии права не ликвидирует пробел, а только преодолевает его в конкретном случае. Ликвидировать пробел может только законодательный орган, внося соответствующие изменения в закон².

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

² Францифоров Ю.В., Овчиникова Н.О. Аналогия закона и аналогия права в Российском уголовном процессе как способ преодоления пробелов в уголовно-процессуальном праве. // журнал «Процессуальное право: вопросы теории и правоприменения». Волгоград: Вестник Волгоградского государственного университета. – 2016. – №1 С. 166.

Таким образом, в настоящем параграфе была рассмотрена возможность применения аналогии уголовно-процессуального закона, как одного из вариантов преодоления пробела в Уголовно-процессуальном кодексе Российской Федерации, связанного с недостаточным правовым регулированием порядка изъятия и осмотра электронных переписок в рамках уголовно-процессуального доказывания.

3.2 Внесение изменений в Уголовно-процессуальный кодекс Российской Федерации

В предыдущем параграфе был сделан вывод о том, что лучшим способом ликвидации пробела в законодательном акте является внесение в него изменений, так как при грамотной законодательной технике этого пробела больше не будет.

В действующей редакции Уголовно-процессуального кодекса России есть статья 185, посвященная наложению ареста, осмотру и выемки почтово-телеграфных отправлений. В части 7 настоящей статьи содержится единственная правовая норма в Уголовно-процессуальном кодексе России, связанная с электронными сообщениями. Данная правовая норма содержит указание на обязательное получение решения суда для осмотра и изъятия электронных сообщений. При этом законодатель не указывает на особенности производства следственных действий и возбуждения перед судом ходатайства о производстве, указанных следственных действий с электронными сообщениями, как он это сделал с почтово-телеграфными отправлениями¹.

В настоящей работе неоднократно отмечалась определенная схожесть категорий почтово-телеграфных отправлений и электронных переписок. В связи с этим следует считать, что наиболее удачным решением для внесения в Уголовно-процессуальный кодекс Российской Федерации новых правовых норм, регламентирующих вопросы доказывания с электронными

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

переписками, будет являться введение новой статьи, которая по содержанию и структуре схожа со статьей 185 настоящего кодекса.

Чтобы упростить правовое регулирование данного вопроса следует сначала внести изменение в часть 7 статьи 185 Уголовно-процессуального кодекса Российской Федерации, в которой будет говориться про наложение ареста на электронные сообщения, передаваемые по каналам электросвязи. Указанную часть следует дополнить отсылкой к статье 185.1 Уголовно-процессуального кодекса России, посвященной непосредственно электронным сообщениям. Таким образом, правовая норма, содержащаяся в части 7 статьи 185 Уголовно-процессуального кодекса России, будет считаться общей правовой нормой по отношению к статье 185.1 Уголовно-процессуального кодекса России.

Статья 185.1 Уголовно-процессуального кодекса Российской Федерации «Изъятие и осмотр электронных сообщений» может выглядеть следующим образом.

Часть 1. При наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях (переписках) или в файлах, вложенных в электронные сообщения, данные электронные сообщения (переписки) могут быть изъяты и осмотрены на основании решения суда. При невозможности получения доступа к электронным сообщениям в натуре, изымать электронные сообщения следует посредством изъятия носителя информации, на котором они находятся (на который они записаны).

Часть 2. Изъятие и осмотр электронных сообщений производятся на основании судебного решения, принимаемого в порядке, установленном статьей 165 настоящего Кодекса. Указанные следственные действия производятся с участием специалиста в области компьютерной техники.

Часть 3. В ходатайстве следователя о проведении следственных действий, указанных в частях 1 и 2 настоящей статьи, указываются: 1) фамилия, имя, отчество и адрес лица, источники отправления или приема

электронных сообщений которого должны задерживаться, изыматься, осматриваться; 2) основания наложения ареста, производства изъятия и осмотра; 3) виды источников отправления или приема, подлежащих аресту; 4) указание владельца источника приема или отправления электронных сообщений, интернет-провайдера, учреждения связи, на которое возлагается обязанность задерживать соответствующие электронные сообщения.

Часть 4. В случае принятия судом решения о производстве изъятия и осмотра электронных сообщений, его копия направляется владельцу источника отправления или приема (электронного носителя) электронных сообщений или организации интернет-провайдера, учреждению связи, которому поручается задерживать электронные сообщения незамедлительно уведомлять об этом следователя (дознателя).

Часть 5. Осмотр, выемка и снятие копий с задержанных и (или) изъятых электронных сообщений производятся следователем (дознателем) в соответствующем учреждении связи, организации провайдера или у лица, являющегося владельцем источника отправления или приема (электронного носителя информации) электронных сообщений.

Часть 6. Изъятие электронного носителя информации, содержащего электронные сообщения, на основании решения суда возможно в ходе следственных действий, предусмотренных статьями 176-177, 182, 183, 184, 185 настоящего кодекса.

Часть 7. В случае, если электронный носитель информации, на котором содержатся электронные сообщения, находится у следователя (дознателя) на момент, когда появилась необходимость получить доступ к электронным сообщениям, необходимо указать в ходатайстве только проведение осмотра указанных электронных сообщений. Правило настоящей части действует только в случаях, когда следователь (дознатель), ранее изымая электронный носитель информации не знал и не мог знать о том, что на нем могут находиться электронные сообщения или, предполагал, что электронные сообщения не будут представлять интерес для следствия.

Часть 8. Запрещается проведение следственных действий, указанных в частях 1 и 2 настоящей статьи, без решения суда в порядке, предусмотренном статьей 165 настоящего кодекса. Указанный запрет также действует и на осмотр электронных сообщений, когда они осматриваются, как составной элемент электронного носителя информации, в ходе комплексного осмотра последнего¹.

В настоящем разделе были рассмотрены два варианта преодоления пробела в уголовно-процессуальном законе, связанном с производством следственных действий с электронными сообщениями: аналогия уголовно-процессуального закона и внесение изменений в Уголовно-процессуальный кодекс Российской Федерации. Последний способ ликвидации пробела более предпочтителен, так как он позволит ликвидировать сложившийся пробел.

¹ Собрание законодательства Российской Федерации. – 24.12.2001. - №52. - Ст. 4921.

ЗАКЛЮЧЕНИЕ

Целью исследования настоящей работы является анализ роли электронной переписки в уголовно-процессуальном доказывании и выбор решений, направленных на устранение проблем, вызванных несовершенством уголовно-процессуального законодательства Российской Федерации в контексте использования электронных переписок в доказывании.

Под электронными переписками понимаются сообщения в электронной форме, которые передаются посредством приборов и устройств по каналам электросвязи из одного места в другое в виде электрических сигналов. Их роль заключается в том, что электронные переписки, являясь одним из средств межличностной коммуникации между людьми, отражают передаваемые сведения, которые фиксируются в виде своеобразных следов.

В ходе исследования электронных переписок в уголовно-процессуальном доказывании были рассмотрены примеры из судебно-следственной и адвокатской практики. Без внимания не осталась практика оперативно-розыскной деятельности, поскольку результаты последней при соблюдении требований Уголовно-процессуального кодекса Российской Федерации, предъявляемых к доказательствам, могут использоваться в доказывании, в том числе, в контексте электронных переписок, поскольку они могут содержаться на носителях, полученных в ходе оперативно-розыскных мероприятий.

В результате исследования были выявлены следующие проблемы и пути их решения.

Первая проблема связана с пробелом в уголовно-процессуальном законе. В части 7 статьи 185 Уголовно-процессуального кодекса Российской Федерации содержится единственная правовая норма, посвященная электронным перепискам (сообщениям) в доказывании, которая содержит только указание на обязательное получение решения суда для выемки и осмотра электронных переписок. В частях 1-6 статьи 185 Уголовно-

процессуального кодекса Российской Федерации сформулированы специальные правовые нормы, которые детально регулируют порядок наложения ареста, осмотра и выемки почтово-телеграфных отправлений. При этом данные правовые нормы, в силу особенностей почтово-телеграфных отправлений, не являются и не могут являться общими по отношению к следственным действиям, объектами которых выступают электронные переписки. Электронные переписки не могут быть воспроизведены и самостоятельно осмотрены без соответствующего электронного носителя, на котором они содержатся, за исключением ситуаций, когда они предоставляются обслуживающей организацией в виде распечаток или единым электронным документом на диске. При этом закон императивно указывает на обязательность получения судебного решения для производства выемки и осмотра электронных переписок. Проблема в том, что в судебно-следственной практике данную норму часто толкуют ограничительно, считая, что, если электронная переписка, к примеру, сохранена в памяти мобильного телефона, то она является его частью, а судебное решение необходимо только в случаях, когда объектом производства следственного действия выступает непосредственно электронная переписка. Пробелом в данной ситуации является отсутствие подробного регулирования производства указанных следственных действий с электронными переписками, которое, к примеру, имеется в случае с почтово-телеграфными отправлениями.

Данная проблема может быть разрешена посредством применения аналогии уголовно-процессуального закона или внесения в Уголовно-процессуальный кодекс Российской Федерации новых правовых норм, регулирующих производство следственных действий с электронными переписками и статус последних в доказывании.

Второй проблемой, выявленной в ходе настоящего исследования, является нарушение должностными лицами органов, осуществляющих оперативно-розыскную деятельность, правил оформления, производства,

представления результатов оперативно-розыскной деятельности следователю (дознавателю). Были рассмотрены нарушения, несущие неустранимый и устранимый характер.

Нарушение правил представления результатов оперативно-розыскной деятельности следователю (дознавателю) имеет место быть, когда сопроводительное письмо, сообщение (рапорт), постановление о представлении результатов оперативно-розыскной деятельности следователю (дознавателю), постановление о производстве отдельного оперативно-розыскного мероприятия, опись отсутствуют или подписаны ненадлежащим лицом. Чтобы исправить указанные нарушения в суд следует предоставить копии указанных выше документов из дела оперативного учета, при этом пояснив, что данные документы не были своевременно приобщены и вшиты в материалы уголовного дела.

Под нарушением правил оформления результатов оперативно-розыскной деятельности следует понимать ситуации, к примеру, когда в акте неправильно указано название оперативно-розыскного мероприятия, привлекаются к участию не представители общественности, а понятые, которые не предусмотрены, как участвующие лица при производстве оперативно-розыскных мероприятий Федеральным законом России «Об оперативно-розыскной деятельности». В подобной ситуации следует допросить в суде в качестве свидетелей оперативных работников и представителей общественности и иных лиц, если последние принимали участие в оперативно-розыскном мероприятии.

В ходе исследования действий адвоката-защитника в контексте темы настоящей выпускной квалификационной работы каких-либо проблем выявлено не было, поскольку Уголовно-процессуальный кодекс Российской Федерации, Федеральный закон Российской Федерации «Об адвокатской деятельности и адвокатуре в Российской Федерации», Стандарт осуществления адвокатом защиты в уголовном судопроизводстве дают адвокату большую диспозитивность в процессе доказывания. Иными

словами, адвокат не ограничен каким-либо закрытым перечнем следственных действий. Это позволяет адвокату более грамотно подобрать тактику защиты в зависимости от развивающихся событий в ходе предварительного расследования и следственного видения.

Иными словами, в настоящей выпускной квалификационной работе была рассмотрена и проанализирована электронная переписка в уголовно-процессуальном доказывании, представляющая собой на сегодняшний день весьма важный элемент доказывания в уголовном судопроизводстве, хотя на первый взгляд возможно не самый значительный по объему. С учетом стремительного развития научно-технического прогресса в эпоху постиндустриального общества можно предположить, что актуальность исследованной темы с каждым годом будет возрастать.

Таким образом, можно сделать вывод о том, что поставленные во введении цели и задачи выпускной квалификационной работы были достигнуты в полном объеме.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК*Нормативные правовые акты*

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ). // *Собрание законодательства Российской Федерации*. – 04.08.2014. – №31. - Ст. 4398.
2. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ: офиц. текст по состоянию на 01.03.2018 // *Собрание законодательства Российской Федерации*. – 17.06.1994. – №25. - Ст. 2954.
3. Об оперативно-розыскной деятельности: федеральный закон от 12.08.1995 №144-ФЗ: офиц. текст по состоянию на 18.03.2017 // *Собрание законодательства Российской Федерации*. – 14.08.1995. - №33. - Ст. 3349.
4. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 18.12.2001 №174-ФЗ: офиц. Текст по состоянию на 18.03.2017 // *Собрание законодательства Российской Федерации*. – 24.12.2001. - №52. - Ст. 4921.
5. Об адвокатской деятельности и адвокатуре в Российской Федерации: федеральный закон от 31.05.2002 №63-ФЗ: офиц. текст по состоянию на 18.03.2018 // *Собрание законодательства Российской Федерации*. – 10.06.2002. - №23. - Ст. 2102.
6. О связи: федеральный закон от 07.07.2003 №126-ФЗ: офиц. текст по состоянию на 29.03.2018. // *Собрание законодательства Российской Федерации*. – 14.07.2003. - №28. – Ст. 2895.
7. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. N 149-ФЗ: офиц. текст по состоянию на 02.03.2018 // *Собрание Законодательства Российской Федерации*. – 31.07.2006. - №31 (ч. №1). - Ст. 3448.

8. О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 1 марта 2012 г. №18-ФЗ: офиц. текст по состоянию на 03.03.2018 // Собрание Законодательства Российской Федерации. – 05.03.2012. - №10. - Ст. 1166.
9. О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 06.07.2016 №374-ФЗ: офиц. текст по состоянию на 28.03.2018 // Собрание Законодательства Российской Федерации. – 11.07.2016. - №28. - Ст. 4558.
10. Об утверждении Правил оказания услуг почтовой связи: постановление Правительства России от 26.09.2000 №725: офиц. текст по состоянию на 29.02.2017 // Собрание законодательства Российской Федерации. – 09.10.2000. - №41. - Ст. 4076.
11. Об утверждении правил оказания телематических услуг связи: постановление Правительства России от 10 сентября 2007 г. N 575: офиц. текст по состоянию на 02.03.2018 // Собрание Законодательства Российской Федерации. – 17.09.2007. - №38. - Ст. 4552.
12. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России, Министерства обороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН, ФСКН, СК Российской Федерации от 27 сентября 2013 г. N 776/703/509/507/1820/42/535/398/68 г. Москва: офиц. текст по состоянию на 05.03.2018 // Российская газета. – 13.12.2013. – №6258. - С. 88-93.
13. Стандарт осуществления адвокатом защиты в уголовном судопроизводстве: офиц. текст по состоянию на 20.03.2018. // Вестник Федеральной палаты адвокатов Российской Федерации. – 2017. - №2.

Судебная практика

14. По жалобе граждан Вахонина Александра Ивановича и Смердова Сергея Дмитриевича на нарушение их конституционных прав частью третьей статьи 220.2 УПК РСФСР: определение Конституционного Суда России от 24.04.2002 № 114-О: офиц. текст по состоянию на 10.03.2018 // Вестник Конституционного Суда Российской Федерации. - №6. – 2002.
15. По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова: постановление Конституционного Суда России от 26.10.2017 N 25-П: офиц. текст по состоянию на 02.03.2018 // Российская газета. - № 259. – 16.11.
16. О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением Конституционных прав граждан: постановление Пленума Верховного Суда России от 01.06.2017 №19: офиц. текст по состоянию на 03.03.2018 // Бюллетень Верховного Суда России. – 01.07.2017. - №19.
17. Бюллетень Верховного Суда России. - 2003. - №8. – С.18, 19.

Учебники, учебные пособия

18. *Безлепкин Б.Т.* Настольная книга следователя и дознавателя / Б.Т. Безлепкин. — М.: Проспект. – 2016. — 252 с.
19. *Галяшина Е.И.* Настольная книга судьи: судебная экспертиза. / Е.И. Галяшина. – М: Проспект. – 2013. – 502 с.
20. *Гармаев Ю.П.* Использование результатов оперативно-розыскной деятельности при расследовании уголовных дел о взяточничестве. / Ю.П. Гармаев, – Иркутск: ИИПК ПР ГП Российской Федерации. - 2014. – 441 с.
21. *Новолодский Ю.М.* Доказывание в практической деятельности адвоката-защитника. / Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2016. - 256 с.

22. *Новолодский Ю.М.* Школа уголовной защиты Юрия Новолакского. Путь к мастерству, первые стадии. / Ю.М. Новолодский. – СПб: ООО «Р-КОПИ». – 2017. – 124 с.

Научные статьи

23. *Багмет А.М.* Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств. / А.М. Багмет, С.Ю. Скобелин. // Сборник статей «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях». Тюмень: Издательство «ТГАМЭУП». – 2013. – №10 (ч. 2) С. 106-111.

24. *Гаврилов М.В.* Наложение ареста на электронную почту, ее осмотр и выемка. / М.В. Гаврилов, А.Н. Иванов. // журнал «Правоведение. Политология». М: Наука. – 2014. – №5 С. 103-111.

25. *Дубоносов Е.С.* Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и проблемы. / Е.С. Дубоносов. // Известия Тульского государственного университета. Тула: Издательство ТГУ. – 2017. – №4. С. 24-30.

26. *Ларинков А.А.* Проблемы представления результатов ОРД для использования в уголовном судопроизводстве (по инструкции от 27 сентября 2017). / А.А. Ларинков // журнал «Криминалистъ». М: ЮИ АГП Российской Федерации. – 2014. – №1 С. 34-40.

27. *Мальков С.* Квалификация сбыта наркотических средств, психотропных веществ или их аналогов с использованием электронных или информационно-телекоммуникационных сетей. / С. Мальков В. Винокуров. // журнал «Уголовное право». М: Право. – 2014. – №4. С. 25.

28. *Осипенко А.Л.* Новое оперативно-розыскное мероприятий «Получение компьютерной информации»: содержание и основы осуществления. / А.Л. Осипенко // Вестник Воронежского института МВД России. Воронеж: Издательство ВИ МВД России. – 2016. – №3 С. 83-90.

29. *Россинская Е.Р.* Судебная компьютерно-техническая экспертиза. / Е.Р. Россинская, А.И. Усов // журнал «Судебная экспертиза». – М: Аст-Пресс. - 2011. - С.99.

Электронные ресурсы

30. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда России от 17 октября 2013 г. N 50-АПУ13-26 // РосПравосудие. - URL: <https://rospravosudie.com> (дата обращения 02.03.2018).

31. Приговор Вахитовского районного суда города Казани республики Татарстан от 06.05.2014 по уголовному делу № 1-184/2014 // РосПравосудие. - URL: <http://sudact.ru/regular/doc/WyavwZ7DR958/> (дата обращения 03.03.2018).

32. Приговор Северского районного суда Краснодарского края от 24.06.2014 по уголовному делу № 1-175/10 // РосПравосудие. - URL: <https://rospravosudie.com/court-severskij-rajonnyj-sud-krasnodarskij-kraj-s/act-468893421> (дата обращения 03.03.2018).

33. Постановление Ленинского районного суда города Владивостока № 22-455/14 от 27.11.2014 // РосПравосудие. - URL: <https://rospravosudie.com> (дата обращения 02.03.2018).

34. Справка по приговору № 1-51/2017 от 17.07.2017 // Карточка судебного делопроизводства Тобольского районного суда URL: <https://tobolsky--tum.sudrf.ru/modules.php> (дата обращения 04.03.2018).

35. Спиридонов М.В. Изъятие электронных носителей информации без участия специалиста как основание для признания обыска незаконным. // М.В. Спиридонов. – Сайт адвоката Спиридонова М.В.: Практика адвоката Спиридонова М.В. по уголовным делам. URL: <https://адвокат-спиридонов.рф/изъятие-электронных-носителей/> (дата обращения 08.03.2018).

36. Шудрова. К. Интернет-мессенджеры: какое приложение обеспечит безопасность вашей переписки. Сайт газеты «Росконтроль». URL:

- <https://roscontrol.com/community/article/internet-messendgeri-kakoe-prilogenie-obespechit-bezopasnost-vashey-perepiski/> (дата обращения 29.03.2018).
37. Иванов А.Н. Выемка электронной почты в сети Интернет. Журнал «Законность» №05/2015 URL: <http://www.crime-research.org/library/Removing.html> (дата обращения 05.03.2018).
38. Videоблог адвоката Колегова А.В. «Адвокатские тайны»: «Исключение недопустимых доказательств». URL: <https://www.youtube.com/watch?v=HCX3IG5TyY4> (дата обращения 02.03.2018).
39. Videоблог адвоката Колегова А.В. «Адвокатские тайны»: «Как строить защиту по уголовному делу?». URL: <https://www.youtube.com/watch?v=> (дата обращения 03.03.2018).
40. Videоблог д.ю.н., профессора старшего советника юстиции в отставке Гармаев Ю.П. Лекция «Использование результатов оперативно-розыскной деятельности в расследовании уголовных дел о незаконном обороте наркотиков и о коррупционных преступлениях»: канал Ю.П. Гармаева на портале Yotube.com «Юрий Гармаев». URL: <https://www.youtube.com/watch?v=XCbVtg3MgqQ> (дата обращения 08.03.2018).
41. Официальный сайт ООО «Оксиджен Софтвер»: ПО «Мобильный криминалист». URL: <https://www.oxygensoftware.ru/ru/company/target/police> (дата обращения 06.03.2018).
42. Официальный сайт организации «COMPELSON Labs». URL: <http://www.mobiledit.com/company/> (дата обращения 06.03.2018).
43. Официальный сайт организации «Cellebrite Mobile Synchronization» LTD. URL: <http://lang.cellebrite.com/ru/mobile-forensics/products/standalone/ufed-touch-ultimate> (дата обращения 07.03.2018).

АННОТАЦИЯ. КЛЮЧЕВЫЕ СЛОВА

Проблемы электронной переписки в уголовно-процессуальном доказывании

В данной выпускной квалификационной работе была рассмотрена электронная переписка, как доказательство в уголовном процессе. Было проанализировано ее доказательственное значение, как в целом, так и на примере отдельных видов преступлений посредством анализа судебной практики. Также были рассмотрены особенности собирания, закрепления, проверки и оценки носителя, содержащего электронные сообщения. Были выявлены существующие проблемы, связанные с электронными переписками в уголовно-процессуальном доказывании, и пути решения данных проблем.

КЛЮЧЕВЫЕ СЛОВА:

Электронные переписки, мессенджеры, доказывание в уголовном процессе, уголовно-процессуальные правоотношения.

ABSTRACT. KEYWORDS.

Problems of electronic correspondence in criminal procedure proof

In this final qualification work electronic correspondence as the proof in criminal trial has been considered. Its evidentiary value as in general, and on the example of separate types of crimes by means of the analysis of jurisprudence has been analysed. Also features of collecting, fixing, check and assessment of the carrier containing electronic messages have been considered. The existing problems connected with electronic correspondences in criminal procedure proof, and a solution of these problems have been revealed.

KEYWORDS:

Electronic correspondences, messengers, proof in criminal trial, criminal procedure legal relationship.