МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ ПОЛУЧЕНИЯ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В ПРАВОПРИМЕНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ИЗ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ ИНТЕРНЕТ В ЦЕЛЯХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ»**

Выполнил
Закомалдин Александр Сергеевич
обучающийся по специальности
40.05.01 Правовое обеспечение национальной безопасности
2018 года набора, 812 учебного взвода

Руководитель
доцент кафедры криминалистики, кандидат технических наук
Харисова Зарина Ирековна

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2023 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Всемирная сеть Интернет, способствующая функционированию различных сервисов, услуг, социальных сетей, а также прочих ресурсов, длительное время является не только общественным благом, но и широко применяется в качестве инструмента совершения большого количества разнообразных правонарушений. Так в качестве примера можно привести незаконный сбыт наркотических средств и психотропных веществ, совершаемый бесконтактно посредством сети Интернет, при этом источником криминалистически значимой информации выступают непосредственно компьютерные данные и следы преступления, которые отражаются в электронном виде на различных ресурсах и материальных носителях. Получение такой информации является актуальной задачей и решается она различными способами. Злоумышленниками все чаще используются новые электронные способы и средства при совершении преступлений через сеть Интернет. Поэтому дальнейшее исследование проблем предупреждения, а также раскрытия и расследования преступлений в данной области, представляется достаточно актуальным.

Ресурсы сети «Интернет» могут быть использованы не только для совершения высокотехнологичных преступлений, но и служить платформой для размещения информационных объектов, которые впоследствии (при соблюдении процессуальных требований) будут иметь доказательственное значение в рамках расследования конкретного уголовного дела.

Для установления истины по уголовному делу следователю необходимо грамотно выстраивать свою работу, применяя не только приемы и рекомендации, выработанные криминалистической наукой при проведении отдельных следственных действий, но и в процессе фиксации сведений и действий, направленных на получение криминалистически значимой

информации, условий, при которых она была получена, для придания ей доказательственного значения.

Важность данной работы заключается в том, что изучение темы грамотной и оперативной фиксации информации в информационно-телекоммуникационных сетях способствует формированию навыков решения задач по раскрытию и расследованию преступлений.

Объект исследования выпускной квалификационной работы составляют общественные отношения возникающие в процессе получения информации, используемой в правоприменительной деятельности, из информационно-телекоммуникационных сетей, в том числе сети «Интернет» в целях раскрытия и расследования преступлений.

Предметом исследования выпускной квалификационной работы являются нормы законодательства Российской Федерации, регулирующие получение информации, используемой в правоприменительной деятельности, из информационно-коммуникационных сетей, в том числе сети «Интернет» в целях раскрытия и расследования преступлений.

Цель настоящей работы заключается в изучении правовых основ и способов получения информации, используемой в правоприменительной деятельности, из информационно-телекоммуникационных сетей, в том числе сети «Интернет» в целях раскрытия и расследования преступлений по материалам территориального органа внутренних дел.

Исходя из цели данной работы можно определить задачи исследования:

определить понятие «информационно-телекоммуникационные сети», а также сети «Интернет» в уголовном и уголовно-процессуальном законодательстве Рос. Фед.;

раскрыть основные методы фиксации доказательственной информации, хранящейся в ресурсах сети «Интернет» в целях раскрытия и расследования преступлений;

выявить особенности фиксации информации, содержащейся в сети «Интернет», в целях раскрытия и расследования преступлений;

рассмотреть проблемы, возникающие при необходимости фиксации доказательственной информации, содержащейся в сети «Интернет».

Особенностью выпускной квалификационной работы является рассмотрение методов «OSINT-разведки» – (open-source intelligence, с англ. – разведка на основе открытых данных) – методов сбора информации о преступнике или организации из открытых источников и ее последующий анализ.

Структура выпускной квалификационной работы состоит из оглавления, введения, двух глав, заключения и списка используемых источников. Работа основывается на нормативно-правовой базе и трудах современных ученых в рассматриваемой области.

Современный цифровой мир полон угроз, как для частных лиц, так и для государства и международного сообщества в целом. Не вызывает сомнения тот факт, что большинство современных информационных технологий обладают ярко выраженным враждебным потенциалом, способным быть направленным против интересов государства, а также прав и свобод отдельно взятой личности.

В начале апреля 2023 года Министерство внутренних дел Российской Федерации (далее – МВД РФ) опубликовало доклад по состоянию преступности в России.[1] В частности, в данной публикации отдельно упоминаются сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий. Количество таких преступлений по сравнению с аналогичным периодом прошлого года

[1] Статистика преступности в Российской Федерации. Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». URL: https://мвд.рф/reports/item/37377025 (дата обращения: 10.01.23).

существенно выросло, говорится в опубликованном МВД РФ докладе «Состояние преступности в России». По предоставленным данным в 2023 году количество преступлений, совершенных с помощью информационно-телекоммуникационных технологий возросло на 22,7% (см. приложение 1).

Также следует отметить, что удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий, по регионам доходит до 50,1%. (см. приложение 2).

Быстрый рост числа людей, пользующихся Интернетом и компьютерными технологиями, открыл новые возможности для преступной деятельности. Это коснулось и России, что подтверждается ростом зарегистрированных преступлений совершенных в сфере телекоммуникаций и компьютерной информации на территории Российской Федерации. Если в 2013 году было зарегистрировано 10942 преступления в указанной сфере, то в 2014 году – 10968, в 2015 году – 43816, в 2016 году – 65949, в 2017 году – 90587 преступлений.[1]

Исходя из приведенной статистики, можно обозначить важность решения проблем, связанных с получением информации из информационно-телекоммуникационных сетей и её своевременной фиксацией.

---

[1] Статистические сведения из сводных отчетов по России о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации за 2013-2017 годы // ИМТС МВД России. URL: https://мвд.рф/folder/101762 (дата обращения: 07.02.2023 г.)

ГЛАВА 1. ПРАВОВЫЕ ОСНОВЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В ПРАВОПРИМИНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ИЗ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ» В ЦЕЛЯХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 1. Понятие «информационно-телекоммуникационной сети» в уголовно-процессуальном законодательстве Российской Федерации

Глобальные процессы информатизации способствуют развитию преступной деятельности в информационной сфере, в связи с чем появляется необходимость внесения изменений в Уголовный кодекс Российской Федерации[1] (далее – УК РФ). Между тем, не все подобные изменения следует признать удачными. В частности, например, это касается установления ответственности за совершение преступлений с использованием электронных

[1] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 30.12.2021) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

сетей как альтернативы совершению преступления с использованием информационно-телекоммуникационных сетей (в том числе сети «Интернет»). На уровне специализированного законодательства не определено соотношение данных понятий, что предопределяет проблемы в квалификации деяний, а также сомнения в необходимости внедрения понятия «электронные сети» в УК РФ.

В условиях глобализации и стремительного развития общества в информационной сфере многие явления и процессы претерпели изменения, в том числе структура и форма современной преступности. Возросла угроза использования информационных технологий для совершения общественно-опасных посягательств, где информационное пространство стало новой платформой преступной деятельности.

Учитывая всемирные процессы глобализации закономерными являются изменения, которые происходят в действующем уголовном законодательстве. На сегодняшний день насчитывается шесть составов преступлений (ч. 1 ст. 171.2; п. «б» ч. 3 ст. 242; п. «г» ч. 2 ст. 242.1; п. «г» ч. 2 ст. 242.2, ч. 2 ст. 280, ч. 1 ст. 282 УК РФ), предусматривающих ответственность за совершение преступлений с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Кроме того, УК РФ содержит также четыре состава преступлений (ч. 1 ст. 185.3; ч. 2 ст. 205.2; ч. 2 ст. 280.1; п. «б» ч. 2 ст. 228.1 УК РФ), предусматривающие уголовную ответственность за совершение преступлений, с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Основой формулирования данного признака стало специализированное законодательство, в частности Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149). Между тем, вышеназванным Федеральным законом не используется и не раскрывается понятие электронных сетей, входящее в состав некоторых преступлений. В свою очередь, другие

понятия – «электронное сообщение», «электронный документ», – характеризуются как информация, обращающаяся в информационно-телекоммуникационных сетях[1].

Кроме того, используемое уголовным законодательством понятие информационно-телекоммуникационных сетей также нельзя признать удачным. ФЗ № 149 не разъясняет какие сети (типы сетей) входят в понятие информационно-телекоммуникационных сетей, что и породило проблему, связанную с внедрением понятия «электронные сети» в диспозиции некоторых составов преступлений. Данный пробел целесообразно устранить на уровне специализированного законодательства.

По мнению доктора юридических наук И. М. Рассолова[2], существовавшее ранее деление на типы сетей, различавшихся по их функциональной принадлежности, теряет актуальность сегодня под воздействием технологической конвергенции (слияния). Это означает, что все современные типы сетей объединены понятием «информационно-телекоммуникационные сети». В свою очередь, в экономической литературе, говоря об электронной сети авторы подразумевают, как правило, сеть «Интернет».

Исходя из вышеизложенного, следует сделать вывод о чрезмерности установления уголовной ответственности за совершение преступлений с использованием электронных сетей (ч. 1 ст. 185.3; ч. 2 ст. 205.2; ч. 2 ст. 280.1; п.«б» ч. 2 ст. 228.1 УК РФ) наравне с использованием информационно - телекоммуникационных сетей, что обусловлено рядом причин: во-первых на сегодняшний день не существует правового разъяснения понятия «электронные

---

[1] Ковлагина Д. А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом. 2016. С. 249. URL: https://moluch.ru/archive/120/33286/ (дата обращения: 03.02.2023).

[2] Рассолов И. М. Право и интернет // Теоретические проблемы. 2016. С. 251. URL: https://cyberleninka.ru/article/n/2004-03-014-rassolov-i-m-pravo-i-internet-teoreticheskie-problemy-m-norma-2003-336-s (дата обращения: 05.03.2023).

сети »; во-вторых, анализ правоприменительной практики не позволяет определить разницу в исследуемых понятиях («электронная сеть » и «информационно -телекоммуникационная сеть ») либо представляет их как взаимозаменяемые, синонимичные; в-третьих, в юридической литературе понятие «электронная сеть» приравнивается к понятию «сеть «Интернет »»; в-четвертых, цель (распространения действия нормы на все ресурсы сети «Интернет »), ради которой, в частности, было включено понятие электронные сети в диспозицию ч. 2 ст. 280.1 УК РФ может быть достигнута правильным конструированием нормы права (по типу ч. 2 ст. 280 УК РФ).

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена ст. ст. 158, 159, 159.3, 159.6 УК РФ.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» введена ответственность виновных лиц по статье 158 УК РФ за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ). Аналогичным образом, с целью усиления уголовной ответственности за противоправные действия с использованием электронных средств платежа, изменены диспозиции и

санкции статей 159.3 и 159.6 УК РФ. Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые на практике нередко используются в качестве инструментария завладения чужим имуществом. В целях борьбы с преступностью в сфере компьютерной информации в УК РФ предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно -телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).

Таким образом, сеть «Интернет » создает поле для совершения преступлений, но в тоже время способствует их раскрытию и расследованию. В свою очередь, для раскрытия и расследования вышеперечисленных составов преступлений необходимо определить аспекты фиксации доказательственной информации, хранящейся в ресурсах сети «Интернет». Стремительный технологический прогресс в современном обществе дает крупный потенциал, оставляя свой след во всех без исключения областях социальной жизни. Совершенствование цифровой экономики и технологий не только содействует развитию общества и государства, но также порождает трудности, вооружая правонарушителей новейшими способами совершения правонарушений.

§ 2. Некоторые аспекты фиксации доказательственной информации, хранящейся в ресурсах сети «Интернет», в целях раскрытия и расследования преступлений

Процесс расследования преступлений включает в себя производство следственных действий, проведение оперативно-розыскных и организационных мероприятий, которые направлены на сбор, исследование, фиксацию, оценку доказательственной информации и установление истины по уголовному делу.

В современных условия, способствующих существенному росту числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, возрастает значение ресурсов сети «Интернет » как глобального «резервуара», хранящего в себе значительные массивы криминалистически значимой информации, способствующей выявлению, раскрытию и расследованию преступлений.

Социальная среда в сетевом пространстве разнообразна. Отдельные ее представители, имеющие социально опасные взгляды, являются составляющей криминогенной среды. Объединение таких субъектов образуют маргинальные группы. Сетевое пространство создает комфортные условия для общения криминально настроенных субъектов с широким кругом населения не только в пределах одного региона, страны, но и мира. Этим можно объяснить количественный рост ресурсов с экстремистской направленностью; сайтов, популяризирующих преступные идеи и образ жизни, распространяющих детскую порнографию, наркотические и психотропные вещества, информацию по их изготовлению; предложения по продаже баз данных с персональными сведениями граждан, номерами кредитных карт и информацией об их владельцах, вирусных программ.

Возрастает разнообразие форм, средств и методов обработки цифровой информации, увеличивается ее общий объем, что зачастую не только способствует общественно одобряемым операциям с информацией, но и может иметь непосредственное отношение к преступной деятельности. Криминалистика должна адаптироваться к изменяющимся условиям, что требует не просто совершенствования, но и постоянного обновления криминалистических знаний о технических и тактических аспектах операций с

цифровой доказательственной информацией в процессе выявления, раскрытия и расследования преступлений.

Выявление, фиксация и изъятие следов неправомерного доступа к компьютерной информации играет определяющую роль в сборе доказательственной базы при расследовании данных преступлений. На основе информации, получаемой при изучении следов, могут быть построены версии об участниках преступления. Зная тонкости процесса образования следов неправомерного доступа к компьютерной информации можно судить о способе совершения преступления, действиях по сокрытию данного преступления, некоторых особенностях лица, совершившего преступление, а также об обстановке совершения данного преступления. Во многом следовая картина определяет тактику расследования преступления.

Как известно, процесс расследования преступлений включает в себя производство следственных действий, проведение оперативно-розыскных и организационных мероприятий, которые направлены на сбор, исследование, фиксацию, оценку доказательственной информации (этапы (стадии) процесса доказывания) и установление истины по уголовному делу.

Доказательство с позиций информационной теории уголовного права и процесса – это единство информации и ее материального носителя. Так, В. С. Балакшин [1], обоснованно считает, что доказательственная база основанная на знаково -информационной системе, в которую условно могут быть включены цифровая информация, содержащаяся на любом электронном носителе, сам носитель, а также процессуально регламентированный порядок сбора, проверки и оценки доказательств, размещенных

[1] Балакшин В. С. Доказательства в теории и практике уголовно-процессуального доказывания: Важнейшие проблемы в свете УПК Российской Федерации // Электронная библиотека. URL: https://search.rsl.ru/ru/record/01002945754 (дата обращения: 02.03.2023).

на электронных носителях (ст. ст. 81, 81.1, 164.1 Уголовно-процессуального кодекса Российской Федерации[1] (далее – УПК РФ) и др.).

Прежде чем рассматривать то, какие существуют особенности криминалистической фиксации цифровых следов и доказательств, необходимо разобраться с тем, что они представляют с точки зрения уголовно -правовой доктрины. В зарубежных источниках акцент сделан именно на цифровой сущности рассматриваемых доказательств; электронная природа носителя учитывается, однако интерес вызывает в первую очередь сама цифровая информация, а не ее носитель. При этом используемые термины могут либо отражать технико -криминалистическую сторону исследуемых объектов, их следовую сущность, либо отсылать к их доказательственному значению. Однако при составлении нормативных документов в большинстве государств используется термин «электронные доказательства ». Такой подход на сегодняшний день кажется самым правильным.

Необходимо рассматривать отдельные содержательные характеристики цифровой информации в контексте ее потенциального преобразования в уголовно -процессуальное доказательство. Так, можно выделить несколько видов характеристик:

опосредованность (существование цифровой информации невозможно без материального носителя);

возможность копирования без утраты объема и содержания копируемой информации (копия отдельного файла полностью ему идентична и может существовать (изменяться) безотносительно оригинала);

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. // Собр. законодательства Рос. Федерации. 2001. № 52. (ч. 1), ст. 4291.

одновременное существование нескольких копий (один и тот же фрагмент цифровой информации может быть зафиксирован на разных, зачастую удаленных друг от друга носителях, которые могут быть синхронизированы, доступ к такой информации могут одновременно иметь различные субъекты);

возможность преобразования в другие формы (так, содержание мультимедийного файла может быть преобразовано в аналоговую форму, скриншот или текстовый документ, которые можно распечатать и т.д.);

возможность существования на различных носителях;

необходимость применения специальных технических средств для восприятия цифровой информации;

обезличенность (в большинстве случаев установление автора или владельца цифровой информации может представлять существенную проблему для правоохранительных органов).

Фиксация доказательств – это удостоверительный процесс, направленный на закрепление криминалистически значимой информации в определенной процессуальной форме уполномоченным субъектом. Подобное мнение имеет законодательную основу [1].

В УПК РФ применяется такой термин, как «фиксация » (ст. 170, 177, 180, 190 УПК РФ). Однако в криминалистическую науку более устойчиво вошло именно по отношению к процессуальным и следственным действиям, направленным на удостоверение сведений, объектов, действий, условий, явлений, механизмов и др. понятие «фиксация». Употребление понятия

---

[1] Постановление Пленума Верховного Суда РФ от 31 октября 1995 г. №8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия: Постановление Пленума Верховного Суда Российской Федерации» (п.п. 16-18) в ред. от 03.03.2015 г. // Российская газета. 1995.

«фиксация » по лексическому значению более ёмкое и удачное, но не исключающее иные лексические синонимичные формы.

В соотношении «фиксация доказательств » и «криминалистическая тактика» одной из задач последней является подготовка и интеграция в практическую деятельность соответствующих современным требованиям способов и средств фиксации хода и результатов следственных и процессуальных действий.

Значительный вклад в комплексное формирование учения о фиксации доказательственной информации внес Р. С. Белкин, определив его место в системе частных криминалистических теорий [1]. Составной частью учения являются формы фиксации доказательственной информации. При этом комбинация форм при выборе тактики фиксации доказательственной информации, хранящейся в ресурсах сети «Интернет», имеет как общие рекомендации, разработанные учением о фиксации доказательственной информации, так и конкретные, характерные только для преступлений, совершенных посредством сети «Интернет », или для фиксации криминалистически значимой информации, хранящейся на сетевых интернет-ресурсах.

В качестве основных объектов фиксации доказательственной информации, размещенной в сети «Интернет», можно назвать следующее:

1. Сведения, указанные в ст. 74 УПК РФ, а именно лог-файлы (текстовые файлы, в которых хранится информация о пользователях, их взаимодействии с сервером, а также системная информация о работе сервера), сведения о сетевых ресурсах, доменах, их владельцах, базы данных с информацией конфиденциальной характера, иные файлы, хранящиеся на персональной электронно-вычислительной машине;

---

[1] Белкин Р. С. Курс советской криминалистики. Т. 2: Частные криминалистические теории // Академия МВД СССР. М. 1978. С. 121.

2. Условия, в результате которых стала возможна дальнейшая фиксация:

а) обнаружение криминалистически значимой информации в ходе мониторинга сетевых ресурсов, на которых пользователями неоднократно размещалась данная информация;

б) выявление информации об использовании при совершении преступления интернет-ресурсов в рамках расследования другого уголовного дела;

в) получение информации от граждан о размещении в сети «Интернет» публикаций, представляющих интерес;

г) заявление потерпевшего о преступлении;

д) получение информации в ходе проведенных оперативно -разыскных мероприятий;

3. Действия, связанные с фиксацией доказательств, и средства, способствующие выполнению этих действий.

К средствам, которые могут применяться следователями и специалистами для фиксации доказательственной информации по рассматриваемому направлению, относятся:

а) специальные технические средства, нацеленные на перехват криминалистически значимой информации, предоставляемой впоследствии органам предварительного расследования;

б) программное обеспечение с возможностями контент -анализа[1] (формализованный метод, основанный на изучении исследуемой текстовой и графической информации содержимого файлов в целях выявления и измерения характеристик, получивших в них отражение, с последующим выявлением

[1] Багмет А. М., Бычков В. В., Скобелин С. Ю. Получение информации, содержащейся в средствах мобильной связи, с применением универсального устройства извлечения судебной информации: метод. рек. // Институт повышения квалификации Следственного комитета Российской Федерации. М. 2013. С. 12.

определенных закономерностей, способствующий повышению эффективности мониторинга сетевых интернет-ресурсов). Его объектами в основном являются информационные ресурсы и тексты в местах социального взаимодействия (социальные сети, форумы, блоги и др.), а также сетевые ресурсы с высокой потенциальной возможностью размещения информации криминального характера, из которых наиболее известными являются закрытые анонимные сети «DarkNet» (даркнет). Использование подобных технических возможностей позволяет обобщать и сопоставлять полученные материалы, благодаря которым возможно установление связей интересующих лиц, их контактных данных, выявить возможных соучастников;

в) программное обеспечение для восстановления удаленной, модифицированной, поврежденной информации с носителей.

Способы фиксации доказательственной информации включают в себя:

процессуальную составляющую, содержанием которой является установленная уголовно -процессуальным законодательством протокольная форма как отражение обстановки, действий, явлений и вербальных сигналов;

технико -криминалистическую составляющую, содержащую графическую форму (планы, схемы, рисунки, графики, чертежи), предметную форму (изъятие предметов в полном объеме или их частей, изготовление слепков, макетов, оттисков), наглядно-образную форму (фотосъемка и видеосъемка, скриншоты).

Согласно действующему уголовно -процессуальному законодательству и рекомендациям, разработанным криминалистами, фиксация доказательственной информации хранящейся в ресурсах сети «Интернет», осуществляется в ходе следующей деятельности:

составления протоколов осмотра места происшествия и прилагаемых к ним иллюстрационных таблиц, схем, планов, чертежей, распечаток экрана монитора («скриншотов »);

применения фото -видеосъемки, которым должно точно соответствовать зафиксированное в протоколе;

составления протоколов допросов потерпевших, представителей потерпевшего, свидетелей, подозреваемых, обвиняемых, экспертов, специалистов, переводчиков, понятых (в необходимых случаях);

составления протоколов обыска по месту жительства, работы, в офисах, серверных помещениях, и т. д.;

составления протоколов выемки договоров об оказании телематических услуг связи, счетов за предоставление услуг связи, протоколы данных о соединениях абонентов с сетью электросвязи и доступа в сеть «Интернет », архива электронного почтового ящика, архива запросов к поисковым системам сети «Интернет » (при наличии соответствующего постановления суда о наложении ареста на почтовые сообщения электронной сети), электронных журналов, отражающих проведенные компьютерные операции, технической документации, иных электронных документов на машинных носителях и др.;

составления протоколов осмотра предметов (персональных компьютеров, ноутбуков, планшетов, мобильных телефонов, Wi-Fi роутеров, модемов, серверов и др.), документов (протоколов данных о соединениях абонентов с сетью электросвязи и доступа в сеть «Интернет», технической документации, иных электронных документов на машинных носителях и др.);

приобщения к материалам дела различного рода справок, выписок, заверенных копий документов и др., полученных в ходе официальных запросов, имеющихся в материалах уголовного дела (истребованная в сотовых компаниях информация о соединениях абонентов и абонентских устройств с указанием месторасположения базовых станций; истребованная информация у модератора сайта, с которого осуществлено, например, мошенничество в сети «Интернет », для установления IP-адреса подозреваемого; истребованная информация о движении денежных средств, находящихся на банковских счетах потерпевшего, подозреваемого, обвиняемого, с отраженным временем

совершенных операций, IP-адресом устройства, с которого осуществлялись операции);

назначения в кратчайшие сроки компьютерной судебной экспертизы (либо иного вида экспертизы, необходимость в которой возникнет в результате расследования уголовного дела) по изъятым в ходе осмотра места происшествия, обыска, выемки предметам и получения заключения эксперта. Целесообразно не осуществлять предварительно запуск персональной электронно-вычислительной машины, отторжение носителей информации, чтобы значимая информация, находящаяся на них, не была стерта или повреждена программно -аппаратными комплексами защиты информации и впоследствии могла стать доказательством по уголовному делу.

Фиксация доказательственной информации, хранящейся в ресурсах сети «Интернет », может осуществляться и в ходе иных следственных действий (не упомянутых перечне, но предусмотренных уголовно-процессуальным законом), если в этом возникнет необходимость в рамках расследования уголовного дела с рассматриваемым нами направлением. Всегда следует помнить о том, что протокольная форма является обязательной (согласно уголовно -процессуальным нормам), а соответственно, и основной по отношению к другим формам фиксации.

При расследовании преступлений, совершенных в сети «Интернет », с использованием сетевого ресурса или в случае хранения информации, которая впоследствии может иметь доказательственное значение, на правильное отражения информации, часто имеющей технический характер, привлекаемые специалисты и эксперты криминалисты. Необходимо учитывать не только углубленные теоретические знания в области компьютерной техники, информационных технологий, программного обеспечения, которыми обладает узкий круг профессионалов, но и практические навыки, полученные в результате профессиональной деятельности, а также предметную специализацию эксперта и специалиста. Эти познания можно использовать не

только для грамотной фиксации, но и во время производства следственных действий, судебных экспертиз и дачи заключения специалиста, а также показаний эксперта и специалиста [1].

Следователь сталкивается при раскрытии преступлений и расследовании уголовных дел с интернет-ресурсами в случаях:

размещения видеороликов в социальных сетях, медиа -хостингах, которые при соблюдении процессуальных и тактико -криминалистических правил становятся доказательствами и (или) поводом для возбуждения уголовного дела;

наличия электронной переписки, несущей смысловую нагрузку для установления всех обстоятельств уголовного дела;

незаконного сбыта или пересылки наркотических средств, психотропных веществ или их аналогов; растений, содержащих наркотические средства или психотропные вещества посредством сети «Интернет »;

незаконной торговли оружием, боеприпасами и взрывчатыми веществами;

незаконной торговли специальными техническими средствами для негласного съема информации, запрещенными законодательством РФ;

незаконного оборота порнографических материалов, в том числе оборота порнографических материалов с изображением несовершеннолетних;

публичных призывов к осуществлению экстремистской деятельности, действий, направленных на нарушение территориальной целостности;

мошеннических действий в сфере информационных технологий [1].

---

[1] Васюков В. Ф., Клевцов В. В. Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений / под ред. А.Л. Осипенко. Воронеж: Воронежский институт МВД России. 2015. С. 82.

Иные варианты следует относить к высокотехнологичной преступности, со сложной структурной составляющей, имеющей квалифицированных специалистов технической направленности, теневые финансовые потоки. Такая высокотехнологичная преступность в начале XXI в. получила название – киберпреступность. Киберпреступность вызывает серьезные сложности в раскрытии и расследовании с точки зрения компьютерно - технической составляющей и имеет латентный характер.

Работая с информацией в интернет-пространстве, целесообразно учитывать следующее:

ссылки на ресурсы с точки зрения технического подхода содержат автоматический переход, аналогичный самому ресурсу (например, в ресурсах социальной сети содержаться ссылки на видео с экстремистским содержанием);

информация, размещенная на интернет -сайтах, динамична, в связи с чем при фиксации обязательно отражение времени и часового пояса;

выясняя источник распространения информации, устанавливают не личность пользователя, а учетные данные программно -аппаратной части;

при изъятии информации с систем хранения данных серверов изымается только необходимая информация, а не весь дисковый массив;

для установления причастности определенного субъекта к совершению преступлений, использовавшего сетевые интернет-ресурсы, осуществляется фиксация самого контента, а также лиц, его разместивших;

для того, чтобы размещенный в сети «Интернет» видео ролик стал доказательством, необходимо не только грамотно изъять его, но и

---

[1] Колычева А.Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет // Вестник Удмуртского университета. Серия «Экономика и право». 2017. №5. С. 111.

зафиксировать сведения о субъекте, его разместившем, с его последующим допросом.

Разработка системы теоретических положений и практических рекомендаций, направленных на удостоверительное закрепление содержательных сведений, размещенных во всемирной системе объединенных компьютерных сетей, об объектах, действиях, условиях, явлениях, механизмах, средствах и способах, отраженных на материальном носителе и отвечающих формам и требованиям уголовно-процессуального законодательства, играет значительную роль в борьбе с преступностью в рассматриваемой сфере.

Таким образом, сотрудникам органов внутренних дел в своей деятельности приходится часто сталкиваться с работой в информационно - телекоммуникационных сетях, поэтому необходимо детальней разобраться в особенностях и проблемах использования сети «Интернет » для раскрытия и расследования преступлений.

Глава 2. Особенности и проблемы использования сети «Интернет» сотрудниками органов внутренних дел.

§ 1. Особенности фиксации информации, содержащейся в сети «Интернет», в целях раскрытия и расследования преступлений

В настоящее время все большее количество граждан по всему миру проводят в сети «Интернет» значительное время, используя его правомерно, например в целях получения заработка и развлечения, однако существуют и те, кто использует информационно -телекоммуникационные сети в целях совершения преступлений. В такого рода сетях содержится большое количество информации, которая может содержать в себе сведения о запрещенных деяниях и иметь доказательственное значение по уголовному делу.

Так, полученная в сети «Интернет» информация подлежит фиксации. По вопросу определения понятия фиксации доказательств существуют различные точки зрения ученых. Так, по мнению Г. Э. Давтян [1], под фиксацией доказательства понимают закрепление, т.е. запечатление фактических данных в установленном законом порядке, что только и позволяет после этого считать их доказательствами по делу. А. В. Белоусовым фиксация доказательств определяется как регламентированная законом деятельность следователя и привлечённых или допущенных к участию в ней других лиц по процессуальному закреплению фактических данных посредством предусмотренных уголовно -процессуальным законом процедур (протоколирование, дополнительные средства фиксации, приобщение к делу предметов и документов и пр.)[2].

Р. С. Белкин[3] определяет фиксацию доказательств как систему действий по запечатлению в установленных законом формах фактических данных, имеющих значение для правильного разрешения уголовного дела, а также условий, средств и способов их обнаружения и закрепления.

Целью фиксации доказательств является закрепление фактических данных для придания им доказательственного значения и дальнейшего использования при расследовании уголовного дела.

При совершении преступных действий в сети «Интернет» остаются, как правило, информационные следы преступления, которые подлежат фиксации. Например, личные страницы пользователей, переписки в социальных сетях,

---

[1] Давтян Г. Э. Собирание и исследование доказательств в Уголовном процессе // Научный электронный архив. URL: http://econf.rae.ru/article/5391 (дата обращения: 02.02.2023). С. 18.

[2] Белоусов А. В. Проблема фиксации доказательств в досудебных стадиях уголовного процесса России: автореф. дис. ... кандит. юрид. наук / А. В. Белоусов. М. 2001. С. 27.

[3] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Российская Е. Р. Криминалистика. Учебник для вузов. М. 2000. С. 173.

скриншоты страниц, содержимое аккаунтов пользователей социальных сетей и т.д.[1]. Также фиксации подлежат лог-файлы (протоколы автоматической регистрации событий, происходящих при работе программного обеспечения), сведения о сетевых ресурсах, доменах, их владельцах, базы данных с информацией конфиденциального характера и иные файлы[2]. Структура криминалистически значимой информации, размещенной в сети «Интернет », с точки зрения ее формы в целом, аналогична электронным доказательствам. Обнаружение информации, даже осуществленное лицом, наделенным процессуальными полномочиями, еще не превращает информацию в доказательство по уголовному делу. Для процессуального закрепления и получения возможности трансформации информации о наблюдаемом интернет-объекте в доказательство следует выполнить ряд требований по правильной его фиксации[3].

Фиксация информации, содержащейся в сети «Интернет », может осуществляться следующими способами:

1. Составление протокола следственного действия с приложением к нему электронных носителей информации, полученных или скопированных с других электронных носителей информации в ходе производства следственного

---

[1] Введенская О. Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. №4. С. 20.

[2] Колычева А. Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет // Вестник Удмурсткого Университета. Серия экономика и право. 2017. № 2. С. 110.

[3] Кульмухамбетова Н. А. Особенности фиксации информации при расследовании преступлений экстремистской направленности в глобальной сети «Интернет» // Новый юридический вестник. Саратов. 2019. №1. С. 59.

действия (ч. 8 ст. 166 УПК РФ)[1]. Например, при осмотре компьютера в переписке в социальной сети был обнаружен документ формата Word, который был скопирован специалистом на компакт-диск;

2. Составление протокола следственного действия с приложением к нему материалов фото - и видеосъемки. Например, для фиксации информации с интернет-сайта следователем производилась фотосъемка страницы сайта;

3. Составление протоколов допроса участников уголовного судопроизводства, которые могут подтвердить или опровергнуть наличие информации в сети «Интернет ». Так, понятой на допросе может подтвердить или опровергнуть факт наличия в сети «Интернет» информации в месте и во время производства следственного действия;

4. Составление протокола осмотра и выемки предметов, которые использовались для размещения информации в сети «Интернет»;

5. Приобщение к материалам дела справок, выписок, заверенных копий документов, полученных в ходе официальных запросов, имеющихся в материалах уголовного дела. Например, истребованная в сотовых компаниях информация о соединениях абонентов и абонентских устройств с указанием месторасположения базовых станций;

6. Назначение соответствующего вида экспертизы по изъятым электронным носителям[2].

Вышеизложенные способы фиксации могут использоваться как отдельно, так и в совокупности.

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. № 249.

[2] Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 59.

В качестве примера способов фиксации информации, полученной в сети «Интернет », можно привести уголовное дело из производства СУ УМВД России по г. Кургану о возбуждении ненависти либо вражды, а равно унижении человеческого достоинства, которым установлено, что у подсудимого по мотивам национальной ненависти возник преступный умысел на совершение публично, с использованием социальной сети «ВКонтакте », действий, направленных на возбуждение ненависти и вражды, унижение достоинства человека и группы лиц по признакам расы, национальности и происхождения, а также принадлежности к социальной группе, путем размещения на своей странице в социальной сети «ВКонтакте» информационного материала, представленного в виде видеофайла. Доказательствами, подтверждающими вину подсудимого, были признаны показания оперуполномоченного, который сообщил, что им с участием понятых в служебном кабинете была просмотрена страница подсудимого «ВКонтакте ». Было просмотрено около 17 видеороликов. Просмотренная информация была записана на диск, который был направлен для исследования. Также просмотренная информация была зафиксирована и распечатана на бумажном носителе. Доказательствами по делу также являлись показания понятого, который подтвердил факт просмотра видеороликов на компьютере в служебном кабинете и копирования информации на CD-диск; показания специалиста; протокол осмотра сайта сети «Интернет » в ходе которого обнаружено 13 видеороликов, направленных на возбуждение ненависти или вражды; протокол осмотра предметов: флэш-карты, двух ноутбуков модели «ASUS », компакт-диска с видеороликами, записанными в ходе осмотра страницы подсудимого «ВКонтакте»[1] .

Фиксация информации, содержащейся в сети «Интернет», требуется при расследовании различных категорий преступлений, например, клеветы; нарушения неприкосновенности частной жизни; кражи; мошенничества;

[1] Уголовное дело № 11901370001000*** // Арх. СУ УМВД России по г. Кургану. 2019.

незаконного приобретения наркотических средств, психотропных веществ или их аналогов; возбуждения ненависти либо вражды, а равно унижения человеческого достоинства; подделки, изготовления или сбыта поддельных документов, государственных наград, штампов, печатей, бланков и так далее. Так, подсудимая вступила с неустановленным лицом, в отношении которого материалы уголовного дела выделены в отдельное производство, в преступный сговор, направленный на сбыт поддельных бланков листов нетрудоспособности. В сети «Интернет » на одном из сайтов неустановленное лицо разместило информацию для неопределенного круга лиц о возможности приобретения листов нетрудоспособности «задним числом », без фактического обращения к врачу, и контактный телефон, по которому можно заказать данные документы. Доказательством по делу являлся, в том числе, протокол осмотра предметов (документов): был осмотрен персональный компьютер, состоящий из монитора и системного блока, подключенный к сети «Интернет ». В поисковой системе был напечатан запрос на поиск «купить больничный ». После чего в результатах поиска, вторым по счету сверху, был установлен соответствующий сайт. При открытии сайта с названием «Купить больничный лист » обнаружена заставка с изображением медицинского персонала, на главной странице размещена информация о номерах телефонов для звонков. На сайте расположена информация о покупке листков нетрудоспособности задним числом, имеется образец, где указано, каким образом осуществляется его заполнение согласно требованиям законодательства РФ[1].

Достаточно распространенным в настоящее время является совершение преступлений с использованием сети «Интернет » в области незаконной деятельности с наркотическими веществами. Проанализировав судебную

---

[1] Приговор по уголовному делу № 1-130/2018 от 23 мая 2018 г. // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/byG53COUhsdC/ (дата обращения: 03.02.2023).

практику по данной категории дел, можно сказать, что сеть «Интернет» используется для приобретения наркотических веществ, для организации незаконного сбыта наркотических веществ, а также для поиска и обучения лиц последующему сбыту наркотических веществ (приговор суда по делу № 1-155/2018 от 24 мая 2018 года [1], приговор суда по делу № 1-11/2018 от 21 мая 2018 года , приговор суда по делу № 1-383/2018 от 17 мая 2018 года).[2]

Указанные обстоятельства свидетельствуют о том, что сеть «Интернет » активно используется для совершения преступлений, постоянно появляются новые способы применения сети «Интернет » в противоправных целях, что требует повышенного внимания, в том числе к вопросам фиксации информации, содержащейся в сети «Интернет », со стороны законодателя и правоприменителя.

При этом при фиксации информации, содержащейся в сети «Интернет», возникают различные проблемы. Так, информация в сети «Интернет » может достаточно быстро изменяться или удаляться автором или иными лицами, особенно информация из социальных сетей и приложений для общения – записи на странице в социальной сети, комментарии, личная переписка. Виновный может удалить информацию из сети «Интернет », в том числе, если ему станет известно о желании потерпевшего обратиться в правоохранительные органы или о факте обращения потерпевшего в данные органы. В связи с этим, при проведении следственных действий необходимо

---

[1] Приговор по уголовному делу № 1-155/2018 от 24 мая 2018 г. // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/j5SHiM7pqd1b/ (дата обращения: 03.02.2023).

[2] Приговор по уголовному делу № 1-383/2018 от 17 мая 2018 года // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/eTzWQk4X36Yj/ (дата обращения: 03.02.2023)

обращать внимание его участников на факт наличия информации в сети «Интернет » в установленное время.

Также в действующем законодательстве не содержится указаний на незамедлительность фиксации информации из электронной среды при проверке сообщения о преступлении.

В соответствии со ст. 144 УПК РФ дознаватель, орган дознания, следователь, руководитель следственного органа обязаны принять, проверить сообщение о любом совершенном или готовящемся преступлении и в пределах компетенции принять по нему решение в срок не позднее 3 суток со дня поступления указанного сообщения.

За установленный законом промежуток времени для рассмотрения сообщения о преступлении есть вероятность утраты информации из сети «Интернет », что может повлечь за собой нарушение прав лица, потерпевшего от преступления. Также при поступлении сообщения о совершении преступления небольшой тяжести, например, клеветы, нарушения неприкосновенности частной жизни, сотрудники следственных органов могут умышленно затягивать срок проведения проверки сообщения о преступлении, так как не желают впоследствии заниматься расследованием преступлений данной категории.

В связи с изложенным целесообразно внести изменения в УПК РФ, дополнив ч.1 ст. 144 УПК РФ указанием на незамедлительность и неотложность осмотра и фиксации информации, которая может быть утрачена за небольшой промежуток времени, при поступлении сообщения о преступлении, в том числе информации, содержащейся в сети «Интернет ».

Необходимо отметить, что в действующем законодательстве не предусмотрен порядок фиксации информации, содержащейся в сети «Интернет », стороной защиты на досудебной стадии. В соответствии со ст. ст. 119, 120 УПК РФ для фиксации информации, содержащейся в сети «Интернет », защитник должен заявить дознавателю, следователю соответствующее

ходатайство, например, об осмотре и фиксации содержимого интернет-страницы. В случае удовлетворения ходатайства информация будет зафиксирована и в дальнейшем может приобрести статус доказательства. Постановление об отказе в удовлетворении ходатайства может быть обжаловано в установленном законом порядке прокурору, руководителю следственного органа либо в суд. Однако за установленный на обжалование промежуток времени существует вероятность утраты информации, содержащейся в сети «Интернет ». В связи с этим, целесообразно обязать следователя производить фиксацию такой информации для дальнейшей ее оценки. Для реализации права стороны защиты на фиксацию информации, содержащейся в сети «Интернет », мы поддерживаем точку зрения О.В. Овчинниковой, которая предлагает дополнить ст. 159 УПК РФ ч. 2.3 нормой следующего содержания: «Стороне защиты не может быть отказано в удовлетворении ходатайства об осмотре и копировании электронной информации, находящейся в глобальной сети «Интернет», если она заявляет, что эта информация подтверждает обстоятельства, подлежащие доказыванию по уголовному делу »[1].

Также, несмотря на введение Федеральным законом «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно -процессуальный кодекс Российской Федерации » ст. 164.1 УПК РФ, регулирующей особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий, некоторые вопросы, связанные с участием специалиста при производстве следственных действий, остаются неясными.

---

[1] Овчинникова О.В. Проблемы собирания электронных доказательств стороной защиты // Вестник Южно-Уральского Государственного Университета. Челябинск. 2018. № 3. С. 30.

Так, в соответствии с ч. 2 ст. 164.1 УПК РФ электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя, содержащейся на них информации, специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Согласно ч. 3 ст. 164.1 УПК РФ следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. Таким образом, копирование информации с электронного носителя возможно следователем и без участия специалиста, если не осуществляется изъятие электронного носителя информации.

Данная позиция законодателя разделяется и судебной практикой. Например, в приговоре по делу о разбое указано, что УПК РФ участие специалиста предусмотрено лишь при изъятии электронных носителей в ходе выемки. В данном случае в ходе осмотра места происшествия производилось лишь копирование информации (видеозаписи) без изъятия самого электронного носителя этой информации. Данная видеозапись была осмотрена и приобщена к материалам уголовного дела в качестве вещественного доказательства в соответствии с УПК РФ, ее источником являлся сервер с видеозаписями с камер видеонаблюдения комплекса красоты и отдыха «Причал»[1]. Также по делу № 1-112/2017 мнение защитника о недопустимости протоколов выемки и осмотра телефона, поскольку в данных следственных действиях не принимал участие специалист, суд признал несостоятельными. Так, вопреки доводам стороны защиты, выемка телефона и осмотр фотоснимков, находящихся в нём, не относятся к изъятию электронных носителей информации, поэтому не требует обязательного участия специалиста

[1] Уголовное дело № 12001370001000*** // Арх. СУ УМВД России по г. Кургану. 2020.

в соответствии с ч. 3.1 ст. 183 УПК РФ. При этом указанные следственные действия проведены в присутствии законного владельца телефона, с его согласия[1].

Таким образом, следователь может произвести действия, направленные на фиксацию информации из сети «Интернет », без участия специалиста. Например, при осмотре компьютера сделать скриншот или распечатать содержимое интернет-страницы.

Спорным также является вопрос об обязательном участии специалиста во всех действиях (мероприятиях), связанных с изъятием информации, содержащейся в сети «Интернет », с электронных носителей информации. В литературе высказываются разные мнения, практика вырабатывает различные подходы. Эффективность, целесообразность и минимизация ущерба для участников – вот основные критерии, которыми должны руководствоваться следователь, дознаватель, а также сотрудник оперативного подразделения при изъятии и фиксации доказательств. При этом надо отметить, что в большинстве случаев, как правило, применяется изъятие электронных носителей информации, что вряд ли совпадает с интересами их владельца (недопустимость, за исключением отдельных случаев, изъятия электронных носителей информации установлена ч. 4.1 ст. 164 УПК РФ только применительно к производству по уголовным делам в сфере предпринимательской или экономической деятельности). Например, изъятию на длительный срок нередко подлежит мобильный телефон, планшетный компьютер, ноутбук [2]. В настоящее время как доказательства особо актуальны

---

[1] Уголовное дело № 12001370001000*** // Арх. СУ УМВД России по г. Кургану. 2020.

[2] Зуев С. В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования // Вестник Южно-Уральского государственного университета. Серия: Право. 2017. № 1. С. 33.

электронные сообщения, передаваемые при помощи мобильных устройств [1]. При этом нередко необходимость участия специалиста при изъятии мобильного телефона отсутствует.

Норма об обязательном участии специалиста при производстве следственных действий закреплена в ч. 2 ст. 164.1 УПК РФ одновременно с нормой, устанавливающей требование к специалисту осуществить копирование информации на другие носители, предоставленные законным владельцем изымаемых носителей или обладателем содержащейся на них информации, по их ходатайству. Это позволяет предположить, что необходимость участия специалиста связывается с его обязанностью произвести копирование информации с изымаемых носителей при наличии ходатайства определенных в законе лиц. В таком случае изъятие электронных носителей информации, если ходатайство на копирование информации не заявлено, не требовало бы присутствия специалиста. Однако правомерна и иная точка зрения, согласно которой участие специалиста направлено главным образом на грамотное проведение изъятия электронных носителей информации и обеспечение их правильного хранения в последующем, а копирование информации выступает для него лишь сопутствующей задачей [2].

В связи с изложенным представляется возможным допускать изъятие электронных носителей информации при производстве следственных действий без участия специалиста, если электронные носители информации изымаются

---

[1] Джафарова Н. Т., Васюков В. Ф. К вопросу об использовании цифровой информации при расследовании уголовных дел // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью. 2016. С. 135.

[2] Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. Воронеж. 2014. № 1. С. 158-159.

целиком, их изъятие производится без копирования содержащейся на них информации и не требует специальных познаний[1].

Также нередко бывает сложно определить место совершения преступления, связанного с распространением информации в сети «Интернет », что впоследствии затрудняет фиксацию информации. Сведения о местонахождении предмета, с которого размещалась информация в сети «Интернет », а также информацию о местонахождении виновного можно получить после установления интернет -провайдера, выяснения IP-адреса компьютера и его местонахождения. Однако размещение информации может быть произведено как со стационарного компьютера, так и через систему беспроводного доступа в сеть «Интернет » в местах общего пользования, например, в развлекательных центрах, кафе. В этом случае определить место совершения преступления становится технически невозможно. В результате сообщения о преступлении нередко неоднократно передаются по подследственности, что может привести к затягиванию сроков проверки сообщения о преступлении, утрате доказательств и невозможности их последующей фиксации [2].

Законодательное регулирование указанной проблемы также отсутствует. В ч. 1 ст. 152 УПК РФ указано, что предварительное расследование производится по месту совершения деяния, содержащего признаки преступления. Согласно ч. 4 ст. 152 УПК РФ предварительное расследование может производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков. Однако на начальном этапе предварительного

---

[1] Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий. 2018. № 4. С. 59.

[2] Овчинникова О. В. Собирание электронных доказательств, размещенных в сети «Интернет» // Правопорядок: история, теория, практика. Челябинск. 2016. № 4. С. 69.

расследования место преступления может быть неизвестно, обвиняемый и свидетели могут быть также еще не установлены.

В данном случае для обеспечения прав потерпевшего, а также своевременного обнаружения и фиксации информации, содержащейся, в том числе в сети «Интернет », целесообразно дополнить ч. 4 ст. 152 УПК РФ возможностью производства предварительного расследования по месту жительства потерпевшего. Указанная возможность закреплена в ч. 4.1 ст. 152 УПК РФ применительно к преступлениям, совершенным вне пределов РФ. При внесении таких изменений сообщение о преступлении при невозможности установления места совершения преступления будет передано по подследственности по месту жительства потерпевшего, что исключит многократную передачу по подследственности и возможную утрату доказательств.

Таким образом, информация, содержащаяся в сети «Интернет», имеет важное значение при расследовании уголовного дела. Особенностью такой информации является возможность ее быстрой утраты-изменения или удаления пользователем. В связи с этим фиксировать информацию, содержащуюся в сети «Интернет», следует незамедлительно. Пробелом в действующем законодательстве является: отсутствие указания на незамедлительность фиксации информации при поступлении сообщения о преступлении, неопределенность места производства предварительного расследования при невозможности установления места совершения преступления и т.д., создают проблемы в своевременной фиксации информации, содержащейся в сети «Интернет», затягивают сроки предварительного расследования. Указанные пробелы нуждаются в устранении, так как сеть «Интернет » продолжает развиваться и активно использоваться.

Нынешнее общество нельзя представить без применения компьютерных технологий, а всемирная сеть «Интернет» стала необходимым элементом существования людей. Стоит отметить, что всякий пользователь интернет -

гаджетов сохраняет личный «интернет -след», пользуясь всеми возможностями сети «Интернет ». В свое время органы внутренних дел могут использовать, оставленные пользователями «интернет-следы » для раскрытия и расследования преступлений. Отличительная черта деятельности многих полицейских ведомств европейский государств напрямую ориентирована на предупредительную работу, по этой причине следует сосредоточить внимание на применение элементов поиска информации из открытых источников данных. Одним из таких элементов является OSINT-ресурсы.

OSINT-разведка (с англ. open-source intelligence – разведка на основе открытых источников данных) – это методы сбора информации о человеке или организации из общедоступных интернет-ресурсов и ее последующий анализ.

К преимуществам OSINT -разведки (далее – OSINT) можно причислить открытость источников данных, размер ресурсов данных, простоту последующего применения, а кроме того, отсутствие расходов на приобретение данной информации.

Исходя из этого, применение методов и техник OSINT возможно расценивать в контексте работы органов внутренних дел в совокупности с иными элементами в рамках определенных моделей противодействия преступности.

В целях объективности использования OSINT в деятельности органов внутренних дел необходимо разделять принципы извлечения информации с открытых источников на общеправовые, которые соотносятся не только вместе с разведывательной и правоохранительной деятельностью, однако и вместе с всевозможными областями социальных отношений; ведомственные, отличительные только для подразделений, которые выполняют оперативно-розыскную либо следственную деятельность только в рамках уголовного производства.

Поиск интересующей информации с помощью OSINT производится через общедоступные информационные ресурсы посредством использования

информационно -поисковых систем. Каждая такая система имеет в своем составе одну или несколько поисковых машин. Поисковые машины представляют собой набор программ-роботов (поисковых программ), которые осуществляют сбор информации в общедоступных сетях в соответствии с установленными правилами.

Анализ информации, содержащейся в социальных сетях и на иных сайтах, хранящих персональные данные, открывает большие возможности для сбора информации о конкретном лице. Данная информация может быть полезна правоохранительным органам в целях раскрытия преступления и получения криминалистически значимой информации по уголовному делу.

Информация о злоумышленнике и о совершенном им деянии, добытая благодаря интернет-разведке OSINT, имеет важное значение для эффективного раскрытия преступления, выдвижения версии, грамотного применения тактических приемов при производстве следственных действий, планирования и организации подготовки проведения тактических операций (комбинаций), а также правильного выстраивания алгоритма действий на различных этапах расследования по уголовному делу. Для данных целей следователю (дознавателю), оперативным работникам и иным сотрудникам правоохранительных органов целесообразно использовать OSINT-сервисы, которые имеются в открытом доступе в сети «Интернет».

Применение приемов OSINT в множестве европейских государств сейчас считается необходимой составляющей деятельности органов внутренних дел, в особенности в период реализации криминалистического, а также экспертного сопровождения расследования правонарушений с целью отыскивания доказательной базы.

Таким образом, OSINT – комплекс методов, а также способов отыскивания данных в таких открытых источниках данных, как социальные сети, а также открытые базы данных в сети «Интернет ». Главными достоинствами OSINT считаются общедоступность источников, а также

отсутствие финансовых расходов с целью извлечения такого рода данных. Применяя технологии OSINT, органы внутренних дел способны: определить личность человека, совершившего преступное деяние, по фотографии; местоположение данной личности, которая находится в розыске, при помощи социальных сетей, в том числе личных страниц как разыскиваемого, так и его друзей; круг знакомств, а также увлечения подозреваемого, историю его передвижений с помощью рассмотрения геопозиционирования.

Однако, стоит отметить, что при фиксации доказательственной информации, содержащейся в сети «Интернет» возникает множество проблем.

§ 2. Проблемы, возникающие при фиксации доказательственной информации, содержащейся в сети «Интернет», в целях раскрытия и расследования преступлений

Информационно -телекоммуникационная сеть «Интернет», являясь самым популярным и необходимым средством коммуникации, играет огромную роль в жизни современного человека. Ежедневное использование самых различных программных приложений, основанных на принципах передачи цифровых данных для общения между людьми, стало нормой.

В сети «Интернет » содержится большое количество информации, в том числе сведения, которые могут иметь доказательственное значение для расследования и раскрытия преступлений. Они обязательно подлежат фиксации, под которой понимается регламентированная законом деятельность следователя и привлечённых или допущенных к участию в ней других лиц по процессуальному закреплению фактических данных посредством предусмотренных уголовно-процессуальным законом процедур [1].

[1] Губарева Е. К., Калентьева Т. А. Особенности фиксации информации, содержащейся в сети Интернет // Вестник Волжского университета им. В. Н. Татищева. 2019. № 2. С. 161.

К таким сведениям, как правило, относятся содержимое аккаунтов, переписки и информация со страницы пользователей в социальных сетях, блогах, лог-файлах, информация о доменах и сетевых ресурсах, а также иные файлы.

Фиксация информации, содержащейся в сети «Интернет », обычно осуществляется при расследовании таких преступлений, как клевета; мошенничество; незаконное приобретение и сбыт наркотических средств, психотропных веществ или их аналогов; нарушение равенства прав и свобод человека и гражданина; подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей, бланков, а также иных преступных деяний [1].

До настоящего времени уголовно -процессуальный закон не регламентировал в должной мере процедуру фиксации или изъятия указанной информации. Однако для того, чтобы такие сведения приобрели форму доказательств, представляется необходимым выполнить определённые требования по их фиксации, осуществляемой следующими способами:

1. Составление протокола следственного действия с приложением к нему электронных носителей информации, полученных или скопированных с других электронных носителей информации в ходе производства следственного действия в соответствии с ч. 8 ст. 166 УПК РФ;

2. Составление протокола следственного действия с приложением к нему материалов фото - и видеосъемки;

3. Составление протоколов допроса участников уголовного процесса, которые могут подтвердить или опровергнуть наличие информации в сети «Интернет»;

---

[1] Колычева А. Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет // Вестник Удмурсткого Университета. 2017. № 2. С. 110.

4. Составление протокола осмотра и выемки предметов, которые использовались для размещения информации в сети «Интернет»;

5. Приобщение к материалам дела справок, выписок, заверенных копий документов, полученных в ходе официальных запросов, имеющихся в материалах уголовного дела.

Вышеперечисленные способы фиксации могут быть использованы субъектом как по отдельности, так и в совокупности. Так, в качестве примера можно привести приговор Октябрьского районного суда г. Омска [1], которым установлено, что подсудимый разместил на своей странице в социальной сети «ВКонтакте » под именем «Денис Доронин » доступные неограниченному числу пользователей множество материалов (не менее 10 графических изображений), направленных по своему содержанию на возбуждение чувства ненависти и вражды, а также на унижение достоинства человека, группы лиц по признакам расы, национальности, происхождения, отношения к религии. В качестве доказательств, подтверждающих его вину, были использованы компакт-диск со скриншотами фотоизображений с личной страницы в социальной сети «ВКонтакте», системный блок черного цвета фирмы «DNS»; показания понятых, подтверждающие наличие фотографий на странице Доронина с изображением свастики; заключение эксперта.

Стоит отметить, что на практике возникают определённые проблемы, связанные с фиксацией информации, содержащейся в сети «Интернет ».

Во-первых, её можно достаточно легко изменить либо вовсе удалить, особенно в случаях, когда она содержится в социальных сетях или приложениях для общения, например, личные переписки, комментарии, записи на странице и так далее. Несмотря на это, действующее законодательство не

---

[1] Приговор № 1-134/2018 от 13 июня 2018 г. по делу № 1-134/2018 [Электронный ресурс] // URL: http://sudact.ru /regular/doc/NrVZXw0Z9PLh (дата обращения: 05.02.2023).

содержит требования о незамедлительности фиксации электронной информации при проверке сообщения о преступлении.

Так, ст. 144 УПК РФ устанавливает трёхсуточный срок со дня поступления указанного сообщения для его проверки, вследствие чего существует большая вероятность того, что в течение данного промежутка времени сведения из информационно -телекоммуникационной сети «Интернет», имеющие доказательственное значение, будут утрачены. Такой результат может повлечь за собой нарушение прав лица, потерпевшего от преступления, поскольку при таких обстоятельствах, установить (зафиксировать) факт наличия чего -то, что противоречило бы уголовному закону, представляется достаточно сложным либо вообще невозможным.

В связи с вышеизложенным представляется целесообразным внести некоторые изменения в ч. 1 ст. 144 УПК РФ, а именно дополнить её требованием о незамедлительном и неотложном производстве осмотра и фиксации информации, которая может быть утрачена за малый промежуток времени, при поступлении в правоохранительные органы сообщения о преступлении.

Во-вторых, имеются некоторые трудности, возникающие в случаях, когда на досудебной стадии сторона защиты желает зафиксировать сведения, содержащиеся в сети «Интернет ». Для реализации права на участие в доказывании адвокату необходимо в порядке ст. ст. 119, 120 УПК РФ заявить соответствующее ходатайство, только после удовлетворения которого информация может приобрести статус доказательства.

Стоит отметить, что следователь либо дознаватель вправе вынести постановление об отказе в удовлетворении ходатайства, которое, конечно, может быть обжаловано в порядке, предусмотренном УПК РФ, руководителю следственного органа, прокурору или в суд, однако в таком случае опять же существует вероятность того, что информация, имеющая значение для уголовного дела, будет утрачена в связи с удалением её автором или по иным

причинам, поскольку процедура обжалования занимает не слишком маленький промежуток времени.

В этой связи наиболее рациональным представляется подход, сущность которого заключается в том, чтобы установить обязанность для следователя (дознавателя) по фиксации таких сведений для их последующей оценки, что может быть обеспечено путём закрепления в ст. 159 УПК РФ нормы следующего содержания: «Стороне защиты не может быть отказано в удовлетворении заявленного ходатайства об осмотре и фиксации электронной информации, находящейся в информационно -телекоммуникационной сети «Интернет», если она заявляет о том, что эта информация устанавливает обстоятельства, подлежащие доказыванию по уголовному делу »[1].

Кроме того, актуальной остаётся проблема, связанная с определением мест совершения преступлений, связанных с распространением информации в сети «Интернет », что также порождает трудности при её фиксации. Это связано с тем, что размещение информации может быть осуществлено не только с домашнего компьютера, но и с помощью сетей Wi-Fi в местах общего пользования, таких как торгово -развлекательные комплексы, рестораны, гостиницы, аэропорты, метро и иной общественный транспорт [2]. В таком случае определение места совершения преступления становится технически сложным, а зачастую и вовсе нереальным, что приводит к увеличению сроков проверки сообщений о преступлениях, поскольку они часто передаются по подследственности, а следовательно, и к повышению вероятности

---

[1] Овчинникова О. В. Проблемы собирания электронных доказательств стороной защиты // Вестник Южно-Уральского Государственного Университета. Челябинск. 2018. № 3. С. 30.

[2] Волкопялова В. С. Проблемы, возникающие при необходимости фиксации доказательственной информации, содержащейся в сети «Интернет» // Вопросы российской юстиции. 2021. №12. С. 286.

невозможности последующей фиксации доказательств и их последующей потере.

По этой причине представляется целесообразным дополнить ч. 4 ст. 152 УПК РФ возможностью производства предварительного расследования по месту жительства потерпевшего.

Одной из наиболее серьезных проблем, является возможность пользователю быть анонимным, в то же время позволяя ему управлять содержимым страницы, то есть самостоятельно в любой момент времени поместить информацию, распространить ее и удалить ее первоисточник. Несмотря на то, что обязанность владельцев сайтов нести ответственность за содержимое их страниц законодательно закреплена, максимальная их ответственность будет заключаться в блокировании доступа к ресурсу, на котором была размещена информация. Однако может не получится установить личность злоумышленника, разместившего эту информацию.

Исходя из вышеизложенного следует сделать вывод о том, что информация, содержащаяся в сети «Интернет», зачастую имеет важное доказательственное значение для разрешения уголовных дел. Однако она легко подвергается изменениям и удалению пользователем, в связи с чем её необходимо оперативно фиксировать. Пробелы законодательства, исследованные в данной работе, порождают проблемы в правоприменительной практике и нуждаются в устранении, поскольку информационно-телекоммуникационная сеть «Интернет » стремительно развивается и активно используется.

ЗАКЛЮЧЕНИЕ

Сеть «Интернет » активно используется для совершения преступлений, постоянно появляются новые способы применения сети «Интернет » в противоправных целях, что требует повышенного внимания, в том числе к вопросам фиксации информации, содержащейся в сети «Интернет », со стороны законодателя и правоприменителя.

Информация, содержащаяся в сети «Интернет », имеет важное доказательственное значение для разрешения уголовных дел. Однако она легко подвергается изменениям и удалению пользователем, в связи с чем её необходимо своевременно фиксировать. Пробелы законодательства, исследованные в данной работе, порождают проблемы в правоприменительной практике и нуждаются в устранении, поскольку информационно-телекоммуникационная сеть «Интернет » стремительно развивается и активно используется.

Целью фиксации доказательств является закрепление фактических данных для придания им доказательственного значения и дальнейшего использования при расследовании уголовного дела.

На сегодняшний день не существует правового разъяснения понятия «электронные сети », при этом анализ правоприменительной практики не позволяет определить разницу в исследуемых понятиях («электронная сеть» и «информационно-телекоммуникационная сеть») либо представляет их как взаимозаменяемые, синонимичные. В современной литературе понятие

«электронная сеть» приравнивается к понятию «сеть «Интернет»», наряду с этим цель (распространения действия нормы на все ресурсы сети «Интернет»), ради которой, в частности, было включено понятие электронные сети в диспозицию ч. 2 ст. 280.1 УК РФ может быть достигнута правильным конструированием нормы права (по типу ч. 2 ст. 280 УК РФ).

Сеть «Интернет» за последнее десятилетие стала важной составной частью повседневной жизнедеятельности человека: как источник получения информации, как развлекательная платформа, как средство общения, как инструмент финансовых операций и пр. Несмотря на это следователи (чаще всего имея навыки владения компьютером на непрофессиональном уровне) испытывают затруднения в детальной работе с сетевыми ресурсами, их специализированной терминологией, механизмом работы и грамотным отражением в процессуальной и следственной форме.

Проанализировав судебную практику и практику СУ УМВД России по г. Кургану, можно сделать вывод, что при фиксации информации, содержащейся в сети «Интернет», возникают различные проблемы, которые требуют законодательного разрешения. Так, в действующем законодательстве не содержится указаний на незамедлительность фиксации информации из электронной среды при проверке сообщения о преступлении.

В связи с изложенным целесообразно внести изменения в УПК РФ, дополнив ч. 1 ст. 144 УПК РФ указанием на незамедлительность и неотложность осмотра и фиксации информации, которая может быть утрачена за небольшой промежуток времени, при поступлении сообщения о преступлении, в том числе информации, содержащейся в сети «Интернет».

В действующем законодательстве не предусмотрен порядок фиксации информации, содержащейся в сети «Интернет», стороной защиты на досудебной стадии. Для реализации права стороны защиты на фиксацию информации, содержащейся в сети «Интернет», предлагается дополнить ст. 159 УПК РФ ч. 2.3 нормой следующего содержания: «Стороне защиты не может

быть отказано в удовлетворении ходатайства об осмотре и копировании электронной информации, находящейся в глобальной сети «Интернет», если она заявляет, что эта информация подтверждает обстоятельства, подлежащие доказыванию по уголовному делу».

Для обеспечения прав потерпевшего, а также своевременного обнаружения и фиксации информации, содержащейся, в том числе в сети «Интернет», целесообразно дополнить ч. 4 ст. 152 УПК РФ возможностью производства предварительного расследования по месту жительства потерпевшего. Указанная возможность закреплена в ч. 4.1 ст. 152 УПК РФ применительно к преступлениям, совершенным вне пределов РФ. При внесении таких изменений сообщение о преступлении при невозможности установления места совершения преступления будет передано по подследственности по месту жительства потерпевшего, что исключит многократную передачу по подследственности и возможную утрату доказательств.

Кроме того, актуальной остаётся проблема, связанная с определением мест совершения преступлений, связанных с распространением информации в сети «Интернет», что также порождает трудности при её фиксации. Это связано с тем, что размещение информации может быть осуществлено не только с домашнего компьютера, но и с помощью сетей Wi-Fi в местах общего пользования, таких как торгово-развлекательные комплексы, рестораны, гостиницы, аэропорты, метро и иной общественный транспорт. В таком случае определение места совершения преступления становится технически сложным, а зачастую и вовсе нереальным, что приводит к увеличению сроков проверки сообщений о преступлениях, поскольку они часто передаются по подследственности, а следовательно, и к повышению вероятности невозможности последующей фиксации доказательств и их последующей потере.

По этой причине представляется целесообразным дополнить ч. 4 ст. 152 УПК РФ возможностью производства предварительного расследования по месту жительства потерпевшего.

С ежегодным ростом пользователей сети Интернет растет и число преступлений, совершаемых с использованием возможностей интернет-технологий. Фиксация доказательственной информации в ходе раскрытия и расследования таких преступлений вызывает значительные сложности у органов предварительного расследования. Связано это и с особенностью следовой картины, и с наличием специальных знаний (или пользовательского опыта) у следователя о работе ресурсов сети Интернет.

В целом, при фиксации доказательственной информации, хранящейся в ресурсах сети Интернет, следователю необходимо учитывать уголовно-процессуальные нормы, общие криминалистические рекомендации, технические особенности работы компьютерных систем и сетевого интернет-пространства, что позволит грамотно и оперативно расследовать и раскрывать различного рода преступления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 21 июля 2014 г. № 11-ФКЗ // Собр. законодательства Рос. Федерации. – 2014. – № 31, ст. 4398.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. // Собр. законодательства Рос. Федерации. – 2001. – № 52. (ч. 1), ст. 4291.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом

Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

4. О средствах массовой информации: федер. закон Рос. Федерации от 27.12.1991 № 2124–1-ФЗ: принят Верховным Советом России 27 декабря 1991 года.

5. О внесении изменений в статью 280.1 Уголовного кодекса Российской Федерации: федер. закон Рос. Федерации от 27.12.1991 № 2124-1: принят Гос. Думой Федер. Собр. Рос. Федерации 4 июля 2014 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 9 июля 2014 г.

II. Учебная, научная литература и иные материалы

1. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Российская Е. Р. Криминалистика: учеб. для вузов. М. 2000. 990 с.

2. Багмет А. М., Бычков В. В., Скобелин С. Ю. Получение информации, содержащейся в средствах мобильной связи, с применением универсального устройства извлечения судебной информации: метод. рек. М. 2013. 52 с.

3. Белкин Р. С. Курс советской криминалистики // Частные криминалистические теории. М. 1978. № 2. 410 с.

4. Белоусов А. В. Проблема фиксации доказательств в досудебных стадиях уголовного процесса России: автореф. дис. ... кандит. юрид. наук. М. 2001. 27 с.

5. Васюков В. Ф., Клевцов В. В. Проблемные аспекты привлечения специалиста к процедуре изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. материалов всерос. науч.-практ. конф. Воронеж. 2015. С. 80-84.

6. Введенская О. Ю. Особенности следообразования при совершении преступлений посредством сети «Интернет». Краснодар. 2015. № 4. 26 с.

7. Волкопялова В. С. Проблемы, возникающие при необходимости фиксации доказательственной информации, содержащейся в сети «Интернет» // Вопросы российской юстиции. Челябинск. 2021. №12. С. 286-292.

8. Губарева Е. К., Калентьева Т. А. Особенности фиксации информации, содержащейся в сети «Интернет» // Вестник Волжского университета им. В. Н. Татищева. 2019. № 2. С. 161-168.

9. Джафарова Н. Т., Васюков В. Ф. К вопросу об использовании цифровой информации при расследовании уголовных дел // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью. Орел. 2016. С. 132-139.

10. Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. Челябинск. 2018. № 4. С. 58-60.

11. Зуев С. В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования // Вестник Южно-Уральского государственного университета. Челябинск. 2017. № 1. С. 31-35.

12. Статистика преступности в Российской Федерации. Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». URL: https://мвд.рф/reports/item/37377025 (дата обращения: 10.01.23).

13. Колычева А. Н. Некоторые аспекты фиксации доказательственной информации, хранящейся в ресурсах сети «Интернет» //Вестник Удмуртского университета. Орел. 2017. №5. С.11-114.

14. Кульмухамбетова Н. А. Особенности фиксации информации при расследовании преступлений экстремистской направленности в глобальной сети «Интернет» // Новый юридический вестник. Саратов. 2019. №1. С. 58-60.

15. Овчинникова О. В. Проблемы собирания электронных доказательств стороной защиты // Вестник Южно-Уральского Государственного Университета. Челябинск. 2018. № 3. С. 30-31.

16. Овчинникова О. В. Собирание электронных доказательств, размещенных в сети «Интернет» // Правопорядок: история, теория, практика. Челябинск. 2016. № 4. С. 67-70.

17. Осипенко А. Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. Воронеж 2014. № 1. С. 158-159.

18. Астраханский суд приговорил общественного деятеля к двум годам колонии за комментарии в соцсети. URL: http://pravona.org/publikazii/astrahanski i-sud-prigovoril-obszestvennogo-deyatelya-k-dvum-godam-kolonii-za-kommentarii-v-socseti.html (дата обращения: 02.02.2023).

19. Давтян Г. Э. Собирание и исследование доказательств в Уголовном процессе. 30 с. URL: http://econf.rae.ru/article/5391 (дата обращения: 02.02.2023).

20. Ковлагина Д. А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом. 2016. С. 249-251. URL: https://moluch.ru/archive/120/33286/ (дата обращения: 03.02.2023).

21. Балакшин В. С. Доказательства в теории и практике уголовно-процессуального доказывания: Важнейшие проблемы в свете УПК Российской Федерации // Электронная библиотека DisserCat. 532 с. URL: https://www.dissercat.com/content/dokazatelstva-v-teorii-i-praktike-ugolovno-protsessualnogo-dokazyvaniya-vazhneishie-problemy (дата обращения: 02.03.2023).

22. Рассолов И. М. Право и интернет // Теоретические проблемы. 2016. 336 с. URL: https://cyberleninka.ru/article/n/2004-03-014-rassolov-i-m-pravo-i-internet-teoreticheskie-problemy-m-norma-2003-336-s (дата обращения: 05.03.2023).

23. Статистические сведения из сводных отчетов по России о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации за 2013-2017 годы // ИМТС МВД России. URL: https://мвд.рф/folder/101762 (дата обращения: 07.02.2023 г.)

III. Эмпирические материалы

1. О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия (п.п. 16-18) [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 31 октября 1995 г. №8. (ред. от 03.03.2015) Доступ из справ.-правовой системы «КонсультантПлюс». (дата обращения: 04.03.2023).

2. Уголовное дело № 11901370001000*** по ст. 282 УК РФ // Архивные данные СУ УМВД России по г. Кургану. 188 л.

3. Уголовное дело № 12001370001000*** по ст. 162 УК РФ // Архивные данные СУ УМВД России по г. Кургану. 230 л.

4. Уголовное дело № 12001370001000*** по ст. 158 УК РФ // Архивные данные СУ УМВД России по г. Кургану. 207 л.

5. Приговор по уголовному делу № 1-130/2018 от 23 мая 2018 г. // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/byG53COUhsdC/ (дата обращения: 01.02.2023).

6. Приговор по уголовному делу № 1-155/2018 от 24 мая 2018 г. // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/j5SHiM7pqd1b/ (дата обращения: 01.02.2023).

7. Приговор по уголовному делу № 1-383/2018 от 17 мая 2018 года // sudact.ru [Электронный ресурс] URL: http://sudact.ru/regular/doc/eTzWQk4X36Yj/ (дата обращения: 01.02.2023)

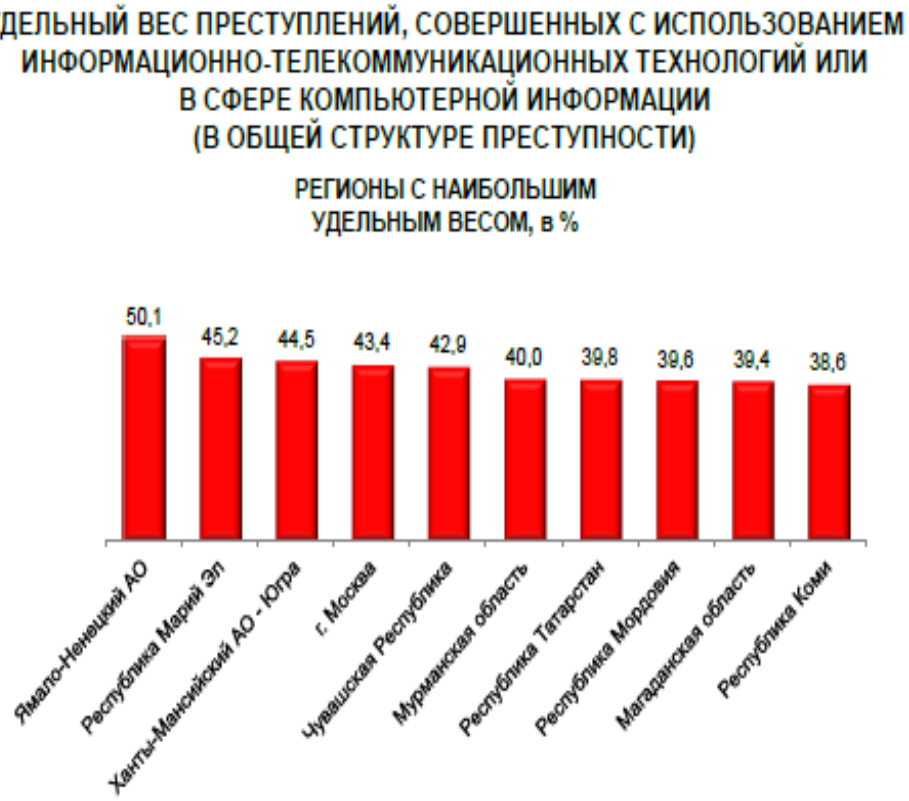
8. Приговор № 1-134/2018 от 13 июня 2018 г. по делу № 1-134/2018 [Электронный ресурс] // URL: http://sudact.ru (дата обращения: 05.02.2023).

ПРИЛОЖЕНИЕ 1

СВЕДЕНИЯ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

	ЗАРЕГИСТРИРОВАНО (в отчетном периоде)		в том числе выявленных сотрудниками		
	Всего	+,- в %	следственных органов Следственного комитета Российской Федерации	органов внутренних дел	органов Федеральной службы безопасности
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	**152434**	**22,7**	**447**	**150672**	**854**
из них тяжких и особо тяжких	81894	22,0	299	80894	492
в том числе совершенных с использованием или применением:					
расчетных (пластиковых) карт	30378	-4,5	61	30233	32
компьютерной техники	8111	-2,0	54	7739	228
программных средств	2141	7,3	18	2057	53
фиктивных электронных платежей	616	115,4	0	592	13
сети "Интернет"	115291	28,8	325	113998	647
средств мобильной связи	66055	34,1	111	65654	185
в том числе					
кража ст. 158 УК РФ	26689	-7,0	89	26555	6
мошенничества ст. 159, 159.3, 159.6 УК РФ	79448	28,8	29	79257	60
из них					
мошенничества ст. 159 УК РФ	77758	31,5	29	77575	52
мошенничества с использованием электронных средств платежа ст. 159.3 УК РФ	1467	-39,9	0	1463	4
мошенничества в сфере компьютерной информации ст. 159.6 УК РФ	223	125,3	0	219	4
незаконные организация и проведение азартных игр ст. 171.2 УК РФ	194	-0,5	4	182	8
публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма ст. 205.2 УК РФ	135	13,4	0	57	75
незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества ст. 228.1 УК РФ	21339	57,0	83	20991	201
изготовление порнографических материалов ст. 242, 242.1, 242.2 УК РФ	658	-26,8	47	604	1
публичные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ	116	-5,7	0	49	67
преступления в сфере компьютерной информации глава 28 УК РФ	4795	158,1	10	4641	115
в том числе					
неправомерный доступ к компьютерной информации ст. 272 УК РФ	4735	196,7	7	4609	91
создание, использование и распространение вредоносных компьютерных программ ст. 273 УК РФ	31	-57,5	0	23	7

ПРИЛОЖЕНИЕ 2



Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

А. С. Закомалдин