МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное образовательное учреждение высшего профессионального образования «Уфимский юридический институт»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему:«**ТАКТИКА СОБИРАНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ»**

Выполнил:
Беккер Илья Иванович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2017 года набора, 711 учебного взвода

Руководитель
доцент кафедры криминалистики,
кандидат технических наук
Харисова Зарина Ирековна

К защите рекомендуется
рекомендуется / не рекомендуется

Начальник кафедры _____ Э.Д. Нугаева
подпись

Дата защиты «___» _____ 2022 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

За последние несколько лет участились случаи совершения преступлений в сфере кибербезопасности и компьютерных преступлений. Это подтверждается и официальными статистическими данными МВД России. Так, например, число киберпреступлений за 2020 год достигло 510,4 тыс. случаев. В 2019 году было совершено 261 тыс. преступлений, что на 51,1% меньше, чем в 2020 году[1].

Стремительный рост компьютерной преступности в 2020 году связан с последствиями пандемии COVID-19, переводом сотрудников на дистанционную основу, сокращением рабочих мест и трудностями в сфере финансов. В 2018 году было зарегистрировано 121 247 киберпреступлений, в 2017 году – 90 587, 2016 – 66 000. Таким образом, с 2020 года количество преступлений, совершенных в киберпространстве, увеличилось в 7,7 раз, по сравнению с 2016 годом[2].

Стоит отметить, что показатели 2021 года схожи с показателями 2020 года, что говорит об устойчивости устремлений преступных элементов к рассматриваемым видам преступлений. Так, всего за 2021 год в изучаемой области зарегистрировано 517 тыс., зафиксировав таким образом рост преступности на 1,4 %. В большинстве случаев злоумышленники используют или применяют для совершения противоправных деяний возможности сети «Интернет» (351463 зарегистрированных уголовных дел), средства мобильной связи (217552 зарегистрированных уголовных дел) и расчетные (пластиковые) карты (165658 зарегистрированных уголовных дел)[3].

Приведенные данные свидетельствуют о том, что стабильно высокое

---

[1] Состояние преступности в России за январь - декабрь 2020 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/ 22678184 (дата обращения 12.03.2022).

[2] Современная кибербезопасность: учебное пособие [Текст] / Н. И. Долженко, Н. А. Жукова, И. А. Ярощук. Белгород: ИД «БелГУ» НИУ «БелГУ», 2021. 78 с.

[3] Состояние преступности в России за январь - декабрь 2021 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/28021552 (дата обращения 22.04.2022).

количество граждан подвергаются преступлениям в рассматриваемых сферах деятельности.

Большой урон наносится не только физическим лица, но и организациям, деятельность хакеров за последние годы представляет существенную угрозу для личных прав и свобод, а также сведений, охраняемых законом.

По информации банков ущерб рассчитывается в несколько миллиардов[1]. Кроме того, злоумышленники добытые преступным путем денежные средства выводят из-под российской юрисдикции с последующей легализацией. То есть совершение преступления в сфере кибербезопасности запускает цепь связанных противоправных деяние, формируя таким образом комплексное негативное явление.

Расследование компьютерных преступлений объективно является сложным процессом, поскольку фиксируется не только физический рост количества преступлений, но и растет подготовленность злоумышленников, они оставляют меньше следов.

Темпы ввода новых способов и средств противодействия этим преступлениям в практику правоохранительных органов не соответствуют складывающейся оперативной обстановке.

Практика показала низкий уровень подготовленности и грамотности граждан в области информационных технологий, недостаточную эффективность созданных инструментов противодействиях угрозам безопасности граждан, исходящих из киберпространства.

С учетом развития технологий, электронная информация становится важным источником доказательственной информации. Поэтому необходимо понимать насколько нынешнее уголовно-процессуальное законодательство соответствует изменяющейся окружающей действительности.

В настоящее время по поводу определения, содержания, а также

---

[1] Андриенко Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам / Ю. А. Андриенко // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). С. 154 (дата обращения 22.04.2022).

процессуального порядка получения, оценки и использования информации на электронных носителях ведутся активные научные дискуссии. Высказываются различные точки зрения, подчас противоположные и взаимоисключающие друг друга.

В числе актуальных вопросов находится правовая неопределенность понятия электронного носителя информации как источника доказательственной информации.

Недостатки правовой регламентации процессуального порядка получения доказательственной информации на электронных носителях отражаются на качестве расследования уголовных дел, правильности сбора и оформления доказательств в виде информации на электронных носителях.

Кроме того, противоречивость правоприменительной практики и недостаток научно обоснованных рекомендаций относительно порядка проверки и использования информации на электронных носителях негативно сказываются при решении задач уголовного судопроизводства.

Приведенные обстоятельства обуславливают актуальность темы настоящего исследования.

Степень научной разработанности темы исследования. Общие вопросы, связанные с криминалистическим обеспечением доказывания и проведения следственных действий исследовалась в работах И.Н. Соловьев, А.И. Долгова, Н.Ф. Кузнецова, В.В. Лунеев, М.И. Мамаев, Б.В. Волженкин, Н.Ф. Бережкова, Р.Н. Марченко, Л.Л. Кругликов, Н.О. Дулатбеков и других.

Непосредственное изучение вопросов использования электронной информации в качестве доказательств по уголовному делу освещалась в трудах таких ученых, как Ю.А. Андриенко, Е.К. Антонович, С.В.Бажанов, А.А.Балашова, Д.В. Бахтеев, В.Б. Вехов, А.И. Зазулин, В.Н.Григорьев.

Вклад этих ученых достаточно велик и весом в теорию по разработке методов работы с электронными носителями информации в рамках уголовного дела. Однако, важно отметить, что споров и дискуссий на эту тему также много и нет единого мнения по тому, как и каким методом бороться с

киберпреступностью.

Объектом выпускной квалификационной работы являются общественные отношения, возникающие в процессе сбора электронной информации в целях фиксирования следов преступления.

Предметом исследования выступает действующее уголовно-процессуальное законодательство, а также научные труды, раскрывающие место и роль электронной информации в процессе расследования преступлений, в том числе в сфере компьютерных преступлений и кибербезопасности.

Цель работы заключается в изучении методов и правил использования электронной информации в процессе доказывания по уголовному делу, а также теоретических и практических проблем работы следователя с электронной информацией.

Задачами дипломной работы являются:

определение понятия электронной информации и анализ классификаций электронных носителей информации;

рассмотрение характеристики правового режима отдельных видов информации, содержащейся на электронных носителях;

определение правого положения электронных носителей информации в системе видов доказательств;

рассмотрение процедуры сбора электронной информации, находящейся на отдельных носителях электронных информации и сетевых носителей;

рассмотрение процедуры сбора электронной информации, находящейся на сетевых носителях;

изучение особенностей проверки и оценки доказательственной информации на электронных носителях.

Методологической базой исследования является системный и комплексный подход к изучению проблемы использования электронной информации при доказывании по уголовному делу. В качестве методов исследования использованы анализ, синтез, классификация, обобщение,

моделирование, сравнение.

Информационной и теоретической базой в процессе написания научно-исследовательской работы являлись законодательные и нормативно-правовые акты Российской Федерации, учебники и учебные пособия отечественных и российских авторов, периодические издания

Эмпирическую базу исследования составили приговоры различных судов судебной системы Российской Федерации по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, в процессе расследования которых осуществлялось собирание доказательств на электронных носителях информации, анализ правовых позиций Конституционного Суда Российской Федерации и правоприменительной практики Верховного Суда Российской Федерации по исследуемым вопросам.

Работа состоит из введения, двух глав, объединяющих шесть параграфов, заключения и списка использованной литературы.

Электронная информация может содержать в себе признаки преступного деяния и иметь ключевое значение в процессе доказывания преступления. Электронная информация, как предмет виртуального мира, проявляется в процессе использования электронных носителей информации, которые выступают в качестве оболочки для цифровых сведений. Поэтому необходимо рассмотреть возможность совершенствования ст. 5 УПК РФ, добавив следующее понятие электронного носителя информации – устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Процессуальный порядок обнаружения, фиксации и изъятия доказательственной информации, содержащейся на электронных носителях, находится в прямой зависимости от вида такого носителя, технологии доступа к находящейся на нем информации, а также правового режима данной информации.

ГЛАВА 1. ПРАВОВАЯ ПРИРОДА ЭЛЕКТРОННОЙ ИНФОРМАЦИИ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВА ПРИ РАССЛЕДОВАНИИ УГОЛОВНОГО ДЕЛА

§ 1. Понятие электронной информации и классификация электронных носителей информации

Совершенствование цифровых технологий имеет значительный положительный экономический эффект, оптимизирует процессы производства, повышает эффективность и производительность труда. Появляется новое программное обеспечение, обеспечивающее работу искусственного интеллекта и иных систем, помогающих в принятии решений. В настоящее время оно используется на производственных предприятиях, в сферах предоставления услуг, а также и в государственном секторе.

Постепенный процесс совершенствования телекоммуникационных технологий требует соответствующего правового регулирования. При этом, зачастую принимаемые нормативные акты создают пробелы и коллизии законодательства, которыми пользуются преступники.

Кроме того, вслед за совершенствованием технического и программного обеспечения, совершенствуются методы работы и преступных схемы различных криминальных элементов.

С учетом принимаемых руководством государства мер по цифровизации всех сфер жизнедеятельности граждан остро встает вопрос правовой регламентации инструментария правоохранительных органов, поскольку очевидно, что традиционные способы и методы раскрытия преступления демонстрируют свою низкую эффективность.

В связи с этим появляется необходимость урегулирования проблемных вопросов, которые создают пробелы в праве и не позволяют правоохранительным органам привлекать к ответственности злоумышленников.

В соответствии с этим требует должного внимания законодательное и научно-практическое обоснование электронной информации как объекта, содержащего следы преступления и имеющего доказательственное значение.

УПК РФ не содержит термина «электронная информация», что существенно усложняет работу в сфере киберпреступности, электронного мошенничества, коррупции, легализации преступных доходов и т.д.

Приведем некоторые примеры.

С 2010 года в нашей стране активно ведется противоправная деятельность с использованием телефонных звонков, нацеленная на получение денежных средств граждан обманным путем. Зачастую при расследовании подобных уголовных дел следователь обнаруживает, что мошенники с помощью различных компьютерных программ маскируют своё местоположение, что не позволяет осуществлять их физический розыск, а также устанавливать иные эпизоды преступной деятельности.

До настоящего момента правоохранительные органы не обладают необходимыми средствами для раскрытия подобных преступлений в случае, если противник оснащен современным техническим оборудованием и программным обеспечением.

Указанное подтверждается данными статистики. Так, например, за 2021 год из 517722 преступлений в рассматриваемой сфере раскрыто всего 118920, что составляет 23,4 %[1]. То есть только по каждому 4 делу получается установить злоумышленника и привлечь его к ответственности. Это говорит о недостаточности мер, принимаемых для борьбы с данными преступлениями.

Поэтому, как показывает практика, наиболее эффективной формой защиты от таких преступлений является профилактика и проведение разъяснительной работы с населением.

Другим примером использования электронной информации при совершении преступления является легализация преступных доходов.

---

[1] Состояние преступности в России за январь - декабрь 2021 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/28021552 (дата обращения 22.04.2022).

Так, руководство компании заключило контракт с иностранной фирмой, зарегистрированной в одной из мировых оффшорных зон. Внешнеэкономический контракт предусматривал приобретение у иностранной компании строительной техники на общую сумму почти двух с половиной миллиардов рублей. В соответствии с указанным контрактом руководство компании в качестве предоплаты должно было перечислить на расчетный счет импортера, открытый в иностранном банке, расположенном в оффшорной зоне, 100 % предоплату за якобы приобретаемую у последнего строительную технику. Российская фирма перечислила со своего расчетного счета через транзитный счет в качестве предоплаты иностранной фирме около четверти миллиарда рублей. Однако в процессе проверки финансовых операций фирмы установлено, что её уставный капитал составляет 10 тыс. рублей, какой-либо фактической хозяйственной деятельности она не осуществляет, собственных свободных денежных средств, обеспечивающих условия указанного валютного контракта не имело и не имеет. Кроме того, в адресе регистрации и по другим указываемым руководством адресам фирма отсутствует[1].

Все эти факты являются признаками фирмы - «однодневки», т.е. юридического лица, специально созданного для осуществления преступной деятельности.

Для того, чтобы доказать противоправную деятельность, необходимо получить сведения у банков, в том числе иностранных, о фактах совершения подозрительных операций, после чего происходит процесс исследования документации и оформления протоколами выемки документов, в которых подробно указывается весь процесс обработки документов, что существенно замедляет процесс расследования. Не стоит при этом забывать, что в производстве у следователя зачастую несколько уголовных дел, по каждому из которых необходимо проводить комплекс следственных действий. Соответственно, в таких условиях риск упущений со стороны следователя

[1]Современная кибербезопасность: учебное пособие [Текст] / Н. И. Долженко, Н. А. Жукова, И. А. Ярощук. Белгород: ИД «БелГУ» НИУ «БелГУ», 2021. 78 с.

велик.

Для того чтобы упростить и ускорить работу следователя, важно определить в уголовном законодательстве место и роль электронной информации при доказывании.

Вместе с тем, стоит отметить, что электронная информация как таковая в уголовном деле не может являться доказательством, поскольку она не материальна. Возможность физической работы с ней появляется только при использовании её носителя. Поэтому можно констатировать, что электронная информация представляет собой сведения, хранящиеся на носителе информации.

Однако вопрос понятия электронных носителей информации (далее – ЭНИ) как в научной теории, так и среди практиков остается дискуссионным. Противоположные точки зрения встречаются по поводу определения, содержания, порядка получения, оценки и использования информации на электронных носителях.

Также, несмотря на то, что понятие «электронный носитель информации» встречается в УПК РФ, оно законодательно не зафиксировано. Данный пробел способствует проблемам понятийного аппарата правоприменителей и судов.

Для решения данной задачей необходимо рассмотреть возможность применения аналогии права, таким образом, составив наиболее полное определение, которое будет корректно в условиях уголовного процесса.

Так, ГОСТ 2.051-2013 «Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой)» устанавливает, что электронный носитель информации представляет собой конструктивно предназначенный для записи, хранения, воспроизведения материальный носитель, обрабатываемый с помощью средств вычислительной техники[1].

[1] ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения // Электронный фонд правовой и нормативно-технической документации: сайт. URL: http://docs.cntd.ru/document/ (дата обращения: 12.09.2021).

Но с точки зрения уголовного процесса такое определение слишком широкое, поскольку затрагивает такие носители информации, в которых микросхемы в ячейки памяти сохраняют какую-либо информацию. Другими словами, бесконтактный термометр, в котором хранятся данные о результатах последних замеров, будет являться электронным носителем информации.

В целях сужения понятия, которое применимо в уголовном процессе, необходимо отметить ключевую роль таких признаков как основное назначение устройства и способы обработки и передачи хранящейся на нем информации.

Поэтому наиболее точное определение, применимое в области уголовного процесса, дает Ю.В. Гаврилин, который определяет электронный носитель информации как устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах[1].

Таким образом, исходя из определения, можно выделить характерные признаки электронных носителей информации.

конструктивная предназначенность для долговременного хранения информации
цифровая форма хранимой на электронном носителе информации
возможность воспроизведения электронной информации в электронно-вычислительных средствах
тождественность оригинала и копии
способность сохранять значительный объем информации при относительно малых его физических габаритах
наличие неразрывной связи между носителем и самой информацией, хранящейся на нем

Рис. 1.1. Признаки электронного носителя информации в уголовном процессе

[1] Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4. С. 48.

Внесение изменений в УПК РФ должно быть научно обоснованным, ввиду чего требуется классифицировать электронные носители информации по особенностям их функционирования и работы с ними.

Наиболее популярные в научных кругах способы классификации представлены на рис. 1.2.

Рис. 1.2. Классификация электронных носителей информации

Исходя из изложенного, можно сделать вывод, что электронная информация может содержать в себе признаки преступного деяния и иметь

ключевое значение в процессе доказывания преступления. Электронная информация, как предмет виртуального мира, проявляется в процессе использования электронных носителей информации, которые выступают в качестве оболочки для цифровых сведений. Поэтому необходимо рассмотреть возможность совершенствования ст. 5 УПК РФ, добавив следующее понятие электронного носителя информации – устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

§ 2. Особенности правового режима информации, содержащейся на электронных носителях

Электронная информация весьма многогранна и может содержать в себе сведения, которые по-разному охраняются государством. Роль права как главного регулятора общественных отношений является ведущей, поскольку именно благодаря закону государство способно влиять на внутренние процессы в целях защиты той или иной информации.

Для этих целей создается главный закон страны – Конституция, в которой декларируются основные права личности и которые подлежат реформированию или отмене только в случае прекращения действия прежнего основного нормативного акта.

Одним из основополагающих прав человека и гражданина в нашей стране является право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, закрепленное в ч. 1 ст. 23 Конституции[1]. Данное право распространяется и на электронную информацию.

[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 14марта 2020 г. № 1-ФКЗ // Собр. законодательства Рос. Федерации.– 2020. – № 11, ст.1416.

Кроме того, данное право является одним из основных в правовом государстве, гарантирует неприкосновенность и невмешательство в частную жизнь, а, значит, должно обеспечиваться со стороны государства. В указанных целях предусмотрен целый ряд законодательных актов, в которых прямо прописывается запрет на какие-либо действия, раскрывающие тайну переписки и иных способов коммуникации.

Однако в настоящее время в реализации данного права наблюдаются существенные трудности, поскольку происходит глубокая трансформация информационных потоков, создаются новые способы её обработки (например, цифровизация), в процессе чего возможны утечки и кражи данных, что нарушает закрепленные в Конституции РФ права.

Для наглядности можно провести аналогию. Например, производитель продукта стремиться уменьшить его себестоимость, а государство, руководствуясь стандартами безопасности жизнедеятельности личности, устанавливает допустимые нормы, соблюдая которые продукт безвреден для потребителя.

Полученная противоправными способами информация зачастую представляется органами дознания и предварительного следствия как сведения, добытые оперативным путем, либо легализуется при проведении других оперативно-розыскных мероприятий, не ограничивающих конституционных прав, что в последующем ложится в доказательную базу и может привести к незаконному привлечению лица к ответственности.

Также имеется практика необоснованного расширения круга лиц, которые допускаются к той или иной личной информации объекта проверки.

Кроме того, организации, которые по роду деятельности получают и обрабатывают персональные данные человека, обязаны соблюдать законодательные требования к оборудованию, к способам хранения и передачи информации, к кругу лиц, допущенных к ней, и т.д.

К сожалению, данной сфере уделяется недостаточное внимание со стороны, как государственных органов, так и компаний. Примером данного

утверждения являются многочисленные новости в средствах массовой информации о краже персональных данных, выкладывании их в открытый доступ, использовании в мошеннических целях.

В связи с этим, российское государство старается принимать исчерпывающие меры по недопущению утечки личных сведений граждан, стремится ограничить к ним доступ со стороны третьих лиц. Так, одной из главных целей развития информационного общества в России является обеспечение равновесия между скоростью обработки информации и механизмом её защиты.

Ведущими специалистами в области конституционного права в целях исследования данной конституционной гарантии разработаны понятия государственной, коммерческой, врачебной, адвокатской тайны, тайны связи, корреспонденции и коммуникации, а законодатели закрепили их в соответствующих нормативных актах.

Обобщенно можно сказать, что все сведения, к которым должен быть ограничен доступ, называются защищаемой информацией.

Защищаемую информацию можно разделить на три большие группы[1]:

информация открытая - на распространение и использование которой не имеется никаких ограничений;

информация запатентованная - охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;

информация, «закрываемая» ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны. К этому виду относят обычно информацию, не известную другим лицам, которая или не может быть запатентована или умышленно не патентуется ее собственником с целью

[1]Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право: Учебник / Под ред. Б.Н. Топорнина. Спб.: Юрид. центр «Пресс», 2019. С. 42.

избежания или уменьшения риска завладения этой информацией соперниками, конкурентами

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для ее собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи.

Во-первых, это секретная информация. К секретной информации в настоящее время принято относить сведения, содержащие государственную тайну.

Во-вторых, конфиденциальная информация. К этому виду защищаемой информации относят обычно сведения, содержащие коммерческую тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан.

Тайной также становится засекреченные предприятием, фирмой сведения, которые помогают эффективно решать задачи производства и выгодной реализаций продукции. Существуют и охраняются также тайны личной жизни граждан, обычно гарантируемые государством: тайна переписки, врачебная тайна, тайна денежного вклада в банке и другие.

Выделяются такие признаки защищаемой информации[1]:

засекречивать информацию, то есть ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;

защищаемая информация может быть отнесена к разным степеням секретности;

защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства

В соответствии с обрабатываемой электронной информацией на носителе в отношении него также применяются определенные меры, ограничивающие доступ к хранящимся сведениям. К таковым можно отнести установления

[1] Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право: Учебник / Под ред. Б. Н. Топорнина. Спб.: Юрид. центр «Пресс», 2019. С. 53.

пароля, соответствующих обязательств для персонала, требований к хранению носителей и т.п.

Таким образом, можно сделать вывод, что электронная информация может быть защищена как законодательно, так и локально. Соответствующим образом защищаются электронные носители информации. Данное обстоятельство имеет прямое значение для доказывания по уголовному делу, т.к. электронные носители информации могут быть признаны вещественным доказательством.

§ 3. Электронные носители информации в системе видов доказательств

Использование различных современных технических средств преступниками в сфере использования электронной информации требуют адекватного ответа от правоохранительных органов. Это предопределяет потребность в работоспособной системе не только выявления, предупреждения, пресечения и доказывания названных преступлений органами внутренних дел, которые, используя свои специальные формы и методы деятельности, а также негласные силы и средства, участвуют наряду с другими правоохранительными органами в обеспечении безопасности Российской Федерации.

Важно, что преступления в сфере кибербезопасности представляют повышенную общественную опасность и имеют в качестве своей основной цели или в качестве значимого проявления обогащение за счет законопослушных граждан, что подрывает авторитет правоохранительных органов и государственного механизма в целом, как огромной бюрократизированной структуры, не способной своевременно и положительно противостоять современным угрозам и вызовам[1].

Постепенное внедрение прогрессивных научных разработок происходит и в деятельности сотрудников органов внутренних дел. На сегодняшний день

[1]Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г. и др. Криминалистика. Учебник [Текст]. – М: Инфра-М, Норма, 2017. 928 с..

экспертам-криминалистам представляется возможность работы с многочисленными техническими средствами, компьютерными программами и иным оборудованием, помогающем в обнаружении следов и поиске лиц, подозреваемых в совершении преступлений, что позволяет быстрее и качественнее обрабатывать электронную информацию, упрощая процесс доказывания.

Кроме того, инновации позволяют интегрировать научные разработки в криминалистическую деятельность, постепенно совершенствуя и упрощая её. Так, тенденции развития в сфере робототехники позволяют нам предполагать, что в скором времени искусственный интеллект найдет свое применение в работе следователей-криминалистов в различных сферах, в том числе при работе с электронной информацией.

Современное законодательство не регламентирует применение искусственного интеллекта в деятельности следователя-криминалиста. Однако уже сегодня мы можем сказать, что роботизированный механизм может принести пользу при проведении некоторых следственных действий. Например, при выемке баз данных, содержащих значительный объем электронной информации, алгоритм может не только искать сведения по заданным критериям, но и обучаться в процессе взаимодействия со следователем для оптимизации поиска.

Высокие технологии находят своё применение и в оффлайн области. Так, предполагается, что следователю в ходе допроса будет помогать искусственный интеллект, задачей которого будет являться определение степени правдивости показаний, даваемых допрашиваемым. Но есть и некоторые технические трудности у данного процесса: пока ни одно научное общество не может дать стопроцентной гарантии, что искусственный интеллект сможет понять истинные эмоции, чувства и мотивы, побуждающие к действиям человека, так будто бы самому роботу присуще отражать в сознании влияние внешних факторов. Однако данный фактор не может полностью исключать возможность участия искусственного интеллекта в процессе уголовного судопроизводства.

Вместе с тем, для доказывания по уголовному делу необходимо участие следователя, который производит сбор вещественных доказательств, позволяющих привлечь злоумышленника к уголовной ответственности.

Согласно нормам уголовно-процессуального закона доказательствами являются любые сведения, на основе которых устанавливаются наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для него[1].

Применительно к действующему законодательству и способам сбора доказательств, можно отметить, что электронные носители информации все чаще избираются в качестве средств доказывания.

Например, при допросе следователь помимо заполнения бумажного протокола вправе проводить аудио- и видеосъемку следственного действия. Результаты использования технических средств представляются в качестве электронной информации, записанной на носитель, и приобщаются к материалам дела.

Но появляется закономерный вопрос – зачем заполнять протокол допроса, если сведения, хранящиеся на электронном носителе, отражают не только процесс допроса, но и позволяют передать эмоциональную окраску происходящего, чего лишен бумажный аналог.

Однако согласно существующих процессуальных норм, электронный носитель информации может быть приобщен к материалам уголовного дела и иметь доказательственное значение только вместе с сопроводительным документом (протоколом, постановлением и т.д). Таким образом, получается, что ЭНИ является только дополнительным средством фиксации хода следственного действия. Поэтому в целях упрощения и ускорения работы следователя по раскрытию уголовного дела целесообразно рассмотреть законодательную возможность изменения статуса электронных носителей

---

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

информации при доказывании.

Рассмотренные особенности проведения допроса полностью характерны и для обыска. В настоящее время на практике практически любой обыск проводится с применением видеозаписи в целях исключения возможных нарушений как прав обыскиваемого, порядка проведения процедуры, так и фиксации обнаруженных предметов, которые могут иметь доказательственное значение[1].

К подобным следствиям действиям, при которых практики зачастую используют технические средства для фиксации их хода, можно отнести также осмотр места происшествия, выемку, проверке показаний на месте, следственный эксперимент.

Вместе с тем, полностью отказаться от составления протокола следственного действия пока не представляется возможным, поскольку не установлен механизм подтверждения подлинности записанных на электронный носитель информации сведений.

Если в протоколе подозреваемый, обвиняемый собственноручно расписывается, подтверждая факт совершения следственного действия и соглашаясь со всем, что написано, то при проведении аудио- или видеозаписи следственного эксперимента не разработан соответствующий механизм.

Представляется целесообразным словесное подтверждение всего, что происходило при следственном действии, а также последующее документальное оформление согласия, например, под надписью на конверте, в который упаковывается электронный носитель информации. Но пока данное предложение остается только в теоретических трудах, рассмотрим, как в современном уголовном процессе организована работа с электронными носителями, имеющими доказательственное значение.

В соответствии с требованиями п. 8 ст. 166 УПК РФ электронный

---

[1]Громов Н .А. Доказательства: их виды и доказывание в уголовном процессе: учеб.-практ. пособие / Н. А. Громов, С. А. Зайцева, А. Н. Гущин. [Текст]. – М.: Приор-издат, 2018. 81 с.

носитель, содержащий файлы аудио-, видеозаписи следственного действия, является приложением к протоколу.

Согласно ч. 4 ст. 190 УПК РФ, в протоколе делается соответствующая отметка с указанием сведений о технических средствах, об условиях аудио- и (или) видеозаписи, факте приостановления аудио- и (или) видеозаписи, о причине и длительности остановки их записи и заявлений по поводу проведения аудио- и (или) видеозаписи.

По окончании следственного действия файл с записью в присутствии участников целесообразно копируется на неперезаписываемый электронный носитель, например, CD-R-диск, с отражением в протоколе используемого программного обеспечения, серийного номера носителя, имени, размера, даты и времени создания файла, а также его контрольной суммы[1].

Учитывая, что использование технологии видео-конференц-связи для производства допроса предусмотрено лишь в ходе судебного разбирательства (ч. 4 ст. 240, ст. 278.1 УПК РФ), представляют интерес предложения Е.К. Антоновича, направленные на дополнение УПК РФ нормой, предусматривающей особенности допроса свидетеля по уголовному делу посредством видео-конференц-связи[2].

Целесообразность уголовно-процессуальной регламентации порядка производства следственных действий, участники которых территориально находятся в разных местах, отмечал и Ю.В. Гаврилин[3]. При этом им

---

[1] Гаврилин Ю. В. Организационно-методическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации // Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий. – М: Академия управления МВД России, 2019. Ч. 1. С. 128.

[2] Антонович Е.К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6 (103). С. 128.

[3] Гаврилин Ю.В. Трансформация уголовно-процессуальной формы в условиях цифровой экономики // Уголовный процесс и криминалистика: теория, практика, дидактика: сб. статей IV Всероссийской науч.-практ. конф. / под ред. А.В. Красильникова. – М: Академия управления МВД России, 2019. С. 118.

выделялись следующие технические условия, обеспечивающие возможность производства дистанционного допроса:

устойчивость канала связи в режиме телеконференции;

возможность преобразование устной речи в письменный текст;

возможность ознакомления участников следственного действия с протоколом в режиме online;

удостоверение протокола с использованием технологий биометрической идентификации и электронной подписи.

Если на видеозаписи зафиксированы события, действия или факты, не отраженные в протоколе следственного действия, но имеющие самостоятельное доказательственное значение, то такая информация подлежит процессуальному оформлению в соответствии с правилами работы с вещественными доказательствами.

Внесение изменений в законодательство, связанное с определением места и роли электронной информации в доказывании по уголовному делу имеет высокий приоритет по следующим причинам.

1. Современные крупные экономические компании представляют собой цифровые платформы, расследовать экономические преступления которых или в отношении которых без проведения специальных технических мероприятий практически невозможно. Так, например, после внесения медиа-платформы «Meta» в список экстремистских организаций, возникла необходимость выявления, предупреждения и пресечения преступлений экстремисткой направленности связанных с указанным юридическим лицом. Однако правоохранительные органы не обладают технической возможностью мониторинга циркулирующего на серверах компании трафика. Кроме того, даже в случае получения такой технической возможности необходимо было бы затратить огромное количество усилие на документирование выявленных признаков преступлений и сбора доказательной базы. Представляется, что выполнить такой объем работы без привлечения искусственного интеллекта и разных технических специалистов невозможно.

2. Усиление значимости данных в экономической деятельности. Основная часть экономики сконцентрирована в таком факторе производства как услуги, связанные с интеллектуальной собственностью, базами данных. В области управления данными возникла тенденция применения «облачных» технологий. Использование таких изобретений позволяет предприятиям снизить затраты на создание и обеспечение собственной цифровой инфраструктуры. То есть за счет «облачных» технологий можно хранить данные, используя различные устройства в режиме «онлайн», не занимая места на картах памяти и других физических носителях. Однако, основной проблемой использования «облачных» технологий является безопасность данных. В настоящее время хакерам из различных стран получить доступ к информации в «облаке» не является невыполнимой задачей, а расследование таких преступлений без соответствующих знаний и навыков в программировании не представляется возможным. Следователю приходится тратить значительное количество сил и привлекать многих специалистов для расследования таких преступлений;

3. Глобальная сеть Интернет теперь служит самым распространённым средством для нахождения необходимой информации и сведений. Способы взаимодействия людей претерпели сильные изменения с появлением в их жизни разнообразных способов общения в режиме «онлайн» реального времени. Социальные сети, мобильные приложения сегодня служат основным источником коммуникации в обществе. Получить доказательственную информацию традиционными методами становится все сложнее;

4. Высокая скорость и большой объем информации. Выполнение заказов, отправка информации, то есть осуществление любых действий влечет за собой мгновенную реакцию, что является одним из востребованных способов привлечения капитала в условиях постоянно меняющихся потребностей людей. В настоящее время работа с большим объемом данных в уголовно-процессуальном смысле реализуется привлечением большего количества человеческих ресурсов, а не с помощью специального технического оборудования и программ;

5. Глобальный характер обмена данными. Отслеживание ситуации на мировом рынке позволяет приспособиться и адаптироваться законодателю и правоохранительным органам к изменяющимся условиям.

Этот не исчерпывающий перечень причин законодательных изменений позволяет говорить о том, что на электронных носителях информации могут содержаться весомые сведения, доказывающие преступную деятельность, а порядок их получения и значение для расследования законом прямо не определены.

Таким образом, можно сделать вывод, что в настоящее время доказательства, зафиксированные на электронных носителях, имеют статус дополнительных средств фиксации хода следственного действия, что позволяет подтвердить изложенную в протоколе информацию. Данное обстоятельство, по сути, является двойной работой, поскольку сведения, записанные с помощью технических средств и упакованные установленным законодательством образом, сами по себе обладают доказательственным значением, описывают эмоциональную окраску происходящего, поэтому представляют собой более ценное доказательство, нежели протокол. Учитывая данный факт, необходимо внести изменения в законодательство, где отразить возможность применения электронного носителя информации в качестве самостоятельного вида доказательства без привязки к протоколу следственного действия, а также проработать механизм подтверждения легитимности и достоверности записанных на носитель сведений.

ГЛАВА 2. ОСОБЕННОСТИ СОБИРАНИЯ, ПРОВЕРКИ И ОЦЕНКИ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

§ 1. Сбор электронной информации на локальных электронных носителях

Законодатель для регулирования вопроса сбора доказательной базы по уголовным делам определил, что процесс доказывания включает в себя собирание, проверку и оценку доказательств в целях установления обстоятельств, входящих в предмет доказывания[1].

Исходя из законодательной дефиниции процесса доказывания, его содержанием являются собирание, проверка и оценка доказательств. Рассмотрим содержание указанной деятельности применительно к доказательствам на электронных носителях информации.

В науке уголовного процесса традиционно считается, что сбор доказательств представляет собой систему действий, направленных на восприятие объективно существующих следов происшедшего события и их процессуальную фиксацию[2].

В современных условиях развития информационного общества роль и значение доказательственной информации, содержащейся на электронных носителях, в уголовном судопроизводстве неуклонно возрастает, в связи с чем возникает необходимость детального правового регулирования порядка ее собирания.

Опосредованным подтверждением обозначенного выше тезиса могут служить статистические данные, согласно которым в период с 2017 по 2020 год отмечается тенденция роста проведенных компьютерных экспертиз электронных носителей информации и увеличения числа установленных с их помощью лиц (рис. 2.1).

---

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

[2] Чурилов С. Н. Криминалистическая методика расследования [Текст]. – М.: Юстицинформ, 2017. 204 с. 38.

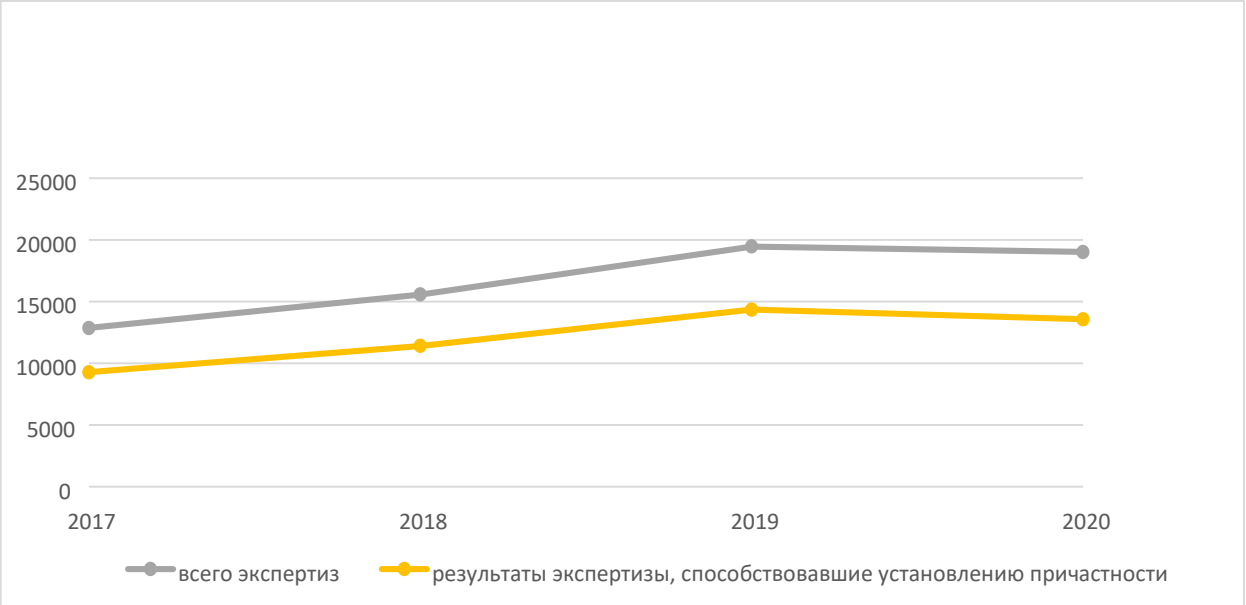

Рис. 2. 1. Компьютерные экспертизы, проведенные в экспертно-криминалистических подразделениях органов внутренних дел с 2017 по 2020 гг.

Понятию сбора доказательств посвящена ст. 86 УПК РФ. При этом законодатель не приводит определение процесса собирания доказательств, отмечая лишь, что он «осуществляется дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий»[1].

Кроме того, в приведенной норме содержится также указание на процессуальные формы собирания доказательств для подозреваемого, обвиняемого, а также потерпевшего, гражданского истца, гражданского ответчика, их представителей, а также защитника.

Обнаружение доказательств означает их отыскание, выявление, установление тех или иных фактических данных, имеющих доказательственное

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

значение, – это начальная и необходимая стадия собирания доказательств[1].

Современные достижения науки и техники могут выполнять существенную вспомогательную функцию.

Так, разрабатываются системы, в которых искусственный интеллект сможет анализировать уголовные дела и безошибочно делать выводы о необходимости проведения того или иного следственного действия, строить следственные версии и судить о виновности лиц, что поможет научить машину анализировать человека, ведя с ним диалог[2].

В таком случае перед учёными будет стоять задача написания алгоритма, который позволит роботизированному механизму составлять вопросы для допрашиваемого на основе имеющихся материалов уголовного дела, менять их в зависимости от ответов и, одновременно с этим, по работе лицевых мышц, жестикуляции и иным признакам определять степень правдивости показаний.

Ввод в действие таких разработок повлечет за собой возникновения нового ряда вопросов.

В первую очередь предоставление искусственному интеллекту возможности проводить следственное действие должно либо наделить робота процессуальным статусом, либо определить его как техническое средство, выполняющее вспомогательную функцию для должностного лица. В случае определения процессуального статуса искусственного интеллекта, возникает необходимость определения того, кто будет нести ответственность в случае допущения роботизированным механизмом ошибок.

Представляется, что необходимо оставлять право последнего слова за следователем, ведь искусственный интеллект на данной стадии развития не обладает достаточными психическими, нравственными и мыслительными способностями, чтобы суметь оценить последствия неверных действий и понять свою вину.

---

[1]Тюнис И. О. Криминалистика. Учебное пособие [Текст]. – М: Проспект, 2020. 220 с.7

[2]Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук / А. И. Зазулин. [Текст]. Екатеринбург, 2018. 250 с.

Однако и создатели таких систем при вводе их в эксплуатацию не могут спрогнозировать и предотвратить всех последствий использования роботизированных механизмов. Возможно, законодатель определит участниками уголовного процесса не только физических лиц, но и роботов, наделенных системами искусственного интеллекта, ведь установленный порядок сбора доказательств, в том числе и на электронных носителях информации, должен быть ускорен.

Но для этого, в первую очередь, будет необходимо расширить количество нормативно-правовых актов или отдельных норм права, связанных с регулированием сферы робототехники.

До тех пор, пока искусственный интеллект по своему процессуальному статусу не будет приравнен к сотрудникам правоохранительных органов, такая система будет считаться техническим средством, способным составить конкуренцию полиграфам, но не экспертам-криминалистам, следователям и иным лицам, уполномоченным производить следственные действия.

Не смотря на то, что дать однозначный ответ на вопрос о возможности применения искусственного интеллекта на данный момент нельзя, мы можем говорить о неизбежности их внедрения в деятельность правоохранителей.

Законодателем сформулированы универсальные требования к порядку собирания доказательств на электронных носителях в специально введенной ст. 164.1 УПК РФ.

Так, «копирование информации определено в качестве приоритетного способа собирания доказательств на электронных носителях по уголовным делам о преступлениях экономической направленности, совершенных в сфере предпринимательской деятельности»[1].

Определен исчерпывающий перечень исключений, позволяющих осуществлять изъятие электронных носителей информации. Каждое изъятие

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

электронных носителей информации должно осуществляться с участием специалиста.

На практике без крайней необходимости стараются придерживаться требования по копированию электронной информации без изъятия её носителей.

Но в некоторых ситуациях, когда, например, объем данных слишком велик или на самом носителе информации могут содержаться запрещенные к распространению сведения не могут быть оставлены пользователю, приходится производить изъятие.

«Изъятие электронных носителей допустимо, если вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации»[1]. Представляется, что указанное основание является трудно реализуемым на практике.

В постановлении о назначении экспертизы указываются материалы, предоставленные в распоряжение эксперта.

Соответственно, на момент вынесения данного постановления в распоряжении следователя уже должны быть указанные электронные носители информации. Очевидно, что обеспечить наличие еще не изъятых материалов не представляется возможным.

«Изъятие электронных носителей допускается на основании судебного решения». Полномочия суда закреплены в ст. 29 УПК РФ, где предусмотрен перечень решений, принимаемых судом в ходе досудебного производства. При этом решения суда об изъятии электронных носителей информации в данном перечне не содержится.

Применительно к п. 2 ч. 1 ст. 164.1 УПК РФ основаниями для изъятия электронных носителей информации выступают решения суда о производстве обыска и (или) выемки в жилище, в ходе которых происходит

---

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

изъятие электронных носителей информации, а также о производстве выемки предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, а также предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, которые могут содержаться на электронных носителях информации, в связи с чем подлежат изъятию[1].

Помимо этого, особенностью изъятия носителя информации является право владельца на получение копии электронной информации. В таком случае он должен сам представить носитель, на который специалист производит копирование.

В настоящее время существует программное обеспечение, в том числе, отечественное, способное зафиксировать факт совершения противоправного деяния, данные из которого могут стать доказательством в суде. Например, DLP-системы (анг. «Data Leak Prevention»), что означает предотвращение утечек данных.

Эти системы активно используются крупными компаниями для обеспечения экономической безопасности и защиты коммерческой тайны. Принцип работы основан на контроле каналов коммуникации сотрудников организации, по которым защищаемая информация может быть передана.

К таковым относятся:

электронная почта;

исходящая почта;

входящая почта;

корпоративная локальная сеть;

веб-ресурсы;

мессенджеры;

USB-носители и др.

---

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

На рис. 2.2. представлены каналы коммуникации, контролируемые программным продуктом «SolarDozor» от компании Ростелеком-Солар.

Рис. 2.2. Каналы коммуникации, которые контролирует DLP-система «SolarDozor»

Исходя из анализа представленных графических данных, можно предположить, что система может отслеживать не только передаваемые по каналам коммуникации сообщения, но и его действия. Эти сведения могут использовать сотрудники отдела собственной безопасности для пресечения возможного экономического ущерба интересам хозяйствующего субъекта и передать их в правоохранительные органы для привлечения злоумышленников к ответственности. Отчеты из указанного программного продукта принимаются судами в качестве доказательств по уголовным делам.

Так, например, Дзержинский районный суд г. Новосибирска 26 февраля 2019 года вынес обвинительный приговор 2 бывшим сотрудникам регионального оператора мобильной связи «МТТ», которые совершили преступление, предусмотренное ч.3 ст.183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

В частности, за 26 тысяч рублей злоумышленники, используя рабочий компьютер другого сотрудника осуществили попытку отправки через

электронную почту файлы, содержащие персональные данные нескольких тысяч клиентов. Эти сведения «Положением о коммерческой тайне» ОАО «МТТ» запрещено передавать третьим лицам без соответствующего разрешения. В ходе судебного разбирательства вина подсудимых была доказана. В качестве доказательства к уголовному делу прилагались материалы внутренней проверки службы безопасности хозяйствующего субъекта, где в виде представлены выгруженные из системы «SolarDozor» отчеты, иллюстрирующие содержание переписки между подсудимыми, между ними и покупателем базы данных, иные сведения, касающиеся способа передачи информации, почтовых адресов, банковских счетов и т.д.[1]

Исходя из изложенного, можно сделать вывод, что в настоящее время сбор электронной информации на локальных электронных носителях зачастую происходит посредствам копирования информации. В некоторых случаях приходится проводит изъятие электронных носителей информации, что требует получения судебного разрешения и привлечения специалиста. Однако с развитием технологий и появлением специального программного обеспечения необходимо принимать во внимание наличие иных источников получения информации, которые необходимо использовать при расследовании уголовных дел.

§ 2. Сбор электронной информации на сетевых носителях

Совершение компьютерный преступлений и преступлений в сфере кибербезопасности сопряжено с передачей сведений, содержащих следы преступления, через компьютерные сети. Поэтому для повышения эффективности расследования необходимо получать информацию, которая хранится на серверах, у операторов связи, а также в облачных пространствах.

[1] Приговор № 1-62/2019 от 26 февраля 2019 г. по делу № 1-62/2019 [Электронный ресурс]. https://sudact.ru/regular/doc/LKScMPwjregular-judge=&_=1652511666837 (дата обращения 03.05.2022).

Зачастую при проведении исследования машинных носителей информации, изъятых у подозреваемого, не удается обнаружить сведения, прямо доказывающие его причастность к совершению преступления.

Любой хорошо подготовленный злоумышленник использует специальное программное обеспечение, которое не позволяет фиксировать операционной системе действия пользователя.

В таких случаях даже проведение экспертизы содержимого машинного носителя информации не позволит получить доказательства преступной деятельности.

Поэтому важно проводить оперативно-розыскные мероприятия и следственные действия в компьютерных сетях, участником которых являлась электронно-вычислительная машина подозреваемого. Не имея доступа к серверу, злоумышленник не сможет настроить систему так, чтобы она не фиксировала данных, передаваемых по используемым каналам коммуникации. Из этого исходит, что сведения, хранящиеся на сетевых носителях, могут являться единственными достоверными доказательствами противоправной деятельности.

Рассматривая особенности собирания доказательственной информации в сети Интернет, следует подчеркнуть следующую технологическую особенность: компьютерная информация передаётся по телекоммуникационным каналам связи с высокой скоростью и практически без ограничений по объему[1].

Кроме того, сеть Интернет не имеет какого-то единого центра обработки и хранения данных. Информация физически хранится на серверах, каждый из которых имеет свой уникальный сетевой адрес.

Действующее законодательство определения «компьютерная сеть» не содержит. Имеющееся законодательное определение сети, по которой

[1] Андриенко Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам / Ю. А. Андриенко // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). С. 45.

передается информация, содержится только федеральном законе от 07 июля 2003 г. № 126-ФЗ «О связи». Он определяет сеть связи как «технологическую систему, включающую в себя средства и линии связи и предназначенную для электросвязи или почтовой связи»[1].

Для понимания многообразия компьютерных сетей, используемых для в настоящее время провайдерами и операторами связи, они представлены на рис. 2.3 в графическом виде[2].

Рис. 2.3. Виды компьютерных сетей

[1] О связи: федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 28 июня 2003 г. // Рос.газ. – 2003. – 13 июля.

[2] Вехов В. Б. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С. В. Зуева. – М: Юрлитинформ, 2019. С. 111.

Важным является тот факт, что информация в процессе обращения в компьютерных сетях оставляет цифровые следы на соответствующих электронных носителях и иных цифровых устройствах, связанных с событием преступления, позволяет установить обстоятельства совершенного преступления и преступника[1]. Ю.В. Гаврилин в этой связи отмечает, что цифровые следы как специфическая форма преобразования компьютерной информации обладают следующими признаками:

отражают событие преступления в информационном поле;

являются материальными по своей природе, но не отражают пространственную форму следообразующего объекта;

являются результатом преобразования компьютерной информации;

служат носителями свойств, присущих компьютерной информации;

обладают способностью к дублированию, т.е. к копированию на другие электронные носители без изменения их характеристик[2].

Собирание доказательственной информации в компьютерных сетях, несмотря на ряд особенностей, осуществляется предусмотренными в УПК РФ процессуальными средствами, основными из которых являются следственные действия, в частности, осмотр места происшествия, обыск, выемка, осмотр предметов. Каких-либо специальных процессуальных средств собирания доказательственной информации в компьютерных сетях действующее уголовно-процессуальное законодательство в настоящее время не содержит[3].

В свою очередь, В.Ф. Васюков и А.Н. Колычева считают, что когда интересующая следствие информация располагается на интернет-сервисе электронной почты, то ее процессуальная фиксация возможна посредством осмотра:

---

[1] Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник университета им. О. Е. Кутафина. 2019. № 3 (55). С. 49.

[2] Гаврилин Ю. В., Шипилов В. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 2.

[3] Криминалистическая тактика / отв. ред. В. Н. Карагодин, Е. В. Шишкина [Текст]. Екатеринбург, 2018. 119 с. 61.

электронной почты на компьютерном оборудовании участника;

производства по уголовному делу и с его согласия;

материального носителя содержащейся на нем перепиской;

полученного от почтового сервиса;

содержания электронной переписки на бумажном носителе (в данном случае применяются правила осмотра для документов)[1].

Обобщая приведенные выше подходы различных авторов к вопросу необходимости совершенствования процессуального порядка собирания доказательственной информации на электронных носителях, представляется необходимым сделать следующие выводы:

Большинство авторов, исследовавших вопрос о процессуальном порядке собирания доказательственной информации в компьютерных сетях, поддерживают тезис о необходимости его совершенствования.

Направлениями такого совершенствования видится введение в уголовно-процессуальное законодательство особых правовых процедур в рамках следственного осмотра и обыска.

§ 3. Проверка и оценка электронной информации на электронных носителях

Под проверкой доказательств в уголовном процессе понимается деятельность следователя и суда, связанная с анализом и синтезом доказательств, сопоставлением их с другими доказательствами и собиранием новых доказательств[2].

Целью проверки доказательств является уяснение качеств и свойств самих проверяемых доказательств – их достоверности или недостоверности, правильности или неправильности, доброкачественности.

---

[1] Васюков В. Ф., Колычева А. Л. Осмотр и фиксация страниц интернет-сайта в сети Интернет // Вестник экономической безопасности. 2019. № 1. С. 116.

[2] Крюкова Н. И., Косолапова Н. В. Криминалистика. Учебное пособие [Текст]. – М: Юстиция, 2019. 256 с.

Проверка доказательств осуществляется путём их сопоставления, установления источника доказательства, а также посредством производства следственных и иных процессуальных действий, в ходе которых получаются новые доказательства, которые, в свою очередь, сопоставляются с проверяемым доказательством.

В ходе проверки исследуются все обозначенные свойства доказательств и источник их происхождения, устанавливается достоверность содержащихся в доказательствах сведений.

Ни одно доказательство, каким бы убедительным и безупречным оно ни казалось, не может быть положено в основу выводов по уголовному делу без их проверки.

Проверке подвергается как содержание доказательства, так и доброкачественность источника его получения в их неразрывном единстве. При этом нарушение указанных правил повлечет за собой тот факт, что доказательство, полученное с нарушением основных положений судопроизводства, хотя и не носящим преступного характера, – недопустимо.

Вместе с тем, с учетом положений теории доказательственного права УПК РФ воспроизводит достаточно совершенную систему характеристик, предъявляемых к доказательственной информации.

Уголовно-процессуальный закон содержит положение, что «каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в их совокупности – достаточности для разрешения уголовного дела»[1].

Относимость доказательства в одних источниках трактуется, как пригодность устанавливать факты, являющиеся предметом доказывания, определять логическую связь между сведениями, которые составляют содержание доказательства, и тем, что нужно установить для правильного

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

разрешения уголовного дела.

«Относящимся к делу признается лишь то доказательство, которое прямо или косвенно подтверждает какие-либо из обстоятельств, подлежащих доказыванию»[1].

В вопросе допустимости доказательств существуют на сегодняшний день спорные моменты, что связано с сущностью допустимости, которую понимают по-разному. Для формирования доказательств первичным материалом служат сведения, которые сами по себе не будут являться доказательствами. Форма сохранения этих сведений зависит от источников.

Справедливо отметить факт того, что нельзя лишать свойства допустимости доказательства, исключение которого может повлечь за собой потерю иных доказательств, вплоть до прекращения уголовного дела.

Таким образом, можно выделить следующие условия допустимости доказательств:

способ собирания, закрепления и проверки сведений о фактах должен быть предусмотрен законом;

порядок собирания, закрепления и проверки сведений о фактах должен соответствовать закону.

И если, лицо, дающее оценку, усомнится в достоверности и относимости собранной и зафиксированной информации, то это приведет к признанию доказательства недопустимым.

Достоверность имеет одну особенность, заключающуюся в том, что требование достоверности не может быть предъявлено заранее к каждому доказательству.

Так, если неотносимость или недопустимость доказательства, как правило, очевидны сразу и такое доказательство исключается из дальнейшего процесса доказывания, то его недостоверность может быть признана только на

---

[1] Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

основе определенной совокупности собранных доказательств.

Что касается такого требования, как достаточность доказательств, то оно в стадии возбуждения уголовного дела представляет собой исключительно оценочную категорию, которая требует от субъектов процесса надлежащего уровня правового сознания и высокой культуры правоприменения[1]. При этом, как правило, предположительный, вероятностный характер носит вывод, основанный на достаточных данных только о совершении преступления на момент возбуждения уголовного дела[2].

Применительно к особенностям доказательственной информации, содержащейся на электронных носителях, имеются выявленные в ходе проведенного исследования сложности, которые возникают при ее проверке.

Так, на электронных носителях зачастую содержится огромное количество файлов, а необходимая для использования в процессе доказывания информация может быть скрыта или уничтожена, вследствие чего для обнаружения или восстановления такой информации требуется специальное программное обеспечение.

По мнению Пастухова П.С., допустимость информации устанавливается с учетом соответствия реквизитов компьютерной информации, таких как тип файла, его объем, время создания, время редактирования, время открытия, сведения о пользователе; установления, каким образом было обеспечено условие ее целостности, а также с учетом соответствия типа (вида) программного средства, которое использовалось для:

формирования (создания) данной информации;

ее копирования, если данная информация была перенесена на другой носитель;

воспроизведения данной информации (характеристики программных средств, например, типа операционной системы, регистрационного номера

---

[1] Левченко О. В. Внутреннее убеждение как метод оценки доказательств в уголовном судопроизводстве // Вестник Волжского университета им. В. Н. Татищева. 2013. № 2. С. 88.

[2] Комментарий к Уголовно-процессуальному кодексу Российской Федерации / под общ.ред. В. В. Мозякова. М., 2021. С. 313.

лицензии и пр.)[1].

Достоверность полученной в ходе следственного действия доказательственной информации на электронном носителе подтверждается присутствием специалиста при осуществлении копирования.

Следующей особенностью проверки электронных доказательств является необходимость обращения к помощи специалиста в ходе работы с такими доказательствами.

Проверка источника доказательственной информации на электронных носителях предполагает, что должны сохраняться подлинники электронных носителей, которые помогут установить отсутствие внесений модификаций с помощью технических средств.

Требует внимания факт установления подлинности источника доказательства на электронном носителе и отсутствия модификации, находящейся на нем информации.

С указанной целью, требуется установление источника происхождения информации на электронном носителе, идентификация ее автора и аутентификация ее владельца (пользователя), что будет являться необходимыми условиями проверки такого свойства доказательства, как его достоверность.

При написании протокола следственного действия необходимо указывать ряд признаков, которые определяют аутентичность информации, скопированной специалистом (количество скопированных файлов, их размер как в отдельности, так и в совокупности, наименование файлов и т. д.).

Изъятие следователем доказательственной информации с электронных носителей в строгом соответствии с процессуальными нормами и разработанными методиками является важнейшей гарантией допустимости доказательств, получаемых в ходе осмотров электронных носителей информации, сопровождаемых выемкой, а также в ходе обысков и выемок

[1] Пастухов П. С. Средства проверки надежности «электронных» доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2019. № 3. С. 170.

электронных носителей информации.

С точки зрения относимости оценивается как содержание компьютерной информации, так и её свойства: дата создания, изменения, открытия. При этом установление связи электронного доказательства с обстоятельствами, имеющими значение для уголовного дела, часто требует участия специалиста или же проведения экспертизы.

Кроме того, доказательственная информация, полученная с электронных носителей, будет обладать признаком относимости, если будет обоснована логическая связь полученных сведений с теми, что необходимо установить по конкретному уголовному делу с целью правильного его разрешения.

Проведение судебной экспертизы электронных носителей информации, в результате которой в уголовном деле появится доказательственная информация, полученная с данных носителей, так же требует внимания при возникновении вопроса достоверности полученной информации.

Прежде всего само постановление о назначении судебной экспертизы должно соответствовать требованиям, изложенным в законе. А это значит, что помимо правильной постановки вопросов эксперту, предоставления ему в упакованном и опечатанном виде электронного носителя информации, с ее назначением должны быть ознакомлены участники уголовного дела, обладающие данным правом.

При оценке экспертного заключения необходимо удостовериться, что эксперт не вышел за пределы своей компетенции и им были соблюдены все правила проведения экспертизы. В связи с тем, что первичная информация, находящаяся на электронном носителе, может быть легко изменена или уничтожена, в том числе и экспертом, последним необходимо руководствоваться принципами работы с информацией на электронных носителях, которые были разработаны Международной организацией по компьютерным доказательствам.

Компьютерно-техническая экспертиза является специальным средством проверки электронных доказательств. При этом сомнения в достоверности

доказательственной информации, полученной с электронных носителей, могут быть вызваны тем, что, в такую информацию легко внести изменения, которые без помощи эксперта будет сложно обнаружить.

При определении достаточности как свойства доказательств применительно к цифровой информации собирать всю имеющуюся на исследуемом электронном носителе информацию необходимости нет. При этом надо отметить, что проверка и оценка электронных доказательств, с одной стороны, естественно подчиняются общим закономерностям, присущим проверке и оценке доказательств по уголовным делам. Но кроме того, вследствие специфики объектов цифровой информации проверка и оценка электронных доказательств требуют применения специальных знаний о природе такого рода информации, а также использования в необходимых случаях соответствующего программного-аппаратного обеспечения.

При оценке доказательственной информации на электронных носителях должно учитываться следующее:

надежность способа, с помощью которого подготавливалась, хранилась или передавалась электронная информация;

надежность способа, при помощи которого обеспечивалась целостность информации;

надежность способа, при помощи которого идентифицировался его составитель;

правильность способа фиксации информации, в связи с тем, что закрепление информации на современном источнике может отражаться на достоверности данного доказательства[1].

В любом случае следователь должен обладать соответствующими знаниями в области информатики хотя бы начального уровня, поскольку неосторожный доступ такого рода информации может привести к потери доказательственного значения интересующей информации.

---

[1] Нахова Е. А. Проблемы электронных доказательств в цивилистическом процессе // Ленинградский юридический журнал. 2019. № 4. С. 302.

Закрепление или фиксация собранной доказательственной информации на электронных носителях подразумевает перенос данной информации на иной, процессуальный источник информации. При этом необходимо удостовериться в том, что искомая информация находится на первичном источнике.

Подводя итог вышесказанному, можно указать на необходимость внедрения системы специфических критериев оценки допустимости доказательственной информации на электронных носителях, к числу которых относятся:

аутентичность информации как возможность достоверного установления источника ее происхождения;

целостность информации как отсутствие изменений в ее составе, содержании и свойствах;

достоверность информации – точное отражение определенных явлений, процессов, деятельности или фактов;

доступность для восприятия с использованием надлежащего программного обеспечения и технических средств обработки, не влекущих внесение в нее изменений.

ЗАКЛЮЧЕНИЕ

Проведенное исследование показало, что в настоящее время актуальны вопросы внесения электронной информации и их носителей в уголовно-процессуальный закон в качестве отдельного вида доказательств.

Электронная информация может содержать в себе признаки преступного деяния и иметь ключевое значение в процессе доказывания преступления.

Электронная информация, как предмет виртуального мира, проявляется в процессе использования электронных носителей информации, которые выступают в качестве оболочки для цифровых сведений. Поэтому необходимо рассмотреть возможность совершенствования ст. 5 УПК РФ, добавив следующее понятие электронного носителя информации – устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная информация может быть защищена как законодательно, так и локально. Соответствующим образом защищаются электронные носители информации. Данное обстоятельство имеет прямое значение для доказывания по уголовному делу, т.к. электронные носители информации могут быть признаны вещественным доказательством.

Таким образом, можно сделать вывод, что электронная информация может быть защищена как законодательно, так и локально. Соответствующим образом защищаются электронные носители информации. Данное обстоятельство имеет прямое значение для доказывания по уголовному делу, т.к. электронные носители информации могут быть признаны вещественным доказательством.

В настоящее время доказательства, зафиксированные на электронных носителях, имеют статус дополнительных средств фиксации хода следственного действия, что позволяет подтвердить изложенную в протоколе

информацию.

Данное обстоятельство, по сути, является двойной работой, поскольку сведения, записанные с помощью технических средств и упакованные установленным законодательством образом, сами по себе обладают доказательственным значением, описывают эмоциональную окраску происходящего, поэтому представляют собой более ценное доказательство, нежели протокол.

Учитывая данный факт, необходимо внести изменения в законодательство, где отразить возможность применения электронного носителя информации в качестве самостоятельного вида доказательства без привязки к протоколу следственного действия, а также проработать механизм подтверждения легитимности и достоверности записанных на носитель сведений.

Сбор электронной информации на локальных электронных носителях зачастую происходит посредствам копирования информации. В некоторых случаях приходится проводит изъятие электронных носителей информации, что требует получения судебного разрешения и привлечения специалиста.

Говоря о сборе электронной информации на сетевых носителях, необходимо отметить, что большинство авторов, исследовавших вопрос о процессуальном порядке собирания доказательственной информации в компьютерных сетях, поддерживают тезис о необходимости его совершенствования. Его направлениями видится введение в уголовно-процессуальное законодательство особых правовых процедур в рамках следственного осмотра и обыска.

В ходе исследования установлена необходимость внедрения системы специфических критериев оценки допустимости доказательственной информации на электронных носителях, к числу которых относятся:

аутентичность информации как возможность достоверного установления источника ее происхождения;

целостность информации как отсутствие изменений в ее составе,

содержании и свойствах;

достоверность информации – точное отражение определенных явлений, процессов, деятельности или фактов;

доступность для восприятия с использованием надлежащего программного обеспечения и технических средств обработки, не влекущих внесение в нее изменений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, 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 14марта 2020 г. № 1-ФКЗ // Собр. законодательства Рос. Федерации.– 2020. – № 11, ст.1416.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 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.

3. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 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. I), ст. 4921.

4. Часть четвертая Гражданского кодекса Российской Федерации от 18 декабря 2006 г. № 230-ФЗ принят Гос. Думой Федер. Собр. Рос. Федерации 24 нояб. 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 8 дек. 2006 г. // Собр. законодательства Рос. Федерации. – 2006. – № 52 (часть I), ст. 5496.

5. О полиции: федер. закон Рос. Федерации от 7 февраля 2011 г. № 3-ФЗ: принят Гос. Думой 28 января 2001 г.: одобр. Советом Федерации Федерального Собрания Рос. Федерации 2 февраля 2001 г. // Собр. законодательства Рос. Федерации. – 2011. – № 7, (ч. I), ст. 900.

6. Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 5 июля 1995 г. // Собр. законодательства Рос. Федерации. – 1995. – № 33. ст. 3349.

7. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июля 2006 г. // Рос.газ. – 2006. – 3 августа.

8. О связи: федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 28 июня 2003 г. // Рос.газ. – 2003. – 13 июля.

9. О коммерческой тайне: федер. закон от 29 июля 2004 г. № 98-ФЗ:принят Гос. Думой Федер. Собр. Рос. Федерации 9 июля 2004 г.: одобрен Советом Федерации Федер. Собр. Рос. Федерации 15 июля 2004 г. // Собр. законодательства Рос. Федерации. – 2004. – № 52, ст. 3283.

10. Об утверждении Перечня сведений конфиденциального характера: указ Президента Российской Федерации от 6 марта 1997 г. № 188 // Доступ из справ.-правовой системы «Гарант».

11. ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения // Электронный фонд правовой и нормативно-технической документации: сайт. [Электронный ресурс]. URL: http://docs.cntd.ru/document/ (дата обращения: 12.09.2021).

II. Учебная, научная литература и иные материалы

1. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г. и др. Криминалистика. Учебник [Текст]. – М: Инфра-М, Норма, 2017. 928 с.

2. Андриенко Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам / Ю. А. Андриенко // Вестник Сибирского юридического института МВД России. 2018. № 3 (32).

3. Антонович Е. К. Использование цифровых технологий при допросе

свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) / Е. К. Антонович. [Текст] // Актуальные проблемы российского права. 2019. № 6 (103).

4. Бажанов С.В. Состояние законности при возбуждении уголовных дел и расследовании преступлений, совершаемых предпринимателями / С. В. Бажанов // Право и экономика. 2017. № 8. 80 с.

5. Балашова А. А. Место и роль электронных носителей информации в системе источников доказательств / А. А. Балашова // Образование. Наука. Научные кадры. 2018. № 4. 94 с.

6. Бахтеев Д. В. Основы теории электронных доказательств: монография / Д. В. Бахтеев; под ред. д-ра юрид. наук С. В. Зуева. [Текст]. М.: Юрлитинформ, 2019. 166 с.

7. Вехов В. Б. Основы теории электронных доказательств: монография / В. Б. Вехов; под ред. д-ра юрид. наук С. В. Зуева [Текст]. – М.: Юрлитинформ, 2019. 398 с.

8. Григорьев В. Н. Основы теории электронных доказательств: монография / В. Н. Григорьев; под ред. д-ра юрид. наук С. В. Зуева. [Текст]. – М.: Юрлитинформ, 2019. 258 с.

9. Громов Н .А. Доказательства: их виды и доказывание в уголовном процессе: учеб.-практ. пособие / Н. А. Громов, С. А. Зайцева, А. Н. Гущин. [Текст]. – М.: Приор-издат, 2018. 81 с.

10. Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук / А. И. Зазулин. [Текст]. Екатеринбург, 2018. 250 с.

11. Зуев С. В. Электронные доказательства, используемые в уголовном процессе: монография / С. В. Зуев; под ред. д-ра юрид. наук С. В. Зуева. [Текст]. – М.: Юрлитинформ, 2019. 148 с.

12. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / под общ.ред. В. В. Мозякова. – М.: 2021. 908 с.

13. Криминалистическая тактика / отв. ред. В. Н. Карагодин, Е. В. Шишкина [Текст]. Екатеринбург, 2018. 119 с.

14. Крюкова Н. И., Косолапова Н. В. Криминалистика. Учебное пособие [Текст]. – М: Юстиция, 2019. 256 с.

15. Кульков В. В. Методика предварительного следствия. Руководство для следователей и дознавателей: практ. пособие [Текст] / В. В. Кульков, П. В. Ракчеева. – М.: Издательство Юрайт, 2017. 288 с.

16. Лавров В. П., Шалимов А. Н., Романов В. И. и др.. Криминалистика. Конспект лекций [Текст]. – М.: Проспект, 2020. 256 с.

17. Макаренко И. А. Общетеоретические основы расследования преступлений: учебник и практикум для академического бакалавриата [Текст] / И. А. Макаренко, Р. И. Зайнуллин, А. Ф. Халиуллина. – М.: Юрайт, 2017. 205 с.

18. Моисеев Н. А. Криминалистическая методика [Текст]. Белгород: БелЮИ, 2017. 196 с.

19. Нахова Е. А. Проблемы электронных доказательств в цивилистическо м процессе // Ленинградский юридический журнал. 2019. № 4. 410 с.

20. Пастухов П. С. Средства проверки надежности «электронных» доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2019. № 3. 284 с.

21. Савельева М. В., Смушкин А. Б. Криминалистика. Учебное пособие [Текст]. – М: Феникс, 2017. 288 с.

22. Скобелин С. Ю. Криминалистика. Учебник. [Текст]. – М: Проспект, 2021. 256 с.

23. Современная кибербезопасность: учебное пособие [Текст] / Н. И. Долженко, Н. А. Жукова, И. А. Ярощук. Белгород: ИД «БелГУ» НИУ «БелГУ», 2021. 78 с.

24. Состояние преступности в России за январь - декабрь 2020 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/ 22678184 (дата обращения 12.03.2022).

25. Состояние преступности в России за январь - декабрь 2021 года

[Электронный ресурс]. URL: https://мвд.рф/reports/item/28021552 (дата обращения 22.04.2022)

26. Толковый словарь русского языка [Текст] / Под редакцией Д. В. Дмитриева. – М.: Астрель, АСТ, 2018. 592 с.

27. Топорков А. А. Криминалистика. Учебник [Текст]. – М: Инфра-М, Контракт, 2019. 464 с.

28. Тюнис И. О. Криминалистика. Учебное пособие [Текст]. – М: Проспект, 2020. 220 с.

29. Чурилов С. Н. Криминалистическая методика расследования [Текст]. – М.: Юстицинформ, 2017. 204 с.

30. Шапошников А. Ю. Практическая криминалистика. Учебник [Текст]. СПб: Питер, 2017. 384 с.

III. Эмпирические материалы

1. Приговор № 1-62/2019 от 26 февраля 2019 г. по делу № 1-62/2019 [Электронный ресурс]. https://sudact.ru/regular/doc/LKScMPwjregular-judge=&_=1652511666837 (дата обращения 03.05.2022).

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

И.И. Беккер