ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДАЛЬНЕВОСТОЧНЫЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МИНИСТЕРСТВА
ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Черкасов Виктор Сергеевич

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ В ДОКАЗЫВАНИИ НА ДОСУДЕБНЫХ СТАДИЯХ УГОЛОВНОГО ПРОЦЕССА

Специальность: 12.00.09 – уголовный процесс

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук
доцент Зуев С.В.

Хабаровск – 2022

ОГЛАВЛЕНИЕ

Введение…….. 3

Глава 1. Электронные средства уголовно-процессуального доказывания: генезис, сущность, правовая природа…….. 15

§ 1.1. Влияние развития информационных технологий на досудебное производство по уголовным делам: процессуальный аспект…….. 15

§ 1.2. Электронные средства уголовно-процессуального доказывания: понятие, виды, природа электронной информации…….. 31

§ 1.3. Роль и значение электронной информации в системе источников уголовно-процессуальных доказательств…….. 58

Глава 2. Совершенствование механизма правового регулирования применения электронных средств в доказывании на досудебных стадиях уголового процесса…… 74

§ 2.1. Собирание электронной информации и (или) ее материальных носителей в ходе производства следственных действий…… 79

§ 2.2. Правовое регулирование применения следственных действий электронно-технического характера…….. 106

§ 2.3. Использование в доказывании результатов розыскной деятельности, осуществляемой с применением электронных средств, следователем и органом дознании…….. 128

Заключение…… 163

Список использованных источников…….. 169

Проложения……... 197

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена тем, что информационные технологии в современном мире интенсивно интегрируются в экономическую, политическую, духовную и социальную сферу жизнедеятельности общества. Обозначенный процесс делает современную жизнь человека, с одной стороны, более комфортным и утилитарной, а с другой, создает дополнительные возможности для совершения преступлений.

Так, криминогенная обстановка характеризуется распространением преступлений, совершенных при помощи компьютерных и телекоммуникационных технологий. По данным Главного информационного аналитического центра МВД России, в 2016 году зарегистрировано 65949 преступлений, приостановлено – 49111. В 2017 году выявлено 90587 преступлений, раскрыто за этот период всего 20424. В 2018 году зарегистрировано 174674 преступления, что больше на 92,8% по сравнению с АППГ; раскрыто 43362. В 2019 году зарегистрировано 240144 преступления, что больше на 80,9% по сравнению с АППГ; раскрыто в том же году 51051 преступление. В 2020 году было зарегистрировано 510396 преступления, раскрыто за отчетный период 94942. В 2021 зарегистрировано 517722, раскрыто 118920 преступления[1].

Статистические данные позволяют сделать вывод, что количество совершаемых преступлений рассматриваемой категории возрастает. При этом их раскрываемость находится на относительно низком уровне.

Не трудно заметить, что внедрение информационных технологий в деятельность правоохранительных органов коренным образом меняет порядок их действий, в том числе при использовании электронных средств в доказывании по уголовным делам. Это обусловлено тем, что значительный массив информации, в

[1] Статистика преступлений, совершаемых при помощи компьютерных и телекоммуникационных технологий за 2015-2021 год / ГИАЦ МВД России; Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/search/ (дата обращения: 20.02.2022).

том числе о частной жизни граждан, хранится на электронных устройствах и передается с помощью сети «Интернет».

Вместе с тем состояние действующего уголовно-процессуального законодательства не позволяет благополучно использовать все возможности, соответствующие последним достижениям науки и техники.

Репрезентативный опрос следователей и дознавателей показал общую неудовлетворенность представителей органов предварительного расследования состоянием уголовно-процессуального законодательства в регламентации использования электронных средств в доказывании. Так, 84% опрошенных указали на потребность в использовании электронных средств в доказывании по уголовному делу; 82% респондентов считают, что необходимо реформировать уголовно-процессуальное законодательство в целях создания условий для применения электронных средств в доказывании по уголовному делу[2].

Изменение процессуальных правил и дальнейшее расширение возможностей органов предварительного расследования в применении электронных средств в доказывании по уголовному делу должно сопровождаться совершенствованием гарантий неприкосновенности частной жизни, а также различных охраняемых законом тайн.

Изложенное приводит к необходимости разработки научно-теоретической и практико-ориентированной концепции, направленной на приведение уголовно-процессуального законодательства, регламентирующего досудебное производство по уголовным делам, в соответствие с информационно-телекоммуникационными потребностями (возможностями) общества и государства с учетом общего расширения применения информационных технологий в уголовном судопроизводстве.

Таким образом, актуальность темы данного исследования определяется, с теоретической стороны, слабой разработанностью вопросов изменения сущности доказывания и доказательств под влиянием информационных технологий, с

---

[2] Анкетирование проводился в период с ноября 2019 по январь 2020 года среди сотрудников следственных подразделений органов внутренних дел из 24 субъектах Российской федерации. Результаты представлены в Приложении № 2.

практической стороны – недостатками уголовно-процессуального регулирования порядка применения электронных средств в доказывании по уголовным делам и защиты различных видов тайн при осуществлении уголовного преследования.

Степень научной разработанности темы исследования. Недостатки правового регулирования процессуального порядка получения информации с электронных носителей, а также сведений, передаваемых посредством электросвязи, были рассмотрены в трудах известных ученых: А.С. Александрова, О.И. Андреевой, Н.А. Архиповой, А.В. Булыжкина, В.Ф. Васюкова, О.А. Зайцев, А.И. Зазулина, С.В. Зуева, Н.А. Зигуры, А.Л. Осипенко, Р.И. Оконенко, П.С. Пастухова, М.С. Сергеева, Д.Н. Серетенцев, В.Ю. Стельмах, Н.Г. Шурухнова и многих других.

Фундаментальные разработки вопросов теории доказывания в уголовном процессе осуществлялись такими процессуалистами, как: В.А. Азаров, В.С. Балакшин, А.Р. Белкин, А.М. Баранов, Л.А Воскобитова, Б.Я. Гаврилов, Л.В. Головко, О.Г. Григорьев, А.В. Гришин, А.А. Давлетов, Ю.В. Деришев, Е.А. Доля, З.З. Зинатуллин, К.Б. Калиновский, В.А. Лазарева, П.А. Лупинцкая, Л.Н. Масленикова, С.А. Шейфер, В.С. Шадрин, М.С. Строгович, В.А. Семенцов, А.В. Смирнов, С.Б. Россинский, Ю.К. Орлов, П.С. Пастухов, О.В. Химичева и другими.

Различные вопросы применения электронных средств в доказывании по уголовным делам в той или иной степени рассматривались в уголовно-процессуальной науке. Влияние информационных технологий на теорию уголовно-процессуальных доказательств рассматривались Н.А. Зигурой (Челябинск, 2010), П.С. Пастуховым (Москва, 2015), коллективом авторов в монографиях под редакцией С.В. Зуева (Москва, 2019).

Проблемы соблюдения конституционных прав гражданина на неприкосновенность частной жизни при собирании электронной информации были детально рассмотрены Р.И. Оконенко (Москва, 2016). Значительный вклад в развитие вопросов собирания, закрепления и оценки сведений, полученных с применением электронных средств, внесли исследования: В.Ю. Стельмаха

(Екатеринбург, 2013), И.А. Зазулина (Екатеринбург, 2018), М.С. Сергеева (Казань, 2018).

Существенное теоретическое и практическое значение в области применения информационных технологий при производстве следственных действий сыграли работы: Е.А. Архиповой (Москва, 2013), И.В. Казначея (Волгоград, 2014). Отдельные вопросы использования электронных технических средств рассматривал И.И. Литвин (Екатеринбург, 2018).

Научные исследования рассмотренных авторов позволили значительно продвинуться в понимании отдельных аспектов использования электронных средств в уголовном судопроизводстве. Однако так и не удалось определить общую тенденцию развития данного явления, выявить особенности его проявления в доказывании на досудебных стадиях уголовного процесса, многие положения требуют дополнительной научной проработки и аргументации.

Объектом исследования выступают отношения, складывающиеся при использовании электронных средств в доказывании на досудебных стадиях уголовного процесса.

Предмет исследования составляют уголовно-процессуальные нормы международного, отечественного и зарубежного права, определяющие порядок применения электронных средств в ходе досудебного производства по уголовным делам, а также соответствующие материалы судебно-следственной практики и положения уголовно-процессуальной науки.

Цель исследования заключается в получении нового знания в области уголовно-процессуальных доказательств, разработке теоретически значимых положений и научно-обоснованных предложений по совершенствованию уголовно-процессуального законодательства, направленного на регламентацию порядка применения электронных средств в доказывании на досудебных стадиях уголовного процесса.

Для достижения указанной цели поставлены следующие **задачи:**

1) раскрыть влияние развития информационно-телекоммуникационных технологий на досудебное производство по уголовным делам;

2) выявить случаи изменения процессуальной формы и определить закономерности формирующейся практики применения электронных средств при установлении обстоятельств, подлежащих доказыванию, органами предварительного расследования;

3) провести ревизию нормативного регулирования уголовно-процессуальных отношений в сфере применения электронных средств на досудебных стадиях уголовного процесса, вскрыть слабые стороны, недостатки, пробелы; предопределить тенденции развития; сформулировать предложения по совершенствованию правового механизма;

4) рассмотреть природу электронных средств, раскрыть их виды, особенности, процессуальные элементы, сопровождающие их применение в доказывании на досудебном производстве по уголовным делам;

5) обобщить теоретические подходы по определению места и роли электронных средств в обеспечении уголовных дел необходимой совокупностью доказательств, отвечающих предъявляемыми к ним требованиями;

6) выявить проблемы использования в доказывании результатов розыскной деятельности, полученных с помощью электронных технических средств, следователем и органом дознания в расследовании преступлений;

7) изучить зарубежный опыт применения электронных средств в доказывании, оценить возможность его использования в отечественном досудебном производстве по уголовным делам.

Теоретическая значимость исследования обусловлена тем, что предложения и выводы автора могут быть основной для дальнейших исследований по применению электронных средств в доказывании по уголовным делам и развития теории уголовно-процессуальных доказательств с учетом влияния информационных технологий на общественные отношения.

Практическая значимость исследования заключается в том, что результаты, выводы, предложения и рекомендации по итогам исследования могут быть использованы в практической деятельности сотрудниками органов предварительного расследования при подготовке предложений по

совершенствованию законодательства. Изложенные в диссертации положения могут быть внедрены в учебный процесс, в том числе для преподавания дисциплины «Уголовный процесс» и иных специальных дисциплин.

Методология и методы исследования. Методологической основой научного познания служит диалектический метод, с помощью которого изучаются количественные изменения общественных отношений, происходящие под влиянием стремительно развивающихся информационно-телекоммуникационных технологий, и, следовательно, приводящие к формированию и закреплению качественно новых уголовно-процессуальных правоотношений по применению электронных средств в доказывании по уголовным делам. В процессе исследования использовался обширный методологический инструментарий. Были использованы общенаучные методы. Так, дедукция использовалась для выявления закономерностей практики правоприменения и единства научных подходов в вопросах применения электронных средств в доказывании по уголовным делам. На основе индукции исследован вопрос действия уголовно-процессуального права в информационно-телекоммуникационном пространстве. Анализ позволил выделить элементы электронных средств в доказывании по уголовным делам. Синтез позволил объединить практический опыт применения информационных технологий при производстве следственных действий в единый механизм правового регулирования. Производилась статистическая обработка результатов социологического исследования.

Применялись частные методы юридической науки, одним из которых являлось лексическое, юридическое и техническое толкование значения понятий в рамках специфики рассматриваемых в исследовании общественных отношений. В свою очередь, сравнительное правоведение использовалось для сопоставления особенностей правового регулирования применения электронных средств в доказывании по уголовному делу в России и зарубежных странах. Системно-структурный метод использовался для установления взаимосвязи между физическими свойствами электронной информации и свойством достоверности уголовно-процессуальных доказательств. Исторический метод использовался для

исследования процесса развития правового регулирования общественных отношений по применению электронных средств в доказывании по уголовным делам.

Эмпирическую основу исследования составляют определения Конституционного суда Российской Федерации, Постановления Европейского суда по правам человека, опубликованная практика Верховного суда РФ. Автором изучено 623 уголовных дела. Проведено анкетирование следователей и дознавателей МВД РФ, следователей Следственного комитета Российской Федерации в общем количестве 536 человек из 24 субъектов Российской Федерации среди которых Хабаровский край, Приморский край, Камчатский край, Красноярский край, Амурская область, Свердловская область, Ростовская область, Москва и др.

Научная новизна диссертационного исследования состоит в том, что выделена система электронных средств в доказывании по уголовным делам как результат влияния информационных технологий на развитие уголовно-процессуальных отношений. Произведено комплексное исследование различных аспектов применения электронных средств в доказывании на досудебных стадиях уголовного процесса.

В работе выделяются такие элементы электронных средств, используемых в доказывании по уголовным делам, как: следственные действия, направленные на собирание и проверку доказательств в электронном виде; электронные носители информации; электронная информация; дистанционные формы коммуникации и способы обращения (подача заявлений, жалоб, ходатайств) посредством электронной связи; сайты; облачные пространства сети «Интернет», программное обеспечение персональных компьютеров и др.

Результатом применения и основным источником доказательств в электронном виде в уголовном судопроизводстве является электронная информация. При определении ее значения в уголовном процессе рассматриваются ее гносеологические особенности и юридические свойства при использовании в доказывании по уголовным делам. В исследовании

обосновывается возможность использования электронной информации в качестве содержательной части вещественных доказательств, иных документов, показаний допрошенных лиц, протоколов следственных действий.

Выявляются закономерности изменения процессуальных форм (процедур) относительно применения тех или иных электронных средств, и каким образом это сказывается или может сказаться на сохранении и обеспечении прав граждан в сфере уголовно-процессуальных отношений. Утверждается, что применение электронных средств в доказывании на досудебных стадиях уголовного процесса способно значительно изменить «облик» традиционного производства по уголовным делам. Обосновывается необходимость существенной модернизации норм уголовно-процессуального законодательства для сохранения стабильности в восприятии законности осуществления уголовного досудебного производства.

Автором выявлены недостатки в обеспечении уголовно-процессуальных и иных правовых гарантий соблюдения прав личности на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при производстве следственных действий, направленных на получение электронной информации, и сформированы предложения по совершенствованию правовых актов, обеспечивающих юридические гарантии защиты различных видов тайн.

Новизну результатов и выводов исследования обеспечили положения, выносимые на защиту:

1. Электронные средства, используемые в доказывании на досудебных стадиях уголовного процесса, – это совокупность уголовно-процессуальных и аппаратно-программных средств направленных на собирание, проверку и оценку доказательств, выраженных в электронном виде, а также обеспечивающих производство следственных действий.

Результатом применения электронных средств и основным источником доказательств в электронном виде в уголовном судопроизводстве является электронная информация. Под электронной информацией следует понимать сведения (сообщения, данные) передача, обработка, воспроизведение которых осуществляется посредством электронных аппаратно-программных средств.

Понятие электронной информации вбирает в себя цифровую и аналоговую информацию, передаваемую посредством электронной связи.

2. Элементами системы электронных средств, используемых в доказывании по уголовным делам, следует считать: следственные действия, направленные на собирание и проверку доказательств в электронном виде, электронную информацию, электронные носители информации, дистанционные формы коммуникации и способы обращения (подача заявлений, жалоб, ходатайств) посредством электронной связи; сайты; облачные пространства сети «Интернет», программное обеспечение персональных компьютеров, которые предопределяют способы собирания, проверки и оценки доказательств.

3. Обобщены научные подходы, определяющие процессуальное положение электронной информации в качестве источника уголовно-процессуальных доказательств. Учитывая дуалистическую природу электронной информации с присущими ей признаками вещественных доказательств и иных документов, а также отсутствие самостоятельного законодательного регулирования порядка обращения с ней, к электронным носителям информации, содержащим следы преступления, следует относиться как к вещественным доказательствам. Когда же требуется информация справочного характера необходимо применять правовой режим иного документа. Признание электронной информации отдельным источником уголовно-процессуальных доказательств породит многочисленные коллизии в устоявшейся правовой доктрине уголовного процесса.

4. Уголовно-процессуальный порядок собирания доказательств с использованием осмотра электронных носителей информации и назначения компьютерно-технической экспертизы без получения судебного решения в отношении электронных носителей, позволяющих передавать информацию по сетям электросвязи, приводит к нарушению права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также иных видов охраняемых законом тайн.

5. С учетом особенностей функционирования современного оконечного оборудования и объема концентрации информации о частной жизни человека на одном электронном носители, разграничительные признаки обыска и осмотра не являются достаточными и не адаптированы к общественным отношениям, сформированным под воздействием информационных технологий. Это приводит к тому, что в следственной практике обыск подменяется осмотром при производстве следственных действий в отношении электронного носителя информации. С учетом научных подходов, разграничительные критерии следует формулировать с учетом положения: «степени возможного вторжения правоохранительных органов в частную жизнь человека».

С учетом названого теоретического положения**,** предлагаются законодательные поправки в ст.ст. 29, 165, 176, 182, 195 УПК РФ, которые учитывают волеизъявление владельца электронного носителя информации и функций устройства по воспроизведению и передачу данных по электросвязи. Определяется, в каких случаях необходимо производить обыск или осмотр электронного носителя информации, а также когда необходимо получать судебное решение для назначения судебной экспертизы и производства обыска электронного носителя информации.

6. Обобщены научные теории, раскрывающие порядок регулирования действия уголовно-процессуального законодательства в нефизическом пространстве («киберпространстве»), сформированном с помощью компьютерных программ и сетей, потоками данным, информационно-телекоммуникационными средствами связи. Предлагается рассматривать названное пространство с точки зрения международных территорий, с учетом определенных ограничений. Объектом трансграничных следственных действий может выступать только индивидуально-определенная область, которая привязана к лицу, посредством данных, которые позволяют или могут позволить его идентифицировать (сетевой адрес, электронная почта и т. д.). Недопустимо производить трансграничные следственные действия в тех случаях, когда может создаться угроза вмешательства в суверенитет иностранного государства или

иным образом затронуты публичные интересы. В данном случае следственное действие необходимо произвести в рамках международной правовой помощи.

7. В соответствии со ст. 164.1 УПК РФ устанавливается требование на участие специалиста при изъятии электронных носителей информации, что является анахронизмом, так как многие современные информационные технологии в большинстве случаев общедоступны, просты в обращении и не требуют специальных знаний. Для разрешения названного недостатка предлагается авторская редакция ст. 164.1 УПК РФ.

8. В целях совершенствования порядка использования электронных средств в доказывании на досудебных стадиях уголовного судопроизводства предлагается исключить ч. 7 из ст. 185 УПК РФ. Следственное действие «контроль и запись переговоров» (ст. 186 УПК РФ) заменить на «контроль электросвязи», которое, кроме мониторинга, перехвата, получения содержания телекоммуникаций, будет включать их арест. Вместо понятия «контроль телефонных и иных переговоров» в ст. 5 п. 14.1. УПК РФ предлагается закрепить понятие «контроль электросвязи» и изложить его в авторской редакции.

Апробация и внедрение результатов исследования. Теоретические положения, выводы и рекомендации, изложенные в диссертационном исследовании, нашли отражение в 18 работах общим объемом 8 п. л., девять из которых опубликованы в научных изданиях, входящих в перечень научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук.

Выводы, изложенные в работе, были представлены на Международной научно-практической конференции «Отечественная наука в эпоху изменений: постулаты прошлого и теории нового времени» (Российский государственный гуманитарный университет, г. Екатеринбург) в 2015 году, Всероссийском круглом столе «Проблемы соблюдения прав участников уголовного судопроизводства» (Дальневосточный юридический институт МВД России, г. Хабаровск) в 2017 году, Межрегиональной научно-практической конференции «Пятнадцатилетний опыт применения УПК РФ: Теория, практика и направления

развития уголовно-процессуального законодательства в России» (Пятый факультет повышения квалификации Московской академия следственного комитета Российской Федерации, г. Хабаровск) в 2018 году, Международной конференции «Актуальные проблемы юридической науки и практики» (Дальневосточный юридический институт МВД России, г. Хабаровск) в 2019 году, Всероссийской научно-практической конференции «Гуманитарные чтения» (Дальневосточный федеральный университет г. Владивосток) в 2020 году, XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае» (Алтайский государственный университет г. Барнаул) в 2021 году. В период с 2016 по 2018 гг. научные работы на основе диссертационного исследования становились лауреатами конкурса «Моя законотворческая инициатива» (г. Москва).

Рекомендации и предложения, содержащиеся в диссертационном исследовании, внедрены в практическую деятельность Следственного управления УМВД России по Приморскому краю, а также в учебный процесс Дальневосточного юридического института МВД России, что подтверждается соответствующими актами.

Структура и объем работы. Исследование состоит из введения, 2 глав, разделенных на 6 параграфов, заключения, списка использованных источников, а также 3 приложений.

ГЛАВА 1. ЭЛЕКТРОННЫЕ СРЕДСТВА УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ДОКАЗЫВАНИЯ: ГЕНЕЗИС, СУЩНОСТЬ, ПРАВОВАЯ ПРИРОДА

§ 1.1. Влияние развития информационных технологий на досудебное производство по уголовным делам: процессуальный аспект

Любая теория есть «система идеальных образов (понятий), отражающих сущность исследуемого объекта, его внутренние необходимые связи, законы его функционирования и развития»[3]. В связи с этим развитие теоретических представлений о влиянии информационных технологий на досудебное производство по уголовным делам логично начинать с уяснения основных понятий, выявления закономерностей и связей исследуемых явлений, генезис их взаимодействия.

В понятийном аппарате отражается специфика изучаемой предметной области. Поэтому настоящее исследование получит отправную точку именно с уяснения того, что такое информационные технологии, каким образом они влияют на уголовный процесс, обусловленный нормами уголовно-процессуального законодательства и практикой правоприменения. Это позволит перенести рассматриваемую систему правоотношений в некую проблемную плоскость, за которой можно увидеть процессуальные действия и решения в рамках досудебного производства по уголовным делам, нуждающихся в преобразовании.

Проблематичность должна предстать перед человеком как неотъемлемая часть исследования существующих предметов и явлений, обнажив некие пробелы и противоречия в уголовно-процессуальной деятельности. Усилить противоречие поможет обнаруженное основное несоответствие между целью и используемыми средствами достижения желаемого результата. Для снижения проблемы может потребоваться изменение средств и координация цели. Изменение цели осуществления правосудия вряд ли отражает потребности общества и

[3] Шептулин А.П. Диалектический метод познания. М. : Политиздат, 1983. С. 20.

государства, в этом плане более уместно гарантированная защищенность и уважение прав и свобод человека и гражданина. Поэтому нашему вниманию будут удостоены средства ее достижения, а именно понятия, нормы действующего законодательства и практика расследования преступлений.

Рассматривая вопрос развития информационных технологий в уголовном досудебном производстве, необходимо определиться с основным понятием «информационные технологии» и его сущностью. В соответствии с п. 2 ст. 2 Федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»[4] (далее Закон Об информации) под информационными технологиями понимается «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

На основании п. 1 ст. 2 того же Закона, информация – это «сведения (сообщения, данные) независимо от формы их представления». Исходя из этого можно заметить, что объем понятия «информационные технологии» вбирает все существующие явления, процессы, способы, где информация является объектом деятельности. При этом законодатель раскрывает наиболее общие функциональные признаки информационных технологий.

Таким образом, к информационным технологиям относится не только многообразие электронно-вычислительных устройств, но и любые другие устройства (механические и аналоговые), объектом деятельности которых является информация. Более того, исходя из законодательного определения, информационной технологией не обязательно должно быть какое-то устройство. Информационной технологией может быть идеальная система, к примеру, символьная языковая система (русский алфавит, фонетика).

Примечательно то, что в научной литературе выделяют восемь информационных революций: 1) естественный интеллект; 2) невербальный язык; 3) вербальный язык; 4) письменность; 5) книгопечатание; 6) телеграф, телефония

[4] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 02.07.2021) // Гарант: справ. правовая система. URL: http://base.garant.ru/12148555/ (дата обращения: 01.08.2021 г.).

и телевидение; 7) электронно-вычислительные машины (компьютерная революция); 8) компьютерные сети и сеть Интернет (Интернет-революция). Первые три революции являли собой эндогенное *(от греч. endon – внутри и genos – происхождение)* развитие технологий для работы с информацией. Память, невербальный и вербальный языки – это внутренние, личностные инструменты человека. Остальные представляют собой применение экзогенных (от *греч. exo – вне, снаружи)* технологий, т. е. использование внешних по отношению к человеку инструментов хранения, обработки и передачи информации[5].

Поэтому современное значение исследуемого термина несколько трансформируется, акцентируется внимание на сферу применения современных электронно-телекоммуникационных технологий. Последние три революции были связаны с внедрением телефонии, телевидения, ЭВМ, компьютерных сетей, то есть аппаратно-программных средств, работа которых преимущественно основана на электромагнитных свойствах материи.

Напомним, что аппаратные средства – это комплекс технических устройств, обеспечивающих ввод, обработку, трансляцию и фиксацию информации, предоставление доступа к удаленным информационным ресурсам. Программные средства – совокупность правил и алгоритмов, записанных на одном из языков программирования, позволяющих пользователю работать с разными видами информации[6].

Более того, в настоящий момент в Российской Федерации на основе международного стандарта ISO/IEC 2382:2015 принят ГОСТ 33707—2016 под названием «Информационные технологии. Словарь»[7], который фактически является переводом и частичной переработкой международного стандарта (словаря) в сфере информационных технологий. В данном словаре в основном

---

[5] Караваев Н.Л. Феномен информатизации: терминологический анализ понятия / Н.Л. Караев // Информатизация образования и науки. 2014. № 4(24). С. 4-6.

[6] Сухова Ж.В. Понятие информационных технологий: сущность и классификация // Инновационные научные исследования: теория, методология, практика. 2016. № 6. С. 73.

[7] ГОСТ 33707-2016 «Информационные технологии. Словарь» / введен в действие Приказом Росстандарта от 22.09.2016 № 1189-ст. // URL: https://docs.cntd.ru/document/1200139532 (дата обращения: 11.06.2020 г.).

содержится терминология, касающаяся информационно-телекоммуникационных технологий (дифференциальное кодирование, оптический диск, пиксель и т. п.).

Некоторые авторы, пытаясь выделить в структуре информационных технологий современные электронные вычислительные программно-аппаратные средства, предлагают использовать иные категории. К примеру, М.О. Медведева предлагает использовать категорию «высокие информационные технологии», которая с точки зрения автора должна обозначать – процессы, методы поиска, сбора, формирования, хранения, обработки, представления, предоставления, передачи, распространения информации и способы осуществления таких процессов и методов с применением средств вычислительной техники и средств телекоммуникации». Как указывает М.О. Медведева: «существенным отличием «высоких информационных технологий» от «информационных технологий» является применение средств вычислительной техники и средств телекоммуникации и специфика процессов в них протекающих»[8].

В научной литературе встречается понятие «информационно-коммуникационные технологии», под которым понимается «совокупность методов, производственных процессов, программно-технических и лингвистических средств, интегрируемых с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей»[9]. При этом в названном источнике понятия «информационные технологии» и «информационно-коммуникационные технологии» отождествляются, что в некоторых случаях не критично и вполне допустимо.

Представляется, что ввод дополнительной категории, обозначающей отдельный вид вычислительных аппаратно-программных информационных технологий, является нецелесообразным, так как уже существуют международные и отечественные стандарты, отождествляющие информационные

---

[8] Зуев С.В., Бахтеев Д.В., Задорожная В.А., Зазулин А.И., Захарова В.К., Пастухов П.С., Стрелкова Ю.В. Информационные технологии в уголовном процессе зарубежных стран: монография. М.: Юрлитинформ, 2020. С. 25.

[9] Хохлов Ю.Е. Глоссарий по информационному обществу. М.: Институт развития информационного общества, 2009. С. 64.

технологии с электронными программно-аппаратными средствами.

Информационные технологии необходимо понимать в широком и узком смысле. В широком смысле под информационными технологиями понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (п. 2 ст. 2 Закона Об информации). В узком – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, совершаемых с использованием электронных аппаратно-программных средств. В рамках исследования категория информационные технологии будет использоваться в узком смысле.

Изучение научных представлений, изменений законодательства и практики расследования преступлений позволило выделить несколько этапов, характеризующих уровень влияния развития информационных технологий на досудебное уголовное судопроизводство.

Первый этап условно можно обозначить как *процесс внедрения информационных технологий в уголовный процесс и утверждение данного направления науки уголовного процесса как приоритетного*. Данный этап сопровождается нормативным закреплением информационных технологий и смежных категорий в УПК РФ, в других нормативных правовых актах, а также появлением первых научных трудов в названной сфере.

Так, законодательное регулирование вопросов, связанных с внедрением в классическую модель уголовно-процессуальных средств доказывания информационных технологий, является достаточно молодым явлением для уголовного процесса. Оно берет свое начало с введением Федеральным законом от 01.07.2010 № 143-ФЗ[10] следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами», предусмотренного ст. 186.1 УПК РФ, а также с введение соответствующего

[10] Федеральный закон от 01.07.2010 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2010. 07 июля.

понятия в ст. 5 п. 24.1. УПК РФ.

Далее, в 2012 году, законодатель, пытаясь расширить уголовно-процессуальное правовое поле в электронно-информационной сфере, Федеральным законом от 28.07.2012 № 143-ФЗ[11] вводит дополнительную категорию «электронный носитель информации» и вносит поправки в ряд статей УПК РФ: 81, 82, 166, 182, 183, предусматривающие специальный порядок изъятия электронных носителей, копирования с них информации, хранения и возврат владельцу при производстве обыска и выемки. Федеральным законом от 03.07.2016 № 323-ФЗ[12] УПК РФ был дополнен статьей 81.1, определяющей механизм признания, хранения и возврата электронных носителей информации при расследовании преступлений в сфере предпринимательской деятельности[13].

Так, понятию «электронный носитель информации» не дано легального определения. Как верно указывают в своей работе В.Ф. Васюков, А.В. Булыжкин: «Анализ литературы, посвященной заявленной проблематике, свидетельствует о том, что большинство авторов, истолковывая указанный термин, опираются на стандарты, установленные в единой системе конструкторской документации. Этой логике, как представляется, следовали и разработчики законопроекта. Между тем, в соответствии с положениями подп. 3.1.9 ГОСТа 2.051-2013, под электронным носителем понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью

[11] Федеральный закон от 28.07.2012 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2012. 01 августа.

[12] Федеральным закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности» // Российская газета. 2016. 08 июля.

[13] В настоящий момент ч. 9.1. ст. 182 и ч. 3.1. ст. 183 УПК РФ, устанавливающие порядок изъятия и копирования информации с электронных носителей при производстве обыска и выемки, Федеральным законом от 27.12.2018 г. № 533-ФЗ признаны утратившими силу. Вместо названных положений в УПК РФ введена статья 164.1. «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

средств вычислительной техники»[14].

Такими свойствами как запись, хранение и воспроизведение электронной информации обладают большинство цифровых устройств, используемых для работы со сведениями, выраженными в электронной форме (флеш-накопитель, оптический диск, ноутбук, мобильный телефон и т. д.), что позволяет включить в категорию «электронные носители информации» неограниченное число технических устройств.

Необходимо отметить, что в 2018 году порядок обращения с электронными средствами был вновь изменен[15]. В частности, УПК РФ был дополнен статьей «164.1. Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

Сравнивая ранее действующие положения ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ относительно новеллы ст. 164.1. УПК РФ, можно утверждать, что произошел ряд существенных изменений в порядке изъятия электронных носителей и копировании информации.

Во-первых, если в прежней редакции законодатель определял порядок изъятия электронных носителей и копирования информации только для обыска (ч. 9.1 ст. 182 УПК РФ) и выемки (ст. ч. 3.1 183 УПК РФ), то теперь подобный порядок установлен для всех следственных действий.

Во-вторых, в ст. 164.1 запрещается изымать электронные носители информации при производстве следственных действий по уголовным делам о преступлениях в сфере предпринимательской деятельности за исключением случаев указанных в ч. 1 ст. 164.1. УПК РФ. Прежде законодателем не устанавливалось ограничений на изъятие электронных носителей.

В-третьих, если в прежней редакции законодатель устанавливал необходимость привлечения специалиста при изъятии электронного носителя и

---

[14] Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6. С. 5.

[15] Федеральный закон от 27.12.2018 № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2018. 29 декабря.

копировании информации (ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ), то в соответствии со ст. 164.1 УПК РФ следователь обязан привлекать специалиста только при изъятии электронного носителя информации. При этом следователь вправе произвести копирование информации с электронного носителя самостоятельно без изъятия носителя.

Названной поправкой законодатель стремится защитить субъектов предпринимательства от необоснованного изъятия электронных носителей информации, что может привести к приостановке хозяйственной деятельности. С позитивной стороны следует оценить установленное законодателем право следователя самостоятельно копировать информацию с электронных носителей, без их последующего изъятия. Однако законодатель, дополняя УПК РФ ст. 164.1, оставил без изменения проблемное положение, касающееся обязательного требования привлечения специалиста при изъятии электронного носителя информации.

Так, в правоприменительной деятельности привлечение специалиста для изъятия электронного носителя информации не всегда представляется возможным. К тому же возникает вопрос о целесообразности использования специальных знаний при изъятии электронных носителей, которые используются повсеместно (CD-RW, флеш-накопители и т. д.).

Важно отметить, что еще до внесения в УПК РФ рассматриваемой новеллы (ст. 164.1), судебная практика неоднозначно разрешала вопрос о необходимости привлечения специалиста для изъятия электронного носителя информации (в соответствии с ч. 9.1 ст. 182 УПК РФ и ч. 3.1 ст. 183 УПК РФ).

Так, в одном случае судом признан несостоятельным довод апелляционных жалоб о том, что в ходе выемки CD-RW диск был изъят у Н. с нарушением требований ч. 3.1 ст. 183 УПК РФ, так как изъятие происходило без специалиста. При этом суд, ссылаясь на нормы ч. 5 ст. 164 УПК РФ и ст. 168 УПК РФ, указал, что следователь только вправе привлечь к участию в следственном действии

специалиста, но не обязан[16]. Тем самым, указывая на соблюдение общего правила, суд, по сути, оставил без внимания надлежащее исполнение специального.

Еще одна позиция судебных органов получила отображение в признании правомерным производства изъятия электронных устройств без участия специалиста, так как не производилось копирование информации[17]. То есть в случае если изымаются «носители» целиком, то, по мнению суда, специальные знания не требуются.

Противопоставлением указанным примерам является апелляционное постановление, принятое 17 октября 2017 года Соликамским городским судом Пермского края. По жалобе защитника был признан в качестве недопустимого доказательства CD –диск, в связи с тем, что изъятие диска проходило без участия специалиста, что является нарушением требований ч. 3.1 ст. 183 УПК РФ[18].

Проанализировав судебную практику, Т.С. Крюкова приводит следующую статистику. Основным способом получения цифровой информации в ходе следственных действий является изъятие электронных носителей информации: такой способ составляет 96% случаев и только 4 % приходится на копирование цифровой информации. При этом только в 10% судебных решений отсутствие специалиста было признано существенным нарушением порядка следственных действий (обыска и выемки), связанных с изъятием электронных носителей, и повлекло за собой признание протоколов следственных действий недопустимыми доказательствами. В большинстве судебных решений вопрос о необходимости привлечения специалиста решается исходя из того, осуществлялось ли

---

[16] Апелляционное определение суда Ненецкого автономного округа по делу № 22-27/2015 от 13 апреля 2015 // URL: https://sudact.ru/regular/doc/UpBwjgpnx4Yx/ (дата обращения: 23.09.2019).

[17] Апелляционное постановление Приморского краевого суда № 22-5674/15 от 24 сентября 2015 // URL: https://sudact.ru/regular/doc/mcLt94ndnd0/ (дата обращения: 23.09.2019).

[18] Апелляционное постановление Соликамским городского суда № 10-83/2017 Пермского края от 17 октября 2017 // URL: https://sudact.ru/regular/doc/0xG9qjZhfxxQ/ (дата обращения: 24.12.2019).

копирование информации с изъятых электронных носителей[19].

Подобные примеры и статистические данные демонстрируют, отсутствие единого представления у судебных органов о надлежащем механизме привлечения специалиста к процедурам изъятия электронного носителя информации и копирования информации.

В соответствии с ч. 1 ст. 75 УПК РФ доказательства, полученные с нарушением требований УПК РФ, являются недопустимыми. Поэтому все используемые правоприменителем интерпретации возможного изъятия, предполагающие отсутствие специалиста в таких процедурах, по сути, являются неправомерно произвольным толкованием текста уголовно-процессуального законодательства.

Фактическую точку в споре относительно унификации правоприменения поставил Конституционный Суд РФ. При рассмотрении жалобы на нарушение конституционных прав на тайну переписки, телефонных переговоров и иных сообщений при изъятии электронных носителей информации в ходе производства обыска Конституционный суд РФ указал, что электронные носители информации изымаются с участием специалиста[20].

Несмотря на обозначенную позицию Конституционного суда РФ, требование по привлечению специалиста для изъятия электронных носителей информации не соответствует современному уровню технического развития. Следует учитывать, что современные информационные технологии настолько просты в обращении, что практически не требуют специальных умений и знаний по их применению. Очевидно, что правила по изъятию электронных носителей информации нуждаются в совершенствовании и адаптации к современным

---

[19] Крюкова Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Использование информационных технологий в уголовном судопроизводстве: проблемы теории и практики. – 2016. № 4. С. 62.

[20] Определение Конституционного Суда РФ от 26 января 2017 № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации» // URL: https://ukrfkod.ru/pract/ opredelenie- konstitutsionnogo-suda-rf-ot-26012017- n-29-o/ (дата обращения: 24.12.2019).

общественным отношениям, сложившимся под влиянием информационных технологий.

Таким образом, в правоприменительной практике собирания информации с электронных носителей существует ряд проблем. Современные информационные технологии, рассчитанные на массового потребителя, не требуют специальных познаний при их использовании. Отсюда возникает вопрос о целесообразности требования обязательного привлечения специалиста для изъятия электронных носителей информации в уголовном судопроизводстве.

Статья 164.1. УПК РФ устанавливает императивное правило на участие специалиста при изъятии электронных носителей информации, что является анахронизмом в регулировании отношений, так как современные информационные технологии в большинстве случаев настолько просты в обращении, что не требуют специальных знаний для их изъятия. Следует заметить, что на данную проблему неоднократно обращалось внимание в юридической литературе[21].

Как указывалось в исследовании, УПК РФ устанавливает императивные правила на участие специалиста при изъятии электронных носителей информации, что подтверждается позицией Конституционного суда РФ. Нарушение положений ст. 164.1. УПК РФ ведет к признанию изъятого электронного носителя информации в качестве недопустимого доказательства.

Рассмотренные примеры судебной практики и статистические данные демонстрируют, отсутствие единого представления у правоохранительных органов о надлежащем механизме привлечения специалиста к процедурам изъятия электронного носителя и копирования информации.

---

[21] Зуев С.В. Указ. соч. С. 35-36; Осипенко А.Н., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 4; Старичков М.В., Антонов В.А. Электронные носители как источники криминалистически значимой информации // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Вып. 3-4. Иркутск: ФГКОУ ВПО «ВСИ МВД России», 2013. С. 123-127; Сотников К.И. Тактика осмотра страниц интернет-сайтов // Вестник криминалистики. 2015. № 2 (54). С. 53; Васюков В.Ф., Семенова С.Е. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3. С. 205.

Сотрудники органов предварительного расследования сходятся во мнении, что требование об обязательном участии специалиста является излишним и требует изменения. В социологическом исследовании О.В. Овчинниковой: «95% опрошенных следователей отметили, что участие специалиста при изъятии электронных носителей информации нарушает принцип процессуальной экономии: 5% опрошенных согласились с целесообразностью участия специалиста при необходимости отсоединения носителей от сети, либо демонтажа устройства для изъятия его составных частей»[22].

Проведенное анкетирование следователей, проходящих повышение квалификации в Дальневосточном юридическом институте Министерства внутренних дел РФ и Пятом факультете повышения квалификации Московской академии Следственного комитета РФ (с дислокацией в городе Хабаровске) в период с марта по сентябрь 2018 года, показало, что 74,6 % опрошенных высказались за исключение из УПК РФ положения об обязательном участии специалиста при изъятии электронного носителя информации. При этом 14,4 % решили оставить данное положение без изменений.

На основании вышеизложенного необходимо исключить из ст. 164.1. УПК РФ требование об обязательном участии специалиста при изъятии электронного носителя и копировании с него информации. Предоставить следователю право привлекать специалиста, когда для работы с техникой действительно требуются специальные познания. Представляется, что участие понятых в следственных действиях широко раскрыты в ст. 170 УПК РФ и в дополнительной регламентации в ст. 164.1. УПК РФ не нуждается, так как изъятие электронных носителей и копирование информации производится в рамках существующих следственных действий[23].

В 2016 году Федеральным законом № 375-ФЗ[24] от 06.07.2016 в статью 185

---

[22] Овчинникова О.В. Собирание электронных доказательств размещенных в сети интернет // Правопорядок: история, теория и практика. 2016. № 4. С. 69.

[23] Предложение по редакции ст. 164.1 УПК РФ см. Приложение № 3.

[24] Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в

УПК РФ, регламентирующую производство следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», вводится часть 7, которая предусматривает возможность производить выемку и осмотр электронных и иных сообщений, передающихся по сетям электросвязи.

Значимые изенения в УПК РФ произошли в 2021. Законодатель добавил возмнозность производить допрос, очную ставку, опознание путем использования видео-конференц-связи (ст. 189.1 УПК РФ)[25].

На данном этапе развития информационных технологий в уголовном процессе начали появляться научные разработки. Так, отдельные вопросы, связанные с использованием информационных технологий в уголовном судопроизводстве, стали рассматриваться в криминалистике с 1990-х годов. Одной из работ является кандидатская диссертация В.Б. Вехова «Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники» (Волгоград, 1995)[26]. В данном исследовании автор рассматривает понятие «машинная информация» как особый объект, представляющий интерес для науки уголовного процесса.

Научные труды, посвященные проблемам использования информационных технологий в уголовном судопроизводстве, появились в 2010 году. В качестве примеров можно привести диссертационные исследования Н.А. Зигуры «Компьютерная информация как вид доказательств в уголовном процессе» (Челябинск, 2010)[27], В.Ю. Стельмах «Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное

части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 11 июля.

[25] Федеральный закон от 30.12.2021 № 501-ФЗ «О Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2022. 11 января.

[26] Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дисс. … канд. юрид. наук. Волгоград, 1995. С. 276.

[27] Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … кан. юрид. наук. Челябинск, 2010.

действие» (Екатеринбург, 2013)[28], П.С. Пастухова «Модернизация уголовно-процессуального доказывания в условиях информационного общества» (Москва, 2015)[29].

На данном этапе признается, что цифровизация в уголовном судопроизводстве неизбежна, и задача состоит в том, чтобы наиболее оптимальным образом урегулировать использование IT-технологий, «внедрить» их в традиционные процедуры, свойственные производству по уголовным делам[30].

Применительно к исследуемому вопросу С.В. Зуев, О.А. Зайцев, О.И. Андреева и другие ученные отмечают, что основные научные исследования по внедрению информационных технологий в уголовное судопроизводство ведутся по ряду направлений[31], среди которых главенствующую роль занимает «разработка теоретических основ и научного обоснования системы информационного обеспечение уголовного процесса», включая такие подразделы, как:

– переход на фиксацию хода процессуальных, в том числе следственных действий с помощью технических средств и сохранение результатов в электронном виде;

– внедрение в уголовно-процессуальную материю удобной и надежной технологии удостоверения процессуального документа любым участником уголовного процесса вместо его обычной подписи;

---

[28] Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: дисс. … кан. юрид. наук. Екатеринбург, 2013.

[29] Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дисс. … д-ра юрид. наук. М., 2015.

[30] Подробнее см.: Химичева О.В., Андреев А.В. Цифровизация как тренд развития современного уголовного процесса // Вестник Московского университета МВД России. 2020. № 3. С. 21-23.

[31] Зуев С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118-120; Андреева О.И., Зайцев О.А. Правовое регулирование уголовно-процессуальных отношений в цифровую эпоху // Вестник Томского государственного университета. 2020. № 455. С. 190-198.; Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция // Вестник экономической безопасности: юридические науки. 2019. № 1. С. 15-25.

– разработка пилотного проекта «Электронное уголовное дело» и апробация его в отдельных субъектах Российской Федерации;

– широкое применение дистанционных форм проведения процессуальных действий на любой стадии уголовного судопроизводства, включая участие в судебных заседаниях всех заинтересованных лиц;

– предоставление потерпевшему в режиме онлайн через Интернет возможности отслеживать движение уголовного дела с момента подачи заявления в электронном форме до вынесения приговора.

Безусловно, перечисленные направления являются примерными, и их перечень может быть дополнен и скорректирован.

Следующим этапом интеграции информационных технологий в уголовное судопроизводство является *широкое использование информационных технологий, переход от фрагментарного использования электронной информации к полноформатному электронному производству по уголовным делам*. Представляется, что именно на данном этапе развития находится российское уголовное судопроизводство.

В качестве аргумента в пользу обозначенной позиции можно привести ряд решений высших судебных инстанций по актуальным вопросам собирания электронной информации. Например, Определение Конституционного Суда РФ от 26.01.2017 № 204-О[32], в котором рассматриваются практические вопросы изъятия электронных носителей и копирования с них информации; Определение Конституционного суда РФ от 25 января 2018 г. № 189-О[33], посвященнного соблюдению права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при производстве следственных действий в

[32] Определение Конституционного Суда РФ от 26 января 2017 № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации» // URL: https://ukrfkod.ru/pract/opredelenie- konstitutsionnogo-suda-rf-ot- 26012017-n-29-o/ (дата обращения: 22.11.2020).

[33] Определение Конституционного суда РФ от 25 января 2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно- процессуального кодекса Российской Федерации // URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-25012018-n-189-o/ (дата обращения: 22.11.2020).

отношении электронных носителей информации; постановление Пленума Верховного Суда РФ от 30.06.2015 № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве»[34]. В последнем документе разъясняется, что обвиняемый, находящийся под стражей или в местах лишения свободы, вправе лично участвовать в судебном заседании с использованием системы видеоконференц-связи, а также иные судебные решения.

В перспективе, по прогнозам современной инженерной науки, человечество переступит порог девятой информационной революции и последующим этапом развития уголовного судопроизводства станет *появление и использование в уголовном процессе информации с учетом иных способов ее передачи, обработки и представления.* Электронная информация перестанет быть всеобъемлемым неисчерпаемым ресурсом, на смену его придут более продвинутые технологии.

Так, 16 июля 2019 года Илон Маск презентовал технологию «Neuralink», позволяющую подключить мозг живого организма к компьютеру. В ходе проведенных экспериментов обезьяна смогла управлять компьютером, не прикасаясь к его органам управления (силой мысли). Илон Маск рассчитывает в ближайшее время получить разрешение на производство экспериментов с человеком и начать внедрение технологии[35].

В настоящее время наука и практика уголовного процесса находится на этапе активного использования электронной информации в доказывании по уголовным делам, в том числе в ходе досудебного производства. Данный этап с учетом его специфики требует более пристального внимания в исследовании вопросов влияния развития информационных технологий на доказывание в досудебных стадиях уголовного процесса.

---

[34] Постановление Пленума Верховного Суда РФ от 30 июня 2015 № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» // URL: https://www.vsrf.ru/documents/own/8439/ (дата обращения: 01.12.2020).

[35] Neuralink нейроинтерфейс для чтения мыслей и управления компьютерами // URL: https://www.popmech.ru/science/493952-neuralink-neyrointerfeys-dlya-chteniya-mysley-i-upravleniya -kompyuterami/#part0 (дата обращения: 10.08.2019).

Таким образом, первый этап интеграции информационных технологий в уголовное судопроизводство представляет собой процесс внедрения информационных технологий в уголовный процесс и утверждение данного направления науки уголовного процесса как приоритетного. Данный этап сопровождается нормативным закреплением информационных технологий и смежных категорий в УПК РФ, другие нормативные правовые акты, а также появлением первых научных трудов в названной сфере.

Следующим этапом интеграции информационных технологий в уголовное судопроизводство является широкое использование информационных технологий, переход от фрагментарного использования электронной информации к полноформатному электронному производству по уголовным делам. Представляется, что именно на данном этапе развития находится российское уголовное судопроизводство.

В перспективе, по прогнозам современной инженерной науки, человечество переступит порог девятой информационной революции и последующим этапом развития уголовного судопроизводства станет появление и использование в уголовном процессе информации с учетом иных способов ее передачи, обработки и представления. Электронная информация перестанет быть все объемлемым неисчерпаемым ресурсом, на смену его придут более продвинутые технологии.

1.2. Электронные средства уголовно-процессуального доказывания: понятие, виды, природа электронной информации

Само по себе понятие «электронные средства» наиболее характерно для технических наук, где оно чаще применяется относительно связи. В технической литературе под «электронными средствами связи» понимается техника передачи информации из одного места в другое в виде электрических сигналов,

посылаемых по проводам, кабелю, оптоволоконным линиям или вообще без направляющих линий[36].

Согласно положениям Типового закона ЮНСИТРАЛ «Об электронной торговле», электронные средства включают в себя электронный обмен данными, электронную почту, телеграф, телекс, телефакс и другие электронные средства, предназначенные для подготовки, отправки, получения и хранения сообщений данных[37].

В Федеральном законе от 07.07.2003 №126-ФЗ «О связи» не содержится определения термина «электронные средства связи», но присутствуют определения двух взаимозависимых терминов «средства связи» и «электросвязь»:

– средства связи – технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи, включая технические системы и устройства с измерительными функциями;

– электросвязь – любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Проведенное исследование российских нормативных правовых актов позволяет прийти к выводу об отсутствии единого законодательного определения терминов «электронные средства», «электронные средства связи» или «средства электронной связи».

Электронные средства, используемые в доказывании на досудебных стадиях уголовного процесса, – это совокупность уголовно-процессуальных и аппаратно-программных инструментов направленных на собирание, проверку и

---

[36] Энциклопедия «Кругосвет» // URL: http://www. krugosvet.ru (дата обращения: 12.02.2021).

[37] Типовой закон об электронной торговле // URL: https://www.uncitral.org/pdf/ russian/texts/electcom/ 05-89452_Ebook.pdf (дата обращения: 13.02.2021).

оценку доказательств, выраженных в электронном виде, а также обеспечивающих производство следственных действий.

В целях дальнейшего развития информационного законодательства, представляется возможным закрепить указанное определение в соответствующих нормативных правовых актах.

Полагаем, что основными видами электронных средств, используемых в доказывании по уголовным делам, будут: электронная информация, электронные носители информации; дистанционные формы коммуникации и способы обращения (подача заявлений, жалоб, ходатайств) посредством электронной связи; сайты, облачные пространства сети «Интернет», программное обеспечение персональных компьютеров, которые предопределяют способы собирания, проверки и оценки доказательств в ходе расследования преступлений.

Одним из элементом средств уголовно-процессуального доказывания являются следствввенные дейсвтия, направленные на получения электронной ниформации, а также формы производства следственных действий с использованием технических средств, специально определенных в УПК РФ. В качестве примера допустимо привести ст. 164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий» и положения ст. 189.1 УПК РФ «Особенности проведения допроса, очной ставки, опознания путем использования системы видео-конференц-связи.

Электронная информация имеет уголовно-процессуальное законодательное закрепление, и ее по праву можно считать основным элементом электронных средств уголовно-процессуального доказывания. Данный феномен требует более тщательного изучения.

В научной юридической литературе можно обнаружить различные точки зрения относительно понятия: «машинная информация»[38], «компьютерная

[38] Карась И.З. Экономический и правовой режим информационных ресурсов // Право и информатика. М.: Изд-во Моск. ун-та, 1990 С. 40.

информация»[39], «электронные доказательства»[40], «электронная информация»[41], «цифровая информация»[42], «цифровой объект»[43].

Продолжительное время понятие «машинная информация» характеризовалось учеными через категорию электронно-вычислительной машины. Еще в начале 90-х гг. И.З. Карась предложил под машинной информацией понимать информацию, циркулирующую в вычислительной среде, зафиксированную на физическом носителе в форме, доступной восприятию ЭВМ, или передающуюся по телекоммуникационным каналам. К последней он относил сформированную в вычислительной среде информацию, пересылаемую из одной ЭВМ в другую, из ЭВМ на устройство отображения или из ЭВМ на управляющий датчик оборудования[44]. В свою очередь, Ю.Н. Батурин рассматривал машинную информацию как информацию, зафиксированную в форме доступной для обработки на ЭВМ[45].

Через некоторое время В.В. Вехов предложил понимать под «машинной информацией» сведения, «циркулирующие в вычислительной среде, зафиксированные на физическом носителе в форме, доступной восприятию ЭВМ, или передающиеся по телекоммуникационным каналам: сформированная вычислительной среде информация, пересылаемая посредством

---

[39] См.: Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … кан. юрид. наук. Челябинск, 2010; Григорьев О.Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дисс. … кан. юрид. наук. Тюмень, 2003.

[40] См.: Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук. М., 2016.

[41] См.: Сергеев М.С. Правовые основы применения электронной информации и электронных носителей информации в уголовном судопроизводстве: дисс. … кан. юрид. наук. Казань, 2018.

[42] См.: Зазулин А.И. Правовые и методологические основы использования использования цифровой информации в доказывании по уголовному делу: дисс. … кан. юрид. наук. Екатеринбург, 2018.

[43] См.: Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дисс. ... канд. юрид. наук. Воронеж, 2010.

[44] Карась И.З Указ. соч. С. 40.

[45] Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 67.

электромагнитных сигналов из одной ЭВМ в другую, их ЭВМ на периферийное устройство либо на управляющий датчик оборудования»[46].

Следует признать, что термин «машинная информация» не получил широкого распространения, так как в нормативно-правовых актах[47] и в повседневном речевом использовании его заменил термин «компьютер».

Позднее в докторском диссертационном исследовании В.В. Вехов, проведя детальный анализ позиций ученых, предлагающих дефиницию «компьютерная информация», выдвинул свое авторское определение, понимая под ней «сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов»[48].

Более развернутое понятие «компьютерной информации» в своем труде приводит Н.А. Зигура, определяя ее, как «сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые посредством использования аппаратных и программных средств фиксации, обработки и передачи информации, а также набор команд (программ), предназначенных для использования в ЭВМ и управления ею, на основе которых суд, следователь, дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела, полученные с соблюдением процессуального порядка их собирания и приобщенные к уголовному делу специальным постановлением»[49].

Анализируя приведенные научные понятия, можно сделать вывод, что авторы для отражения сущности термина «компьютерная информация»

---

[46] Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дисс. … канд. юрид. наук. Волгоград, 1995. С. 32.

[47] В 1996 году в принятом Уголовном кодексе Российской Федерации глава 28 получила название «Преступления в сфере компьютерной информации». В примечании к ст. 272 УК РФ дается понятие компьютерной информации.

[48] Вехов, В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дисс. … докт. юрид. наук. Волгоград, 2008. С. 83.

[49] Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … кан. юрид. наук. Челябинск, 2010. С. 187.

используют технические особенности рассматриваемой категории. Несмотря на то, что определение Н.А. Зигуры сконструировано через уголовно-процессуальные отношения, дефиниция, предлагаемая В.Б. Веховым, является, на наш взгляд, более точной, так как в объем понятия включается аналоговая электронная информация, а не только цифровая.

Необходимо дать дополнительное разъяснение относительно аналоговой и цифровой информации. Как отмечает А.Л. Осипенко: «Практически любые данные могут быть переведены в компьютерную форму, которая в настоящий момент ассоциируется с цифровой формой представления данных. Интенсивный процесс «оцифровки данных» наблюдается во всех сферах человеческой деятельности, и, по некоторым оценкам, сегодня не оцифровано лишь чуть более 2 % доступной информации»[50].

Действительно, большинство существующих в настоящий момент электронных устройств являются цифровыми, однако аналоговые электронные устройства[51] продолжают использоваться в повседневной жизни.

Примером аналоговых электронных устройств могут служить различные телефоны, работа которых основана на аналоговых линиях связи[52], когда электромагнитный сигнал не проходит «оцифровку» при передаче по линиям связи между абонентами[53]. Аналоговые линии телефонной связи обширно используются на территории России[54]. В качестве дополнительных примеров аналоговой электроники можно привести: радиосвязь, в том числе и обычное радио, аналоговое телевидение, которое распространено на территории Дальнего

---

[50] Осипенко А.Л. Указ. соч. С. 85

[51] Аналоговые электронные устройства – предназначены для приема, преобразования, передачи электрического сигнала, изменяющегося по закону непрерывной (аналоговой) функции. Цит.по: Опадчий Ю.Ф., Глудкин О.П., Гуров А.И. Аналоговая и цифровая электроника. М.: Горячая Линия-Телеком, 2005. С. 10.

[52] Основано на работе аналоговой автоматической телефонной станции.

[53] Подробнее см.: Стив, Ш. Основные типы абонентских телефонных линий и услуг / Ш. Стив // URL: https://www.osp.ru/lan/1996/02/131926 (дата обращения: 22.09.2020).

[54] Политическая дороговизна IP-телефонии // URL: https://www.osp.ru/lan/1996/02/131926 (дата обращения: 22.09.2020).

Востока[55].

Разграничивая аналоговую информацию от дискретной, необходимо проанализировать процесс передачи информации с точки зрения информатики.

Информация, то есть смысл, который должен понять получатель с помощью сообщений (символов, образов, звуков), передается посредством сигнала. Понятие сигнала происходит от латинского signum – знак[56]. Сигнал - это физический процесс или явление, несущее сообщение о каком-либо событии. По своей природе и типу передающей среды сигналы делятся на механические, тепловые, световые, электрические, электромагнитные, звуковые.

Рассмотрим механизм передачи информации. Так, если водитель автомобиля видит знак ограничения максимальной скорости, то сообщение для него представляет символ – цифра 60 в красной окружности, сигналом в данном случае будет являться свет, отраженный от знака дорожного движения и попадающий в глаза водителя автомобиля, информацией же является понимание, что на данном участке дороге максимальная скорость ограничена 60 км/ч.

Характер сигнала и особенности сообщения, передаваемого им, позволяют выделять различные виды и информации[57].

Как верно указывает А.И. Зазулин, сигналы по своей структуре могут быть дискретными или аналоговыми (непрерывными). Аналоговый сигнал представляет собой величину, непрерывно изменяющуюся во времени, амплитуду, частоту, фазу. В качестве примера можно привести человеческую речь (механическую волну), изображение на фотографии (отраженная от поверхности электромагнитная волна). Дискретными являются те, которые состоят из отдельных различимых символов – букв или цифр. Существует

---

[55] Полный охват цифровым телевидением территории Дальнего Востока обойдется в 7 миллиардов рублей // URL: https://www.dvnovosti.ru/khab/2018/02/27/79502/ (дата обращения: 22.03.2020).

[56] Подосинов А.В. Латинско-русский и русско-латинский словарь. М.: ФЛИНТА, 2014. С. 114.

[57] Зуев С.В. Балашов А.Н., Бахтеев Д.В., Брановицкий К.Л., Вехов В.Б., Григорьев В.Н., Долганичев В.В.,. Зазулин А.И, Зайцев О.А., Максимов О.А., Медведева М.О., Овсянников Д.В., Овчинникова О.В., Пастухов П.С., Тушканова О.В. Основы теории электронных доказательств: монография. М.: Юрлитинформ, 2019. С. 25.

особый тип дискретной информации, который не может быть непосредственно воспринят человеком и закреплен в протоколе. Речь идет об отдельной разновидности дискретного сигнала – цифровой, выраженным в кодировке двоичных чисел (0 и 1). Последовательностью нуля и единицы можно выразить текст, изображение, звук[58].

Чтобы человек мог воспринимать значение цифровой информации, её необходимо преобразовать в понятную для человека аналоговую форму (аналоговый сигнал). Для этого цифровой код при помощи программно-аппаратных средств (цифро-аналоговый преобразователь) преобразуется в аналоговый сигнал (механическая волна, исходящая от колонок, свет, исходящий от экрана компьютера и т. д.). Процесс может идти и в обратном направлении, когда аналоговая информация попадает в устройство, к примеру, видимый свет (электромагнитная волна) попадает в камеру видеонаблюдения, после чего преобразуется в виде кода («1» и «0»), а затем сохраняется на физическом уровне, например, на оптический диск.

По мнению А.И. Зазулина: «Цифровая информация не существует в природе, это изобретение человеческого разума. Между тем большая часть первичной информации в окружающем мире представлена в форме аналоговых сигналов, да и сам человек, будучи творением природы, может непосредственно воспринимать только аналоговые сигналы»[59].

Однако, как указано выше, существуют электронные устройства, которые не преобразуют аналоговый сигнал в цифровой. При этом действие как аналоговых, так и цифровых электронных устройств основано на электромагнитных физических свойствах[60]. Не исключены случаи, когда

---

[58] Зазулин А.И. Правовые и методологические основы использования использования цифровой информации в доказывании по уголовному делу: дисс. … кан. юрид. наук. Екатеринбург, 2018. С. 78-79.

[59] Зуев С.В., Балакшин В.С., Вехов В.Б., Григорьев В.Н., Зазулин А.И., Зайцев О.А., Медведева М.О., Никинит Е.В., Овчинникова О.В., Пастухов П.С., Родиыилина В.А., Смолькова И.В., Стельмах В.Ю., Шаевич А.А. Развитие информационных технологий в уголовном судопроизводстве: монография. М.: Юрлитинформ, 2018. С. 68.

[60] Опадчий Ю.Ф., Глудкин О.П., Гуров А.И. Аналоговая и цифровая электроника М.: Горячая Линия-Телеком, 2005. С. 10-13.

объектом следственного действия будет выступать аналоговый электронный сигнал. Исходя из изложенного, содержание понятия «компьютерная информация» должно охватывать как аналоговую, так и цифровую информацию. Поэтому, на наш взгляд, понятие «компьютерной информации», предложенное В.Б. Веховым является более точным и перспективным с учетом дальнейшего вектора развития информационных технологий.

Несмотря на то, что в настоящий момент определение понятия «компьютерная информация» закреплено в примечании к ст. 272 УК РФ, ряд авторов предлагает использовать иную терминологию. Так, В.Ю. Агибалов со сведениями, выраженными в электронной форме, отождествляет цифровой объект – «зафиксированную на материальном носителе компьютерную информацию, представленную в виде системы дискретных информационных блоков, обеспечивающую их хранение и использование по целевому назначению»[61].

Данная дефиниция по своей смысловой значимости отражает технический процесс отображения цифровой информации аналогично с определением, предлагаемым Н.А. Зигурой, и не учитывает существование аналоговой электронной информации, что не отвечает потребностям уголовно-процессуального законодательства.

Понятие «электронная информация» предлагает использовать М.А. Ефремова, понимая под данной категорией «сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи»[62].

Относительно приведенного термина «электронная информация» следует привести замечание В.М. Быкова и В.Н. Черкасова. Авторы утверждают, что «компьютерная информация является одним из видов электронной информации». Полагаем, что все как раз наоборот. Это электронная информация представляет

---

[61] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М.: Юрлитинформ, 2012. С. 89.

[62] Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. № 7. С. 52.

собой частный случай компьютерной информации»[63].

Соглашаясь с замечанием В.М. Быкова и В.Н. Черкасова, отметим, что в сфере информационных технологий под компьютерами понимаются электронно-вычислительные машины (ЭВМ) и аналоговые вычислительные машины (АВМ). АВМ оперируют информацией только в форме аналоговых сигналов, не перекодируя их в цифровые[64]. Примерами аналоговых компьютеров являются различные пневматические устройства, использующиеся для обработки информации в нефтедобывающей промышленности и металлургии, где передача электрических сигналов может привести к взрывам и авариям[65]. Первые компьютеры были полностью механическими. В их работе не использовались электромагнитные физические свойства.

В тех случаях, когда сообщение, продуцируемое АВМ, станет понятным человеку без использования электронных аппаратно-программных средств, отнесение такой информации к электронной будет ошибкой. В связи с отсутствием такого важного свойства электронной информации, как посредничество электронных аппаратно-программных средств между физическим и семантическим уровнем существования электронной информации, данный вид сведений не будет обладать специальными свойствами, и может рассматриваться как вещественное доказательство (обычный предмет).

При этом если информация, являющаяся результатом работы АВМ, будет переведена в понятную для человека форму с помощью электронных аппаратно-программных средств, то такую информацию допустимо отнести к электронной. В качестве примера можно привести QR-код, который также является электронной информацией, так как расшифровка сообщения и информации, которую он несет, возможна с помощью ЭВМ.

Понятие «цифровая информация» предлагает использовать А.И. Зазулин. По мнению ученого, обязательным признаком названного определения является

---

[63] Быков В.М., Черкасов В.Н. Понятие компьютерной информации как объекта преступлений // Законность. 2013. № 12. С. 38.

[64] Зазулин А.И. Указ. соч. С. 83.

[65] Юнг У. Аналоговая электроника. Бостон, Оксфорд, 2002. С. 220.

кодировка в двоичной системе счисления[66]. Действительно, двоичная система кодировки является самой распространенной, но не единственной[67]. Не исключены варианты того, что в ближайшее время появятся новые более эффективные системы кодирования[68].

Таким образом, в уголовно-процессуальной науке существует множество точек зрений относительно сведений, образующихся с помощью электронных информационных технологий. Рассматривая вопрос, какое из названных определений является наиболее подходящим для использования в уголовном процессе, необходимо учитывать, что в законодательстве закреплено понятие компьютерная информация.

В примечаниях к ст. 272 УК РФ указано, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Любопытно, что в отзыве Верховного Суда РФ 07.04.2011 № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» отмечено, что предложенный термин «электрические сигналы» не вносит достаточной ясности в определение понятия и требует дополнительного пояснения[69].

Критически характеризует понятие электронного сигнала в своих трудах М.А. Ефремова, указывая, что «согласно теории информации и связи, разработанной Клодом Шенноном, сигнал – это материальный носитель

---

[66] Зазулин А.И. Указ. соч. С. 95-96.

[67] В ЭВМ кроме двоичной системы счисления (кодировки) используется восьмеричная, десятеричная и шестнадцатеричная. Подробнее см.: Бурдинский И.Н. Системы счисления и арифметика ЭВМ. Хабаровск: Изд-во Тихоокеан. гос. ун-та. 2008. С. 9-11.

[68] В настоящий момент идут разработки новой системы кодировки информации, основанной на «кубитах». При этом «кубит» имеет совершенно иную природу счисления, основанную на квантовой механике. Подробнее См.: Ключко В.И. Квантовые технологии как основа квантового компьютера. // Научные труды КубГТУ. 2017. № 3. С. 136-140.

[69] Официальный отзыв Верховного Суда РФ от 07 апреля 2011 № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» // URL: http://base.consultant.ru/cons/cgi/online.cgi? req=doc; base=PRJ;n= 87058 (дата обращения: 12.12.2020).

информации, используемый для передачи сообщений в системе связи… По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, оптическими и т.д.…. Теперь законодатель не привязывает компьютерную информацию лишь к машинному носителю, электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Таким образом, под защиту уголовного закона попала и та информация, которая еще не зафиксирована на каком-либо носителе или устройстве, а находится в процессе передачи. Это должно расширить сферу применения данной статьи. Однако информация, передаваемая по беспроводным и оптическим каналам связи, не будет являться объектом уголовно-правовой охраны, т.к. не подпадает под определение электрических сигналов при трактовке этого термина с точки зрения физики. В связи с этим использование такого термина, как «электрический сигнал», лишь вводит в заблуждение и поэтому нуждается в дальнейшем разъяснении или замене более подходящим термином»[70].

Мнение М.А. Ефремовой о том, что сведения, передаваемые беспроводными и оптическими каналами связи, не попадают под определение электрических сигналов, является спорным, так как свет и есть электромагнитная волна. На электромагнитных свойствах материи построены и другие беспроводные способы передачи электронной информации. Это подтверждается теорией электрической связи в информатике, где под «сигналом понимается физический процесс (электрический ток или радиоволны), способный распространяться в пространстве и нести в себе информацию»[71].

Следует признать, что категория «электрический сигнал» порождает неточность, так как в данном случае не очевидно, охватывается ли ею многовариантные формы физического уровня существования компьютерной информации. Несмотря на указанные недостатки, действующая редакция дефиниции «компьютерная информация» отвечает потребностям

---

[70] Ефремова М.А. Указ. соч. С. 51.

[71] См.: Романов Б.Н., Краснов С.В. Теория электрической связи. Сообщения, сигналы, помехи, их математические модели: учеб. Пособие. Ульяновск: Ульяновский гос. технический ун-т, 2008. С. 7.

информационных общественных отношений и уголовно-процессуального права, так как охватывает не только цифровые данные, но и аналоговые.

Так, в предыдущей редакции ч. 1 ст. 272 УК РФ компьютерная информация определялась как информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Скорее всего, данное определение отождествляло компьютерную информацию только с цифровой формой. Можно предположить, что законодатель изменил дефиницию компьютерной информации для увеличения многообразия вариаций электронных сведений, попадающих в объем понятия.

Законодатель использует категорию «компьютерная информация» в иных нормативных правовых актах. Так, в закон «Об оперативно-розыскной деятельности»[72] п. 15 было введено новое оперативно-розыскное мероприятие (далее ОРМ) «получение компьютерной информации». Исходя из этого, законодатель констатирует, что новым самостоятельным объектом ОРМ является «компьютерная информация». Указанная поправка косвенно отражается и на уголовно-процессуальных отношениях. Так, в соответствии с ст. 89 УПК РФ, результаты оперативно-розыскной деятельности могут быть использованы в качестве доказательств, если они соответствуют требованиям УПК РФ. При этом УПК РФ еще не содержит в качестве самостоятельного объекта правового регулирования категорию «компьютерная информация».

Несмотря на изложенное, полагаем что, использование категории «электронная информация» является более точным с точки зрения лексического значения. Так, под компьютером понимается электронная вычислительная машина[73], что фактически привязывает электронные сведения к цифровым данным. При этом понятие «электронная информация» вбирает все многообразие сведений, существующих на основе электромагнитных свойств материи.

---

[72] Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 12.07.2021) // Гарант: справ. правовая система // URL: https://base.garant.ru/10104229/ (дата обращения: 20.06.2021 г.).

[73] Толковый словарь русского языка В.В. Лопатин. // URL: http://www.вокабула.рф (дата обращения: 20.01.2021 г.).

Таким образом, предлагается как в уголовно-процессуальном законодательстве, так и в одноименной науке использовать категорию «электронная информация», под которой следует понимать сведения, передача, обработка, воспроизведение которых осуществляется посредством электронных аппаратно-программных средств.

Рассмотрев понятие электронной информации, необходимо раскрыть особенности её отражения в создании человека. Данное свойство имеет определенную специфику, так как может оказать влияние на такое свойство уголовно-процессуальных доказательств как достоверность.

Чтобы понять особенности отражения электронной информации, обратимся к труду ученого-криминалиста Н.Н. Федотова, который на основе большого практического опыта работы по борьбе с киберпреступлениями, обосновывает возникновение нового раздела в криминалистической технике – «форензики» (компьютерной криминалистики), посвященного «исследованию доказательств в виде компьютерной информации, правилах, сбора, закрепления, представления таких доказательств, применительно к российскому законодательству»[74].

Рассуждая о методах познания, которые используются в компьютерной криминалистике, Н.Н. Федотов приходит к немаловажному выводу: «Дело в том, что основным объектом исследования (форензики) является компьютерная информация, которая в принципе не может наблюдаться человеком непосредственно…Непосредственные органы чувств человека – зрение, слух, осязание, не в состоянии воспринимать компьютерную информацию»[75]. Далее автор указывает, что подобное обстоятельство не уникально только лишь для «компьютерной информации». Человек, использует различные приборы (микроскопы, эхолокаторы, вольтметры и т. д.) для исследования объектов, которые не могут восприниматься органами чувств человека непосредственно. При помощи таких инструментов-посредников человек способен наблюдать и изучать то, что не наблюдается невооруженным глазом.

---

[74] Федотов Н.Н. Форнзика – компьютерная криминалистика. М.: Юридический мир, 2007. С. 2, 11.

[75] Там же С. 16.

В своем труде Н.Н. Федотов, приходит к важному умозаключению: «При изучении компьютерной информации количество и сложность таких посредников настолько велики, что количество это переходит в качество. Мы не всегда знаем всех посредников, стоящих между информацией на компьютерном носителе и нашими глазами. Мы с большим трудом может представить, какие именно преобразования претерпела информация по пути от своей исходной формы до наших глаз»[76].

Далее автор обосновывает свое утверждение примером, противопоставляя отражение электронной информации отражению материальных следов преступления, обнаружение и фиксация которых может происходить не только с помощью органов чувств человека непосредственно, но и с помощью специальных технических средств.

Так, Н.Н. Федотов предлагает: «Представим себе, что на месте преступления обнаружен след – отпечаток обуви. Он воспринимается органами чувств человека непосредственно. Если для восприятия и требуются какие-то технические средства, то лишь самые простые (например, фонарик или очки), принцип действия которых ясен любому и легко представим. А чаще технических средств и вовсе не требуется. Следователь и понятые видят своими глазами отпечаток обуви, прекрасно понимают механизм его возникновения. Не испытывая сомнений, они фиксируют этот след в протоколе, а после готовы показать под присягой, что видели именно отпечаток обуви. И у судьи не появится сомнений, что они могли видеть не то, что было на самом деле. Совсем по-другому с компьютерной информацией»[77].

Далее Н.Н. Федотов рассуждает: «Представим, что на месте происшествия на жестком диске сервера в лог-файле[78] обнаружена запись. Чтобы увидеть эту запись потребуется посредничество следующих технических средств: механизм жесткого диска, контролер жесткого диска с внутренней микропрограммой

---

[76] Там же С. 16

[77] Федотов, Н.Н. Указ. соч. С. 16-17.

[78] Лог-файл – это файл или база данных с записями о событиях, относящихся к определенной информационной системе или программе / Федотов Н.Н. Указ. соч. С. 350.

(firmware), внешний ATA-контроллер, программное обеспечение BIOS, операционная система, файловая система (драйвер)…Вот сколько посредников стоят между компьютерной информацией и глазами «очевидца»! Все они изготовлены разными производителями. Не для всех из них имеются одинаковые технические стандарты… И ни в одном из этих средств нельзя быть полностью уверенным – все знают об ошибках в программном обеспечении, о возможности вирусов и программных закладок. Могут ли понятые уверенно утверждать, что именно они видели? Даже не рассматривая возможности намеренных закладок в программ»[79].

Анализируя указанные примеры в диалектическом единстве, необходимо понимать, что для познания сущности процесса отражения сведений, выраженных в электронной форме, недостаточно классических подходов в рассмотрении механизма отражения материальных следов, основанного на принципе взаимодействия следообразующего и следовоспринимающего объектов.

Если классическое отражение основано на физических детерминантах, то отражение сведений, выраженных в электронной форме, которые способны воспринимать органы чувств человека, обусловлено функционированием множеством аппаратно-программных элементов, то есть искусственной технической средой, полностью управляемой человеком.

Как верно отмечает В.Ю. Агибалов: «Принципиальным отличием электронно-цифрового отображения является то, что на материальном носителе фиксируется не отражение самого взаимодействующего объекта или процесса с присущими ему проявлениями и свойствами, а лишь его цифровой образ, сформированный с использованием какой-либо формализованной (как правило, упрощенной и оптимизированной в заданном направлении) модели реального объекта или процесса. Фактически следа в традиционном криминалистическом его понимании нет, имеется только цифровой образ (цифровое значение

[79] Федотов Н.Н. Указ. соч. С. 18.

параметров математической модели, описывающей реальный объект), на основании которого (при определенных условиях) можно сформировать сигнал или некий физический процесс (звук, изображение, набор компьютерных данных), подобный (с определенной степенью схожести) исходному следообразующему объекту»[80].

Чтобы понять вышеизложенное умозаключение и детально раскрыть сущность отражения электронной информации, обратимся к труду Д.В. Пашнева, разработавшему теоретическую систему, наглядно демонстрирующую механизм преобразования электронной информации в понятный для человека вид. Автор предлагает рассматривать электронную информацию на трех уровнях: физическом, логическом, семантическом. Рассмотрим более подробно, что представляет каждый из уровней[81].

1. Физический уровень – уровень машинных носителей, где информация представлена в виде конкретных характеристик вещества (намагниченность домена – для магнитных носителей, угол и дальность плоскости отражения лазерного луча – для оптических дисков) или магнитного поля (амплитуда, фаза, частота). Этот уровень предназначен для «понимания» содержания данных и их обработки техническими средствами компьютерной техники.

Исходя из характеристики физического уровня, можно сделать вывод, что электронная информация всегда привязана к материальному носителю, к примеру, намагниченная поверхность жесткого диска, структурное изменение поверхности оптического диска (CD-диск), электромагнитной волне, за счет её характеристик (частота, амплитуда). Изложенный аргумент подтверждается умозаключением В.А. Мещерякова: «Все виды виртуальных следов в конечном счете сохраняются на материальных носителях»[82].

---

[80] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М.: Юрлитинформ, 2012. С. 13.

[81] Пашнев Д.В. Понятие и классификация следов преступного использования компьютерных технологий // Компьютерная преступность и кибертерроризм. 2004. № 2. С. 159-161.

[82] Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста. 2013. № 5. С. 265.

2. Логический уровень – уровень представления более сложных структур данных (от байта до файла) на основе элементарных компонентов физического уровня. На этом уровне проявляется цифровая форма представления данных (код «0» и «1»). Он предназначен для «понимания» содержания данных и их обработки аппаратно-программными средствами компьютерной техники. Отметим, что для аналоговой электронной информации логический уровень отсутствует.

Логический уровень существования информации может быть реализован на разных носителях физического уровня. Один и тот же цифровой код может быть записан на оптическом диске, жестком диске, флеш-накопителе или преобразован в электромагнитноую волну и отправлен в пространство.

Более того, части одного файла (на семантическом уровне являющимся, к примеру, аудиозаписью) могут храниться на разных физических носителях, расположенных удаленно в пространстве друг от друга (даже в разных странах). Примером этому является технология BitTorrent, созданная в 2001 году Бремом Коеном[83]. Аналогичная ситуация справедлива и для сайта в сети «Интернет», физическая реализация которого возможна на разных носителях. О данной особенности компьютерной информации высказывается В.А. Мещеряков: «Виртуальный след не имеет физически целостной структуры. Он может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких физических носителях цифровой информации, подключенных как к одному, так и нескольким (возможно, территориально расположенных на значительных расстояниях) компьютерам, объединенным в вычислительную сеть»[84].

Вышесказанное позволяет утверждать, что физический уровень существования компьютерной информации является крайне гибким и многообразным, поэтому критерий привязанности к носителю информации в привычном понимании теряет свое значение, так как одна и та же информация

---

[83] Агибалов В.Ю. Указ. соч. С. 87-88.
[84] Мещеряков В.А. Указ. соч. С. 269.

логического уровня может быть реализована на разных видах физического уровня.

Еще одним важным свойством информации логического уровня является возможность копировать цифровой код, при этом копия будет тождественна оригиналу. Как справедливо отмечает А.Л. Осипенко, «не менее важна возможность выполнять копирование компьютерных данных при полном совпадении исходных данных и копий, производимых в неограниченном количестве»[85]. Действительно, логический уровень информации (цифровой код) может быть скопирован без потери данных и содержания.

3. Семантический уровень – уровень смыслового представления информации. На этом уровне информация преобразуется в понятный человеку вид: текст, графику, звук и т. д., и позволяет ему воспринимать и понимать содержание данных. Отметим, что как аналоговую, так и цифровую электронную информацию необходимо преобразовывать в понятную для человека форму.

Важным свойством электронно-цифровых данных является то, что информация на логическом уровне может быть модифицирована и изменена (изменен сам цифровой код), но при этом семантический уровень информации существенно изменен не будет, чтобы человек не смог понять его смысл. К примеру, для уменьшения объема занимаемым файлом физического пространства его преобразуют в другой формат, из-за чего он меняет свой цифровой код и уменьшается на физическом уровне (преобразования фотографии из формата raw в формат jpg) и при этом может потерять в качестве при представлении на семантическом уровне (качество изображения уменьшается, но при этом уже может быть не заметно для человека). При модификации цифрового кода он полностью изменяется, однако аналоговая информация (семантический уровень) остается такой же.

Полагаем, что для установления обстоятельств, имеющих значение для уголовного дела, в большинстве случаев будет важным именно семантический

[85] Осипенко А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы существования // Вестник ВИ МВД России. 2016. № 3. С. 85.

уровень представления электронно-цифровой информации (изображение, звук, текст). Логический уровень будет иметь значение в том случае, если объектом преступления является компьютерная информация или если вредоносная программа была использована в качестве орудия или средства совершения преступления, когда посредством вредоносных программ происходит какое-либо вмешательство в работу программно-аппаратных средств или модификация компьютерной информации.

Для понимания, какие изменения были произведены на логическом уровне отражения информации, необходимы специальные знания. В свою очередь для уяснения содержания семантического уровня представления электронной информации специальных знаний не требуется.

Учитывая, что электронная информация имеет особенность отражения, которая выражена в наличии многообразных посредников между исходной электронной информацией и органами чувств человека, необходимо разобраться, как данная особенность будет влиять на свойство достоверности уголовно-процессуальных доказательств.

Под достоверностью доказательств понимается – «фактическое свойство, означающее, что сведения по своему содержанию соответствуют действительным фактам и не вызывают сомнения в их истинности (признаки достоверности доказательств)»[86].

Допустимо предположить, что количество аппаратно-программных средств и сложность их взаимодействия настолько велико, что это количество переходит в качество.

Как указывает А.И. Зазулин: «Именно возникновение сомнений в достоверности компьютерной информации является в настоящее время одной из самых острых проблем, связанных с ее использованием в доказывании по уголовным делам»[87].

---

[86] Лебедев В.М., Давыдов В.А. Научно-практический комментарий к Уголовно-процессуальному кодексу Российской Федерации. М.: Издательская группа ИНФРА-М, 2014. // URL: http://www.consultant.ru (дата обращения: 01.02.2020).

[87] Зазулин А.И. Указ. соч. – С. 187.

В то же время Н.А. Зигура, доказывая необходимость выделения компьютерной информации в качестве отдельного вида доказательств, приводит следующий аргумент: «Компьютерная информация создается с помощью алгоритма, заданного программой. В свою очередь, программа создается человеком... Поскольку процесс обработки данных осуществляется техническими средствами ЭВМ (аппаратными и программными), то можно говорить о возникновении и получении (восприятии) информации опосредовано через «интеллектуальное сознание человека»»»[88].

Следует отметить, что не все ученые согласны с тем, что, наличие множественных программно-аппаратных посредников между электронной информацией и органами чувств человека является юридически значимым свойством, способным повлиять на достоверность доказательства.

Обращает на себя внимание вывод П.С. Пастухова, что «в определении природы электронного доказательства посредническая роль компьютера и операций по кодированию и раскодированию информации равно, как и посредничество эксперта, специалиста со специальным оборудованием при прочтении информации, имеющейся на объекте, существенного значения не имеет»[89].

Интересная позиция содержится в труде Р.И. Оконенко. Так, автор рассуждая о целесообразности подхода по выделению электронной информации в отдельный вид доказательств, приводит в качестве аргумента - использование специальных криминалистических устройств, одним из них является сенсорный газоанализатор. И цитрует работу Н.В. Долгополова и М. Яблокова: «Работа прибора происходит в несколько этапов: сначала молекулы вещества попадают в специальный детектор, далее соответствующая информация преобразуется в электронный вид, сопоставляется с иной информацией, сохраненной в памяти устройства, после чего на мониторе появляется вывод об идентификации

---

[88] Зигура Н.А. Разграничения компьютерной информации и «иных» документов // Вестник южно-уральского государственного университета. Серия: право. 2008. № 8. С. 54.

[89] Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дисс. … д-ра юрид. наук. М., 2015. С. 9.

полученного образца как одного из известных устройству веществ либо указание на отрицательный результат»[90].

Основываясь на указанных данных Р.И. Оконенко приходит к слудующему умозаключению: «Если мы признаем за компьютерной информацией статус отдельного вида доказательств, то нам будет необходимо придать такой статус и показаниям электронных криминалистических приборов, как простых, так и сложных. Указанные показания будут признаваться не свойствами физических объектов, но независимыми от них данными, которые необходимо будет отдельным образом изымать, опечатывать, хранить, документально оформлять, исследовать, оценивать и уничтожать в соответствии со специально предусмотренными для этого правилами. Напротив, гораздо более последовательной представляется позиция, заключающаяся в том, что данные электронных приборов, полученные путем считывания информации с объектов материального мира, аналогичны по своей физической и логической природе компьютерной информации, которая также получена путем считывания информации с объекта материального мира (в данном случае – с диска) и далее так же, посредством кодирования, доведена в форме понятных семантических символов до сознания человека. На основании изложенного можно заключить, что кодирование информации не может являться основанием для придания «электронным доказательствам» особого процессуального статуса»[91].

Таким образом, Р.И. Оконенко приходит к выводу, что использование аппаратно-программных посредников для преобразования физического и логического уровня существования компьютерной информации в понятную для человека аналоговую информацию не является априорным догматом, позволяющим сомневаться в достоверности компьютерной информации.

Данный подход является небезосновательным. Действительно, особые

---

[90] Долгополов Н.В., Яблоков М.Ю. «Электронный нос» – новое направление индустрии безопасности // Мир и безопасность. 2007. № 3. С. 54-59.

[91] Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук. М., 2016. С. 29-30.

правила приобщения к материалам уголовного дела и оценки результатов работы криминалистических приборов (электронных дальномеров, фотоаппаратов, видеокамер и т. д.), действие которых основано на преобразовании информации в электронно-цифровой код, в значительной степени способны усложнить работу правоохранительных органов.

Как было указано выше, одно из особенных свойств существования сведений, выраженных в электронной форме, заключается в том, что семантический уровень (тождественная аналоговая информация) может существовать в многочисленных вариациях на физическом и логическом уровнях. При этом для участников уголовно-процессуальных отношений в большинстве случаев имеет значение именно семантический уровень существования компьютерной информации – звук, изображения, текст и т. д., на котором зафиксированы юридические факты, к примеру, запись с камер видеонаблюдения, на которой отражены действия лица, совершающего преступление.

Можно ли в данном случае не учитывать опосредованность восприятия значимых для уголовного дела сведений?

Представляется верным, что нет необходимости подвергать скепсису работу компьютера и других электронных устройств, т.к. электронная информация формируется на физическом и логическом уровне и в дальнейшем представляется в понятном для человека виде на семантическом уровне «благодаря объективным физическим закономерностям и программному алгоритму»[92]. Законы физики и программные алгоритмы существуют объективно, вне зависимости от воли и сознания человека.

Действительно, программы создаются человеком и поэтому носят интеллектуально-волевой элемент создателя, однако в информационной среде существуют объективно, что означает – все программные алгоритмы, которые используются массовым потребителем, функционируют автономно без контроля

[92] Оконенко Р.И. Указ. соч. – С. 25.

со стороны создателя аппаратно-программных средств[93], что не требует априорного скепсиса в таком свойстве электронной информации как достоверность.

Необходимо отметить, что выраженные выше суждения, не касаются тех случаев, когда в программу был внесен вредоносных алгоритм, направленный на модификацию компьютерной информации и изменения порядка действия программно-аппаратных средств. В данном случае для установления достоверности информации потребуются специальные знания и экспертные исследования.

Важно понимать, что доказательства, выраженные в электронно-цифровой форме, существуют в искусственно-созданной человеком среде (киберпространстве) и легко поддаются внешнему изменению (удалению, модификации и т. д.).

В данной ситуации необходимо вести речь об умышленном изменении электронной информации. В каждом конкретном случае субъекту доказывания следует решить вопрос о необходимости проверки достоверности доказательств исходя из фактических обстоятельств дела.

В ряде случае о достоверности электронной информации могут указывать её атрибуты, например, электронно-цифровая подпись. Современные возможности экспертных исследований позволяют установить подлинность электронной информации. Как указывает А.И. Зазулин: «В рамках информационно-технической и фоноскопической экспертиз могут быть получены ответы на вопросы о том, была ли записана представленная информация на указанный первичный носитель (видеокамеру, диктофон), имеются ли признаки модификации или нарушения непрерывности записи, является ли файл

[93] Разработчик программы, может производить поддержку продукта, к примеру, через сеть «Интернет» обновлять программу, фактически, изменяя её, для всех пользователей унифицировано. Не исключен вариант, когда разработчик использую доступ к программе умышленно изменить её алгоритм для нанесения вреда пользователю. Однако в данном случае необходимо говорить об общественно опасных действиях конкретного лица, а не свойствах достоверности электронной информации как доказательства по уголовному делу.

оригиналом или копией»[94].

Следует отметить, что на практике электронная информация используется для проверки доказательств. Например, в соответствии с апелляционным постановлением Пермского краевого суда от 27 июня 2017 г. по делу № 22–3815/2017[95] был оставлен без изменения приговор суда о признании Н. виновным в даче заведомо ложных показаний (ч. 1 ст. 307 УК РФ) по уголовному делу. Одним из основных доказательств, подтверждающих его виновность, являлись электронные письма, где осужденный Н. обсуждал условия заключения фиктивной сделки с контрагентами.

Более того суд признает допустимым и достоверным использование в целях доказывания копию электронной информации, полученную в ходе производства предварительного расследования от участников уголовного судопроизводства.

Так, Челябинский областной суд в апелляционном порядке рассмотрел уголовное дело, по которому приговором Копейского городского суда Челябинской области гр. Иваненко был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 105 УК РФ. Согласно приговору суда гр. К., находясь в алкогольном опьянении, вступил в конфликт с гр. Х., в ходе развития которого между ними произошла драка. После окончания драки гр. К. сел за руль легкового автомобиля, и используя автомобиль как орудие преступления, совершил наезд на гр. Х., сбив последнего с ног. После чего гр. К. повторно совершил наезд на гр. Х., лежащего на земле. Адвокат гр. К. высказал суждение о том, что копирование видеозаписи с регистратора ставит под сомнение тождественность копии оригиналу. Однако суд апелляционной инстанции посчитал несостоятельной позицию стороны защиты о признании недопустимыми доказательствами видеозаписи от 7 июня 2014 г., протокола изъятия DVD+R диска, поскольку диск изымался у свидетеля К., который скопировал видеозапись с регистратора свидетеля Г. на ноутбук, а потом

[94] Зазулин А.И. Указ. соч. – С. 189.

[95] Апелляционное постановление Пермского краевого суда от 27.06.2017 по делу № 22–3815/2017 URL: // http://sudact.ru/regular/doc/ujT5XE740h5x (дата обращения: 01.12.2020).

осуществил запись на DVD+R диск[96].

Точную оценку использования электронной информации в качестве доказательства по уголовному делу сформулировал П.С. Пастухов: «Внедрение в доказывание информационных и телекоммуникационных технологий, использование электронной информации, компьютерной техники повышают точность и объективность знаний, но не изменяют природы судебной истины и не дают новых аргументов в пользу объективной истины. Поскольку истина устанавливается человеком судьей, постольку она остается вероятной. Компьютер, программа – это не субъекты доказывания, которые изменяют стандарты истинности процессуальных решений, а только технические средства, облегчающие деятельность по доказыванию… необходимо сохранить гуманистическую основу познания-доказывания, особенно в том, что касается оценки и проверки доказательств. Интеллектуально-волевой аспект доказывания относится к исключительным полномочиям судьи»[97].

В ходе проведенного опороса 76,2% сотрудников органов предварительного расследования ответили, что только в отдельно взятых случаях, когда есть сомнения в достоверности электронно-цифровой информации, в зависимости от обстоятельств уголовного дела, следует подвергать полученные данные дополнительной проверке. И только 12% респондентов считают, что во всех случая необходимо производить дополнительную проверку достоверности (аутентичности)[98].

Электронная информация обладает следующими свойствами:

1. Отражение электронной информации не подчиняется классическим правилам отражения материальных следов, основанных на принципе

---

[96] См.: Зуев С.В., Балакшин В.С., Вехов В.Б., Григорьев В.Н., Зазулин А.И., Зайцев О.А., Медведева М.О., Никинит Е.В., Овчинникова О.В., Пастухов П.С., Родиылина В.А., Смолькова И.В., Стельмах В.Ю., Шаевич А.А. Развитие информационных технологий в уголовном судопроизводстве: монография. М.: Юрлитинформ, 2018. С. 42.

[97] Пастухов П.С. Указ. соч. – С. 5.

[98] Анкетирование проводилось с января по март 2020 года среди сотрудников органов предварительного расследования, проходящих повышение квалификации в ДВЮИ МВД России и Пятом факультете Московской академии СК РФ в дислокации в г. Хабаровске. Приложение № 1.

взаимодействия следообразующего и следовоспринимающего объекта. Процесс отражения электронной информации обусловлен переводом аналоговой информации в дискретный код (цифру) с использованием программно-аппаратных средств. Если речь идет об аналоговой электронной информации, то она может не переводится цифровую форму.

2. Электронная информация не может существовать без физического носителя, однако важно понимать, что физический носитель является крайне условным, так как электронная информация может быть сохранена на различные формы физических носителей (оптическом, электромагнитном, механическом и т. д.), в том числе находящихся в разных пространственных промежутках.

3. Электронную информацию можно копировать неограниченное количество раз. При этом копия будет тождественна оригиналу.

Рассмотренные особенности электронной информации создают определенную специфику при характеристике такого свойства, как достоверность сведений. Наличие многочисленных аппаратно-программных посредников между электронной информацией и органами чувств человека не является основанием для априорного скептического отношения к достоверности электронной информации, так как аппаратно-программные средства функционируют по детерминированным физическим и программным алгоритмам.

Электронная информация существует в искусственно созданной человеком виртуальной среде и легко поддается изменению (удалению, модификации и т. д.). При каком-либо обращении с электронной информацей следует вести речь о возможном внесении изменений, и в каждом конкретном случае субъекту доказывания необходимо проводить проверку достоверности полученных данных.

Таким образом, смеем утверждать, что использование понятия «электронная информация» в поле уголовно-процессуального законодательства имеет ряд преимуществ. Во-первых, такая информация выражена в электронно-цифровой форме и не зависит от средств их хранения, обработки и передачи. Во-

вторых, применяемая часто категория «компьютерная информация» является одним из видов электронной информации. Под компьютером понимается электронная вычислительная машина, что фактически привязывает электронные сведения к цифровым данным. При этом электронная информация вбирает все многообразие сведений, существующих на основе электромагнитных свойств материи. В связи с вышеизложенным целесообразно использовать категорию «электронная информация».

1.3. Роль и значение электронной информации в системе источников уголовно-процессуальных доказательств

Дискуссия о роли и значении электронной информации (в юридической литературе обобщено «электронных доказательств») в системе источников уголовно-процессуальных доказательств продолжается в настоящее время и не получила точного разрешения. Существующие теоретические точки зрения допустимо обобщить в четырех научных подходах.

Согласно первому научному подходу, электронную информацию необходимо относить к существующим источникам уголовно-процессуальных доказательств. Так, анализируя виды объектов киберпространства (электронные сообщения, базы данных, сайт (страница) в сети «Интернет», электронный документ, программа для ЭВМ), В.Б. Вехов относительно положений ч. 2 ст. 74 УПК РФ и смежных с ней статей пришел к выводу, что указанные виды документированной информации допускаются в качестве вещественных доказательств (ст. 81 УПК РФ) и иных документов (ст. 84 УПК РФ)[99].

Указывая на основания отнесения электронной информации к перечисленным выше источникам доказательств, А.А. Тушев приходит к следующему умозаключению: «Разграничиваются вещественные доказательства и иные документы в зависимости от источника получения информации – если такая информация получена из внешнего вида электронного носителя, его

[99] Вехов В.Б. Работа с электронными доказательствами в условиях изменяющегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 23.

свойств, то это вещественное доказательство, если же из содержания электронного носителя, то это – иной документ»[100].

В свою очередь А.В. Рыбин рассматривает электронную информацию через понятие электронные документы и соответственно относит электронную информацию к источнику доказательств «иные документы»[101].

В рамках рассматриваемой точки зрения Р.И. Оконенко утверждает, что «в уголовно-процессуальном праве «электронные доказательства» относят либо к вещественным доказательствам, либо к иным документам»[102].

По мнению Р.И. Оконенко, информация действительно обладает определенными особенностями, однако это не делает её отдельным видом доказательств. Данные особенности должны быть обусловлены уголовно-процессуальными отношениями и влиять на такие свойства доказательств как относимость и допустимость. До этого момента особенности электронной информации могут учитываться только в криминалистическом смысле, как специфический механизм следообразования[103].

Критически отнеся к идеи выделения «электронных доказательств» в качестве самостоятельного вида доказательств А.М. Баранов утверждая, что «В существующих ныне в теории уголовного процесса классификациях доказательств основания для деления имеют юридическую природу, поскольку в этом есть как теоретический, так и практический смысл. Для чего нужна предлагаемая классификация, в основе которой лежат технические требования, мне трудно понять»[104].

---

[100] Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. 2012. № 3. С. 196.

[101] Рыбин А.В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты: дисс. ... канд. юрид. наук. Краснодар, 2005. – С. 11-13.

[102] Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук. М., 2016. С. 20.

[103] Оконенко Р.И. Указ. соч. С. 32

[104] Баранов, А.М. Электронные доказательства: иллюзия уголовного процесса XXI В. // Уголовная юстиция. 2019. № 13. С. 66.

Второй подход заключается в том, что электронная информация выражает собой специальную категорию в рамках уже существующих источников доказательств и поэтому должна наделяться специальным правовым статусом.

Подтверждения данного тезиса изложены в работе П.С. Пастухова, где автор указывает, что «электронные вещественные доказательства – это материальные носители электронной информации о доказываемых фактах, явлениях, процессах в информационной среде Интернет, телекоммуникационных каналах связи, а также электронные документы или объекты, которые объективно, то есть по своему происхождению, месту и времени обнаружения, свойствам, признакам, имеющихся в них информационных и материальных следах, связаны с событием, ставшим предметом уголовного расследования, и соответственно способные служить средствами к обнаружению преступления, установлению преступника или оправданию невиновного, опровержению либо подтверждению обвинения… Электронными вещественными доказательствами могут выступать не только материальные носители электронной информации, но сама электронная информация, ставшая результатом преступного действия, сгенерированная в информационной среде как след преступления»[105].

В связи с выдвинутыми умозаключениями П.С. Пастухов предлагает внести следующую поправку в положение об электронных доказательствах: «Следы преступления, оставленные в информационной среде Интернета, находящиеся в телекоммуникационных каналах связи, в случае надлежащего копирования, позволяющего подтвердить их аутентичность в суде, могут быть признаны вещественными доказательствами»[106].

Аргументы в пользу обозначенной научной позиции приводит Ю.Н. Соколов, который утверждает, что информация в электронной форме, выраженная в виде вещественных доказательств, обладает определенной спецификой – доказательственное значение здесь имеет не сам материальный носитель, но та информация, которая на нем содержится. В связи с этим автор

---

[105] Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дисс. … д-ра юрид. наук. М., 2015. С. 8.

[106] Пастухов П.С. Указ. соч. С. 13.

предлагает отдельно включить в ст. 81 УПК РФ указание на то, что вещественным доказательством может признаваться также информация в электронном виде, которая служила орудием преступления или сохранила на себе следы преступления, либо на которую были направлены преступные действия[107].

Третий научный подход относится к проблеме источников уголовно-процессуальных доказательств в целом и предусматривает отказ от законодательной модели исчерпывающих источников доказательств.

Так, В.Т. Томин, считает исчерпывающий перечень источников доказательств, представленный в ч. 2 ст. 74 УПК РФ, не только излишним, но и вредным, т.к. противоречит принципу свободной оценки доказательств и неоправданно сдерживает потенциальное развитие средств доказывания[108].

Особый интерес вызывает работа В.П. Гмырко, И.А. Зинченко. Авторы, детально проанализировав доктринальные концепции, иностранные нормы уголовно-процессуального права, а так же практические исследования ученых, пришли к следующему суждению: «Нет практической и научной необходимости определять в будущем законодательстве единое понятие процессуальных доказательств, равно как и устанавливать исчерпывающий перечень их видов. Важнее закрепить в нормах внятные критерии недопустимости доказательств и определить процедуры их включения в доказательственное обращение. Юридическая природа доказательств – сфера процессуальной доктрины, а оперативное реагирование на проблемы, возникающие в практике доказывания, – домен высшей судебной инстанции»[109].

Необходимо отметить, что в рамках научного подхода, критикующего позицию исчерпывающего перечня источников доказательств, появилась точка зрения о том, что парадигма чрезмерной законодательной детерминованности

---

[107] Соколов Ю.Н. Информационные технологии в уголовном судопроизводстве: монография. Екатеринбург : Телекоммуникационное Право, 2010. С. 116.

[108] Томин В.Т. Уголовный процесс: актуальные проблемы теории и практики. М.: Издательство Юрайт, 2009. С. 217.

[109] Гмырко В.П., Зинченко И.А. Парадоксы доказательственного права // Библиотека криминалиста. 2014. № 2. С. 17.

уголовно-процессуального доказывания не отвечает потребностям по интеграции электронных доказательств в уголовно-процессуальном праве.

Относительно названной позиции любопытную точку зрения выражают А.С. Александров и С.И. Кувычков: «Во-первых, использование электронной информации в качестве доказательств фактически стирает различия между следственными действиями и оперативно-розыскными мероприятиями, в ходе которых данная информация получается, используется для расследования преступлений и потом представляется суду. Во-вторых, следует отказаться от существующего перечня источников доказательств, который приводится в части 2 ст. 74 УПК РФ – это изживший себя анахронизм. Доказательствами надо считать сведения, полученные любой из сторон, не запрещенным законом способом, которые позволяют установить обстоятельства, имеющие существенное значение по делу. Эти сведения могут быть получены от лиц, из предметов или процессов. В-третьих, надо решать вопрос об усилении технической оснащенности как специалистов экспертных подразделений, так и сотрудников аппаратов дознания и следствия органов внутренних дел. В сфере уголовного процесса пора переходить от письменного делопроизводства к электронному: вместо протоколов надо использовать аудио- и видеозаписи. Тогда и использование электронных доказательств станет не экзотикой, а обычной практикой»[110].

Соглашаясь с мнением А.С. Александрова и С.И. Кувычкова, П.С. Пастухов[111] в одном из своих трудов приходит к следующему умозаключению: «На наш взгляд, вопрос о «процессуализации» «электронных доказательств» следует решать не через создание нового источника доказательств в следственной системе доказательств, а через смену парадигмы

---

[110] Александров А.С., Кувычков С.И. О надежности «электронных доказательств» в уголовном процессе // Библиотека криминалиста. 2013. № 5. С. 83.

[111] Пастухов П.С. Проблемы законодательного регулирования использования электронной информации в качестве доказательств по уголовному делу // «Черные дыры» в Российском законодательстве. 2015. № 3. С. 127.

доказательственного права»[112]. Автор связывает изменение парадигмы во внедрении электронного делопроизводства (электронных протоколов следственных действий) с введением института депонирования, снятием разграничений между доказательственными значениями сведений, полученными в результате оперативно-розыскных мероприятий и следственных действий, а также иными изменениями, которые позволят повсеместно использовать электронную информацию в качестве доказательств.

Четвертый научный подход связан с необходимостью выделения электронной информации в отдельный источник доказательств.

Так, В.Ю. Агибалов, детально проанализировав физико-технические аспекты отражения электронной информации, пришел к выводу, что она существенно отличается от имеющихся в УПК РФ источников доказательств. На основе сделанных выводов автор предлагает дополнить ч. 2 ст. 74 УПК РФ п. 3.2) цифровые объекты, а также ввести ст. 80.1. «Цифровые объекты», где в ч. 1 закрепить понятие «цифровой объект – зафиксированная на материальном носители компьютерная информация, представленная в виде системы дискретных информационных блоков, обеспечивающих их хранение и использование по целевому назначению»[113].

Несмотря на глубину и достоверность исследования, проведенного В.Ю. Агибаловым, в нем детально рассмотрены именно криминалистические аспекты образования следов в киберпространстве. Уголовно-процессуальные аспекты, обосновывающие выделение «цифрового объекта» в качестве отдельного источника доказательств, автором практически не приводятся.

Одной из наиболее обстоятельных работ в рамках рассматриваемого научного подхода является труд Н.А. Зигуры. Так, автор утверждает, что «компьютерная информация» значительно отличается по своим свойствам от таких источников уголовно-процессуальных доказательств как «иные»

---

[112] Пастухов П.С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств // Общество и право. 2015. № 1. С. 192.

[113] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М.: Юрлитинформ, 2012. С. 35-40, 89.

документы и вещественные доказательства и нуждается в выделении в отдельный источник доказательств[114].

Отличие компьютерной информации от вещественных доказательств Н.А. Зигура аргументирует по следующим признакам[115]:

– по доказательственному значению. Вещественное доказательство – это предмет, и доказательственное значение определяется физическими свойствами или местоположением предмета. Компьютерная информация – это содержание сведений. Хотя эта (эти сведения) информация находится на материальном носителе, иначе она не может быть признана доказательством. Но внешний вид этого носителя никак не отражает ту информацию, которая на нем записана. Доказательное значение имеет сама информация, а не ее носитель;

– по механизму образования. Для вещественных доказательств характерно механическое элементарное отражение фактов. Механизм формирования компьютерной информации определяется алгоритмом, который задан разработчиком (коллективом разработчиков) и реализуется в конкретной программе. Таким образом, программа является средством отражения фактов;

– по признаку восприятия. В вещественном доказательстве информация содержится в своем естественном, некодированном виде, и преобразование ее с помощью технических средств для восприятия не нужно. Компьютерная информация всегда опосредованна через машинный (физический) носитель информации, вне которого она не может существовать, и восприятие её (компьютерной информации) возможно только посредством технического средства (компьютера);

– по признаку среды существования. Вещественное доказательство является частью аналоговой среды. Компьютерная информация - это среда программных и технических средств – электронная среда.

В целом, соглашаясь с позицией Н.А. Зигуры о разграничении электронной информации от вещественных доказательств, необходимо уточнить ряд

---

[114] Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … кан. юрид. наук. Челябинск, 2010. С. 50-73.

[115] Там же. С. 72-73.

моментов. Так, природа механизма отражения вещественных доказательств и электронной информации действительно является различной, но при этом носит объективный характер, так как представление электронной информации в понятном для человека виде (семантическом уровне), осуществляется по объективно существующим программно-техническим алгоритмам, что детально было рассмотрено в исследовании.

Необходимо коснуться такого важного отличительного признака вещественных доказательств от иных источников, как «незаменимость и уникальность»[116]. Указанный признак основывается на том, что ни у одного объекта материального мира нет и не может быть тождественного ему двойника. Вещественные доказательства разграничиваются от иных документов как источников доказательств, своей «незаменимостью и уникальностью». Данные свойства выражены в изменениях, которые произошли в материальном объекте при совершении преступления и не могут быть повторены вновь.

Общеизвестно, что электронную информацию возможно многократно копировать. При этом копия будет тождественна оригиналу. Тогда возникает вопрос, не теряется ли свойство «незаменимости и уникальности» при отнесении электронной информации к вещественным доказательствам. В отношении поставленной проблемы необходимо обратиться к мнению С.В. Зуева, который указывает, что «исходная характеристика вещественного доказательства как информационного следа остается. След преступления – это то изменение, которое произошло в информационной среде вследствие действий преступника. То, что преступные действия осуществлялись особым способом, в особой среде не меняет сути феномена электронного вещественного доказательства. Его исходные свойства объективности и уникальности присущи и электронному вещественному доказательству»[117].

---

[116] Строгович М.С. Курс советского уголовного процесса: Основные положения науки советского уголовного процесса. М., – 1968. С. 110.

[117] Зуев С.В., Балакшин В.С., Вехов В.Б., Григорьев В.Н., Зазулин А.И., Зайцев О.А., Медведева М.О., Никинит Е.В., Овчинникова О.В., Пастухов П.С., Родиыилина В.А.,

Обратимся к следующему примеру. Предположим, что преступное деяние было зафиксировано на камеру наружного наблюдения. Электронная информация, содержащая запись о событии преступления, обладает свойством «незаменимости и уникальности», так как зафиксированное посредством стандартизированных программно-аппаратных механизмов видеокамеры преступное деяние привело к созданию «уникальной и неповторимой» электронной информации, которая сохраняется на электронном носителе. При этом данная информация была создана объективно по детерминированным программно-аппаратным алгоритмам видеокамеры без вмешательства человека.

Представляется верным, что возможность копирования электронной информации с одного электронного носителя на другой, с полным тождеством оригиналу, не лишает её свойства «незаменимости и уникальности». Свойство многократного и «тождественного» копирования является лишь особенностью электронной информации как специфичного объекта реальности, что не лишает возможности приобщения таких сведений к уголовному делу в качестве вещественных доказательств.

Дополнительно необходимо отметить, что электронная информация не является материальным объектом окружающего мира. Обязательным атрибутом «вещественности» с точки зрения общепринятого семантического значения слова «вещественный», понимается «составленный или образованный из вещества, материальный, доступный чувствам нашим, т.е. не духовный»[118].

На фактическое различие между материальным отражением и программно-аппаратным уже неоднократно обращалось внимание в юридической литературе. По мнению Л.Б. Красновой, «традиционные следы представляют собой отображение на одном материальном объекте внешнего строения другого материального объекта, тогда как основными взаимодействующими объектами при образовании виртуальных следов являются программные и информационные

Смолькова И.В., Стельмах В.Ю., Шаевич А.А. Развитие информационных технологий в уголовном судопроизводстве: монография. М.: Юрлитинформ, 2018. С. 112.

[118] Даль В.И. Толковый словарь живого великоросского языка. М.: Русский язык, 1955. Т. 4. С. 460.

элементы компьютерных объектов, которые не обладают материальной формой и, соответственно, не имеют внешнего строения»[119].

На справедливость отличия механизма отражения материальных следов и электронной информации указывает В.Ю. Агибалова: «Для понимания сущности, особенности возникновения и содержания такой информации исследователи пытались использовать хорошо зарекомендовавшую теорию следообразования, разработанную в рамках криминалистической трасологии. Однако уже первые такие попытки показали свою неэффективность. Основной причиной тому являлось механическое понимание процессов следообразования, связанного в основном с контактным взаимодействием следообразующего и следовоспринимающего объетка. Под следом понималось отображение на одном объекте внешнего строения другого объекта материального объекта»[120].

Таким образом, электронная информация отличается от вещественных доказательств по следующим критериям:

1) по механизму образования. Для вещественных доказательств характерно механическое отражение структуры следообразующего объекта в структуре следовоспринимающего или существование отдельного материального объекта. Электронная информация сохраняется, обрабатывается, передается и воспроизводится в понятный для человека вид на основе электромагнитных физических свойств материи с помощью аппаратно-программных средств;

2) по признаку восприятия. Вещественные доказательства воспринимаются органами чувств непосредственно. Электронная информация воплощается в понятную для человека форму с помощью программно-аппаратных средств, поэтому её восприятие всегда происходит опосредованно;

3) по содержанию доказательственной информации. В вещественном доказательстве юридически значимым представляется структура материального объекта. Для электронной информации значение для уголовного дела имеет

---

[119] Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: дисс. ... канд.юрид. наук. Воронеж, 2005. С. 79.

[120] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М.: Юрлитинформ, 2012. С. 29.

информационное содержание электронного носителя информации, а не сам материальный объект.

Рассмотрев основные отличия вещественного доказательства от электронной информации, проведем сравнительный анализ электронной информации в отношении такого вида уголовно-процессуальных доказательств, как иные документы.

В рамках рассматриваемого научного подхода интерес представляет мнение Н.А. Зигуры, которая указывает, что электронная информация создается программой, а «традиционный» аналоговый документ – непосредственно человеком. В своих трудах автор подчеркивает, что «компьютерная информация создаётся с помощью алгоритма, заданного программой. В свою очередь программа создаётся человеком… Поскольку процесс обработки данных осуществляется техническими средствами ЭВМ (аппаратными и программными), то можно говорить о возникновении и получении (восприятии) информации опосредованно через «интеллектуальное сознание человека». Компьютерная информация создается и/или формируется машиной, но не человеком»[121].

Названный критерий, на наш взгляд, является спорным. Так как несмотря на то, что логический алгоритм действия программных средств действительно создается человеком, однако после его реализации он начинает существовать объективно по заложенным в него разработчиком правилам.

Вторым основанием разграничения электронной информации от иных документов, выдвинутым Н.А. Зигурой, является критерий привязки к носителю информации. Автор указывает, что «основное отличие электронного документа отсутствие жесткой привязки к носителю»[122], что позволяет одному и тому же электронному документу воплощаться в разных вариантах на физическом уровне, то есть существовать на разных носителях информации.

Данный критерий сложно назвать юридически значимым, как уже отмечалось в исследовании, на законодательном уровне признается юридическая

---

[121] Зигура Н.А. Разграничения компьютерной информации и «иных» документов // Вестник Южно-уральского государственного университета. Серия: право. 2008. № 8. С. 54.

[122] Зигура Н.А. Указ. соч. С. 54.

сила электронного документа, заверенного электронно-цифровой подписью, к юридической силе официального бумажного документа (к примеру, ст. 474.1 УПК РФ). При этом подобный электронный документ, как и другая электронная информация, не имеет жесткой привязки к материальному носителю. Стоит отметить, что автор не объясняет, как именно данный критерий может повлиять на основные свойства уголовно-процессуальных доказательств. Более того, в ст. 84 УПК РФ не предъявляются какие-либо специальные свойства в аутентичности и уникальности материального носителя информации, так как в рамках «иного документа» как источника доказательств имеет значение содержание информации на материальном носителе, а не сами физические свойства материального носителя.

Отметим, что в соответствии со ст. 5 закона «Об обязательном экземпляре документа», под документом понимается «материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения»[123]. Под приведенное понятие документа можно отнести многие формы выражения электронной информации: текст, изображение, аудио, видеозапись или их комбинацию.

Однако не каждая электронная информация будет обладать реквизитами, которые позволяют её идентифицировать. Не исключены случаи, когда в электронной информации данные реквизиты будут скрыты или удаленны. Например, компьютерный вирус «Wanna cry» не имел каких-либо идентификационных реквизитов, по которым можно было бы обнаружить его создателя или первоначальный источник заражения. Предположения о создателе вируса могли делать эксперты на основании особенностей цифрового кода

[123] Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов» (ред. от 08.06.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/103526/ (дата обращения: 20.06.2021 г.).

вируса[124].

Названную электронную информацию достаточно сложно отнести к юридическому понятию официальный и неофициальный документ, и к такому виду доказательств как иные документы.

Следовательно, электронная информация обладает как признаками вещественных доказательств, так и иных документов, но полностью с данными источниками доказательств не отождествляется. Наименьшее число схожих признаков наблюдается между электронной информацией и вещественными доказательствами.

Таким образом, в науке уголовно-процессуального права допустимо выделить следующие научные подходы относительно места и значения электронной информации в системе источников уголовно-процессуальных доказательств:

1. Электронную информацию необходимо относить к существующим источникам уголовно-процессуальных доказательств.

2. Электронная информация является специальной категорией в рамках уже существующих источников доказательств и поэтому должна наделяться специальным правовым статусом.

3. Следует отказаться от законодательной модели исчерпывающих источников доказательств.

4. Электронную информацию необходимо выделить в отдельный источник доказательств.

Рассматривая обозначенные научные подходы, считаем, что действующие источники уголовно-процессуальных доказательств позволяют полностью охватить все виды сведений, выраженных в электронной форме, и приобщить их к материалам уголовного дела в качестве вещественных доказательств или иных документов. Следует отметить, что ни в одной из процессуальных отраслей российского законодательства не выделяют электронную информацию

[124] Вирус «Wanna cry» заразил десятки тысяч компьютеров по всему миру // URL: https://www.1tv.ru/news/2017-05-13/325201 (дата обращения: 01.06.2019).

(электронные доказательства) в качестве самостоятельного источника доказательств, за исключением отдельных форм ее выражения: в виде аудио- и видеозаписей (ст. 76 КАС РФ, ст. 77 ГПК РФ).

Полагаем, что выделение электронной информации (электронные доказательства) в качестве отдельного источника доказательств, наряду с иными документами может привести к коллизии права. В данном случае будет не совсем понятно, к какому источнику доказательств отнести электронный документ, заверенный электронно-цифровой подписью, к электронной информации или иным документам?

Важно отметить, что при использовании специальных электронных криминалистических устройств, являющихся компьютером (электронный газоанализатор, лазерный дальномер, электронные весы, фотоаппарат, видеокамера и т. д.), для получения информации с данных предметов их отдельный осмотр не осуществляется. Показания устройств сообщаются участникам следственного действия и вносятся в протокол без специальных правил приобщения к материалам уголовного дела. Придание электронной информации статуса отдельного источника уголовно-процессуальных доказательств может привести к тому, что для приобщения к материалам уголовного дела результатов использования специальных электронных криминалистических устройств потребуется производство отдельных следственных действий, что значительно затруднит ход предварительного расследования.

Учитывая, что существующие источники доказательств позволяют полностью охватить все виды сведений, выраженных в электронной форме, необходимо установить, к кому именно источнику следует относить электронную информацию.

В юридической литературе вопрос об отнесении электронной информации к вещественным доказательствам или иным документам является

дискуссионным[125]. Более того, решения высших судебных инстанций также не вносят достаточной ясности к обозначенной проблеме. Так, Конституционный суд РФ, высказывая правовую позицию относительно вопроса о возможности исключения из перечня доказательств аудио- и видеозаписей, произведенных гражданами с целью подтверждения факта вымогательства, ссылается на ст. 84 УПК РФ иные документы[126]. Верховный суд в одном из своих определений, говоря о видеозаписи, указал, что к иным документам относятся любые носители информации, полученные, истребованные или представленные в соответствии с ст. 86 УПК РФ[127].

Системный анализ ст.ст. 81, 81.1. УПК РФ, позволяет утверждать, что электронную информацию необходимо в большинстве случаев приобщать к материалам уголовного дела через электронный носитель информации в качестве вещественного доказательства, что в настоящий момент и наблюдается в практической деятельности органов предварительного расследования[128].

Однако следует отметить, что отнесение электронной информации к вещественным доказательствам является юридической фикцией и допускается в этом качестве только из-за конструкции уголовно-процессуальных норм о вещественных доказательствах. Электронная информация по своим фактическим признакам не может являться вещественным доказательством.

Как справедливо отмечает П.С. Пастухов: «Верно то, что электронная

---

[125] См.: Диденко К.В. Документы вещественные доказательства и «иные документы»: проблемы разграничения // Проблемы в российском законодательстве. 2008. № 2. С. 291-292.; Зазулин А.И. Компьютерная информацию в уголовном процессе: сущность и способы закрепления как доказательства по уголовному делу. // Бизнес в законе: экономико-юридический журнал. 2015. № 6. С. 130-133.; Федотов И.С., Смагина П.Г. Электронные носители информации «вещественные доказательства» или «иные документы»? // Вестник ВГУ. 2014. № 3. С. 191-199.

[126] Определение Конституционного суда РФ от 12 мая 2012 года № 814-О «Об отказе в принятии к рассмотрению жалобы гражданина Аносова Игоря Викторовича на нарушение его конституционных прав статьями 74, 75 и 81 Уголовно-процессуального кодекса Российской Федерации» // URL: http://www.garant.ru/products/ipo/prime/doc/70089288 (дата обращения: 12.12.2018).

[127] Апелляционное определение Верховного суда РФ от 04 июня 2013 года № 41-АПУ13-13сп // URL: https: //www.garant.ru/products/ipo/prime/doc /70304792/ (дата обращения: 19.12.2018).

[128] См.: Приложение № 1.

информация находится на материальном носителе, иначе она не может быть признана доказательством. Но внешний вид этого носителя никак не отражает ту информацию, которая на нем записана: доказательственное значение имеет сама информации»[129]. В продолжение этого вывода С.В. Зуев утверждает: «Получается своего рода оксюморон – беспредметное вещественное доказательство»[130].

Исходя из изложенного, система источников уголовно-процессуальных доказательств в полной мере позволяет приобщать к материалам уголовного дела все существующие формы электронной информации. При разрешении вопроса об отнесении электронной информации к вещественным доказательствам или иным документам, ее целесообразно было бы приобщать к материалам уголовного дела в качестве иных документов, а не вещественных доказательств, как того требует законодатель.

[129] Пастухов П.С. Электронное вещественное доказательство в уголовном судопроизводстве // Вестник ТГУ. 2015. № 396. С. 151.

[130] Зуев С.В. Указ. соч. С. 111.

ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ В ДОКАЗЫВАНИИ НА ДОСУДЕБНЫХ СТАДИЯХ УГОЛОВОГО ПРОЦЕССА

2.1. Производство следственных действий для получения электронной информации и (или) ее материальных носителей

Согласно устоявшейся правовой доктрине доказывание по уголовным делам, в том числе на досудебном производстве, осуществляется посредством собирания, проверки и оценки доказательств[131]. При этом следует заметить, что оценивание не всегда должно проводиться относительно конечного результата. Законность собирания электронной информации требует соответствующей предварительной оценки до начала следственного действия (осмотра, обыска, назначения и производства судебной экспертизы и т.д.), а также в период его проведения. Применительно к электронным средствам доказывания актуальным

[131] См., например: Азаров В.А. Действительно ли объективная истина – цель доказывания в уголовном судопроизводстве? // Библиотека криминалиста. 2012. № 4. С. 7-10; Белкин А.Р. Теория доказывания: научно-методическое пособие М.: Издательство НОРМА, 1999; Деришев Ю.В., Олиференко Т.Г. Всесторонность, полнота и объективность исследования обстоятельств как принцип современного уголовного судопроизводства // Ввестник омской юридической академии. 2016. № 1. С. 56-60.; Орлов Ю.К. Проблемы теории доказательств в уголовном процессе. М., 2009; Доля Е.А. Проверка доказательств в российском уголовном процессе (стадия предварительного расследования) // Правоведение. 1994. № 1. С. 27-28; Кокорев Л.Д., Кузнецов Л.Д. Уголовный процесс: доказательства и доказывание. Воронеж. Изд-во Воронеж. ун-та. 1995; Зинатуллин З.З. Уголовно-процессуальное доказывание. Ижевск: Детектив-Информ, 2003; Лазарева В.А. Доказывание в уголовном процессе: учебно-практическое пособие. М.: Высшее образование, 2009; Балакшин В.С. Доказательства в Российском уголовном процессе: понятие, сущность, классификация: монография. Екатеринбург: Изд-во УрГЮА, 2015; Громов Н.А., Зайцева С.А., Гущин А.Н. Доказательства их виды и доказывание в уголовном процессе: учебно-практическое пособие. М.: Приор-издат, 2006; Лупинская П.А. Общее и особенное в правилах о доказательствах и доказывании в УПК РФ и ГПК РФ // Lex russica (русский закон). 2005. № 4. С. 707-718; Россинский С.Б. Собирание доказательств как «первый» этап доказывания по уголовному делу // Юридический вестник Самарского университета. 2020. Т. 6. № 3. С. 901-103; Шейфер С.А. Доказательства и доказывание по уголовным делам. М.: Издательство Норма. 2020. и др.

становится вопрос о возможном причинении ущерба конституционным правам граждан.

Современные информационные технологии многократно увеличили оборот частной информации между людьми. Электронные устройства и интернет-сервисы позволяют мгновенно отправлять сообщения, управлять банковским счетом, бизнесом, получать государственные услуги и т. п. При этом получаемые или отсылаемые электронные данные не обязательно хранятся в памяти самого электронного носителя информации. Размещение информации и коммуникация на подобных сервисах происходит при помощи удаленных серверов (электронных хранилищ данных), которые могут находиться, в любой точке планеты.

Учитывая объем личной информации, к которой возможно получение доступа через электронный носитель со стороны правоохранительных органов, важно понимать уголовно-процессуальные гарантии, обеспечивающие защиту частной электронной информации при производстве предварительного расследования. Одной из основных проблем является вопрос о распространении права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений на электронные сообщения, доступ к которым сотрудник получает через изъятый электронный носитель информации.

Анализ судебно-следственной практики показывает, что в большинстве случаев для изучения содержания электронной информации, доступ к которой производится через электронный носитель (к примеру, сотовый телефон), и её приобщение к материалам уголовного дела используется компьютерно-техническая экспертиза или осмотр предметов. При этом для производства данных следственных действий судебное разрешение не требуется.

Подтверждая позицию о проведении компьютерно-технической экспертизы электронных носителей информации для получения и приобщения компьютерной информации к материалам уголовного дела, обратимся к приговору Железнодорожного районного суда г. Пензы от 4 августа 2016 года №1-

198/2016[132].

Так, гр. К. решением суда был признан виновным в совершении покушения на незаконный сбыт наркотических средств группой лиц по предварительному сговору в особо крупном размере (ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ). Неустановленное следствием лицо, использующее логин «gektor», через программу связи «CoverMe» посредством электронных сообщений связалось и предложило К. осуществлять совместный сбыт наркотических средств. Роль К. заключалась в получении наркотического вещества в тайнике по указанию пользователя «gektor» и дальнейшей транспортировке и размещению наркотического вещества в местах, указанных лицом, использующим логин «gektor». Однако К. свой преступный умысел не смог завершить, так как был задержан. Среди доказательств, подтверждающих вину К., было заключение компьютерно-технической экспертизы в отношении изъятого у К. мобильного телефона. Согласно заключению, в телефоне обнаружено программное обеспечение «CoverMe», предназначенное для защищенного обмена сообщениями, фотографиями и видео, а также для осуществления звонков. История переписки и контакты, фотографии возможных мест закладки, приложения были представлены на оптическом диске. Оптический диск был осмотрен в судебном заседании, установлено, что в телефоне, используемом К., имеется приложение «CoverMe», отражены фотографии возможных мест закладок наркотических средств, а также переписка с лицом под ником «gektor», свидетельствующая о действиях подсудимого по незаконному сбыту наркотических средств (адреса закладок, указание о том, куда надо ехать, вопросы о плате за фасовку).

Представляется, что в данном случае имеет место нарушение конституционного права человека и гражданина «на тайну иных сообщений», предусмотренного ч. 2 ст. 23 Конституции РФ.

Правоприменительная практика демонстрирует, что допустимо не только

---

[132] Приговор Железнодорожного районного суда г. Пензы от 4.08.2016 №1-198/2016 // URL: https://rospravosudie.com. (дата обращения: 18.03.2021).

исследовать содержание электронных сообщений через производство компьютерно-технической экспертизы электронных носителей информации (компьютеров, мобильных телефонов и т. д.) без судебного решения, но и при производстве следственного осмотра предметов.

Для подтверждения данного аргумента обратимся к приговору Воркутинского городского суда № 1-362/2017 от 03 ноября 2017 года[133], согласно которому, Х. был признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1, ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ. Одним из доказательств, подтверждающих вину Х., является протокол осмотра предметов: мобильного телефона «IPhone 6», изъятого при личном досмотре Х. Осмотром установлено, что подсудимый Х. осуществлял переписку посредством смс-сообщений и сервиса мгновенных сообщений «WhatsApp» с абонентами А., Б., В., свидетельствующую о сбыте наркотического средства и о приобретении наркотического средства, оплата которого произведена безналичным расчетом путем перечисления денег на банковский счет, что в совокупности свидетельствует о приобретении изъятого при задержании и личном досмотре подсудимого наркотического средства и психотропного вещества для последующего сбыта неопределенному кругу лиц на территории города Воркуты. Исходя из приговора суда, судебное решение для производства осмотра электронных сообщений через мобильный телефон «IPhone 6», принадлежащий подсудимому Х. следователем получено не было.

Более того, в настоящий момент, привлекая для производства осмотра предметов специалиста, который применяет соответствующие аппаратно-программные комплексы, допустимо подбирать пароли защиты от электронных устройств. К таким комплексам С.Ю. Скобелин относит следующие: универсальное устройство извлечения судебной информации (UFED–Universal Forensic Extraction Devise), «Мобильный криминалист», XRY, MOBILedit, «Тарантул» и другие, а также отмечает, что посредством комплекса UFED

[133] Приговор Воркутинского городского суда № 1-362/2017 от 03.11.2017 // URL: https://sudact.ru/regular/doc/65iTmvghAqmv/ (дата обращения: 01.12.2020).

«можно получить информацию о паролях, журналах вызовов, текстовых сообщениях, контактах в электронной почте, мессенджерах, записях в календаре, медиафайлах, геотегах, приложениях, служебных данных (список IMSI, данные последней сим-карты, коды блокировки); данных журнала «Lifeblog», содержащего список действий с телефоном; о переписке в различных социальных сетях («ВКонтакте», «Одноклассники», «Twitter», «Facebook») с помощью таких приложений, как «Skype» и др.»[134].

Для подтверждения сказанного обратимся к приговору Ясногорского районного суда от 1 февраля 2016 г. № 1–1/2016[135] в отношении Н. и К., х признаных виновными в совершении преступления, предусмотренного п. «а» ч. 2 ст. 204 УК РФ, – коммерческого подкупа, то есть в незаконной передаче лицу, выполняющему управленческие функции в коммерческой организации, денег за совершение действий в интересах дающего, в связи с занимаемым этим лицом служебным положением, группой лиц по предварительному сговору. Так, Н. и К. участвовали в аукционе по заключению договора аренды нежилого помещения муниципального имущества Ясногорского района. Для обеспечения победы в рамках аукциона Н. и К. передавали денежные средства лицам, выполняющим управляющую функцию в коммерческой организации, чтобы последние отказались от участия в аукционе. Среди доказательств, подтверждающих вину Н. и К., представлен протокол осмотра предметов, из которого следует, что осмотрен мобильный телефон, изъятый у Н. в ходе осмотра места происшествия. Из памяти данного телефона извлечена посредством программно-аппаратного комплекса UFED TOUCH переписка между абонентами Н. и К. через приложение «Viber». В данной переписке Н. и К. обсуждают вопросы по участию в аукционе и передаче денежных средств иным лицам за отказ их от участия в аукционе.

Чем же обусловлен подход правоприменителя для получения доступа к частным сведениям, выраженным в электронной форме через электронный

---

[134] Скобелин С.Н. Использование специальных знаний при работе с электронными следами. // Российский следователь. 2014. № 20. С. 31-32.

[135] Приговор Ясногорского районного суда от 1 февраля 2016 г. № 1–1/2016 // URL: // http://sudact.ru/regular/doc/GwUF4hU8L2Hp (дата обращения: 01.04.2021).

носитель информации, без судебного разрешения?

Так, В.Ф. Васюков, проанализировав нормативно-правовые акты, регулирующие способы получения правоохранительными органами электронной информации в порядке уголовно-процессуальной и оперативно-розыскной деятельности, указывает на следующее правило: «Правоотношения, регулируемые федеральными законами, касаются только принципов сохранения в тайне данных, которые были доверены гражданином только определенной организации или должностному лицу. Если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля»[136].

Данное правило полностью согласуется с позицией Конституционного Суда РФ, который в Определении от 25 января 2018 г. № 189-О указал, что «проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения»[137].

В 2016 г. принят Федеральный закон № 375-ФЗ[138], которым в ст. 185 УПК РФ была введена ч. 7, согласно которой «при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных, передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены

---

[136] Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. 2016. № 10. С. 67.

[137] Определение Конституционного суда РФ от 25 января 2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно- процессуального кодекса Российской Федерации // СПС «Консультант плюс» // URL: https://legalacts.ru/sud/opredelenie- konstitutsionnogo- suda-rf-ot- 25012018-n- 189-o/ (дата обращения: 12.03.2020).

[138] Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 11 июля.

их осмотр и выемка». Однако данное следственное действие, как подчеркивает В.Ф. Васюков[139], относится к получению электронных сообщений из учреждений связи, что фактически законодательно исключает судебный контроль над получением сведений с электронных носителей информации посредством следственного осмотра и производства экспертизы.

Таким образом, сложившийся уголовно-процессуальный механизм собирания доказательств через электронный носитель информации, нарушает конституционное право человека и гражданина на неприкосновенность частной жизни, предусмотренное ст. 23 Конституции РФ.

Функциональные возможности информационных технологий открывают доступ не только к электронным сообщениям, которые попадают под тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренную ч. 2 ст. 23 Конституции РФ, но и других видов охраняемых законом тайн. Рассмотрим некоторые из них.

Так, свидетельский иммунитет, предусмотренный ст. 51 Конституции РФ, закрепляет правило, связанное с волеизъявлением лица о даче показаний относительно обстоятельств имеющих значения для уголовного дела. В данном случае закон закрепляет запрет на получения идеальных (личных) доказательств, содержащихся в сознании свидетеля без его волеизъявления. Однако электронная информация существует объективно в окружающей среде.

Учитывая вышеизложенное, можно провести аналогию с собиранием материальных следов преступления, которые не содержатся в сознании участника уголовного судопроизводства (трасологических следов, предметов, документов, почтовых отправлений, телефонных переговоров и т. д.). При производстве следственных действий, направленных на сбор указанных доказательств, сотруднику органа предварительного расследования совершенно безразлично волеизъявление свидетеля, подозреваемого или обвиняемого. Поэтому логично предположить, что действие свидетельского иммунитета на получение электронной информации не распространяется.

---

[139] Васюков В.Ф. Указ. соч. С. 65.

Достаточно важным вопросом является допустимость использования электронных сообщений лиц, обладающих «профессиональным» свидетельским иммунитетом, предусмотренным ч. 3 ст. 56 УПК РФ.

Не исключен вариант того, что лица, перечисленные в ч. 3 ст. 56 УПК РФ, могут использовать интернет-мессенджеры в своей профессиональной деятельности. При этом электронные сообщения указанных лиц не являются показаниями, из чего можно сделать вывод, о том, что и свидетельский иммунитет на них не распространяется.

В рамках исследования соблюдения режимов «профессиональных» тайн интересна следующая ситуация. Так, детальную регламентацию получила адвокатская тайна. В соответствии с ч. 1 ст. 8 Федерального закона «Об адвокатской деятельности и адвокатуре Российской Федерации»[140] проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения. Однако не исключены случаи, когда адвокат подвергается уголовноому преследованию и сведения, имеющие значение для уголовного дела, могут содержаться в его мобильном телефоне или ином электронном носителе информации. В данном случае возникает проблема, как при исследовании изъятого электронного носителя ограничить доступ правоохранительных органов на ознакомление с информацией, касающейся адвоката и его доверителя? Положения ст. 450.1. УПК РФ не дают ответа на данный вопрос.

Следует отметить, что Европейский суд по правам человека (далее ЕСПЧ) также не нашел однозначного ответа в отношении обозначенной проблемы. Показательным примером является Постановление ЕСПЧ от 16 октября 2007 года «Визер и компания «Бикос бетейлигунген ГмбХ» (Wieser and Bicos Beteiligungen

---

[140] Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (ред. от 31.07.2020) // Гарант: справ. правовая система // URL: https://base.garant.ru/12126961/ (дата обращения: 20.06.2021 г.).

GmbH) против Австрии»[141]. Согласно постановлению, Визер (физическое лицо) совмещал адвокатскую деятельность с владением и управление холдинговой компанией «Бикос бетейлигунген ГмбХ», являющейся вторым заявителем по делу. Компания «Бикос бетейлигунген ГмбХ» фактически располагалась в юридическом офисе Визер. Региональный суд Австрии выдал судебное разрешение на производство обыска в офисе компании.

В ходе обыска изымались и исследовались документы, если заявитель возражал против немедленного исследования документов, они опечатывались и передавались в региональный суд в соответствии с УПК Австрии. Также было произведено исследование компьютера, находившегося в офисе, и записано несколько файлов на диск. При исследовании компьютера присутствовал представитель адвокатской коллегии.

Оценивая производство обыска ЕСПЧ указал, что обыск и изъятие электронных данных заявителей представляли собой вмешательство властей в право на уважение «корреспонденции». Суд указал, что обыск является правомерным, однако при этом гарантии адвокатской тайны соблюдались в отношении документов, а не электронных данных. Уклонение полицейских от соблюдения определенных процессуальных гарантий, имевших целью помешать «произволу» и защитить профессиональную тайну адвоката, делает обыск и изъятие электронных данных первого заявителя несоразмерными преследуемой законном цели. ЕСПЧ констатировал нарушение ст. 8 «Конвенции о защите прав человека и основных свобод»[142] в части исследования электронной информации, попадающей под режим адвокатской тайны.

Таким образом, ЕСПЧ распространяет действие адвокатской тайны на сведения, выраженные в электронной форме, и указывает на необходимость соблюдения в их отношении специальных правил при обыске касательно

---

[141] Дело «Визер и компания «Бикос бетейлигунген ГмбХ» (Wieser and Bicos Beteiligungen GmbH) против Австрии» (жалоба № 74336/01) Постановление ЕСПЧ от 16 октября 2007 // URL: https://base.garant.ru/5693183/ (дата обращения: 20.02.2020 г.).

[142] Конвенция о защите прав человека и основных свобод (ред. от 24.06.2013) // КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_29160/ (дата обращения: 13.07.2021 г.).

адвоката.

В настоящий момент УПК РФ не содержит норм, раскрывающих вопрос распространения свидетельского иммунитета на электронные сообщения в связи осуществлением профессиональной деятельности лиц, указанных в ч. 3 ст. 56 УПК РФ.

Следует признать, что в уголовно-процессуальном законодательстве существует необходимость расширения границ тайны «свидетельского иммунитета», вытекающего из субъектного состава, предусмотренного ч. 3 ст. 56 УПК РФ, на электронную информацию (электронные сообщения), которые названные лица создают и распространяют в ходе осуществления профессиональной деятельности. Для сравнения, в Уголовно-процессуальном кодексе Федеральной Республики Германия (далее УПК ФРГ)[143] режим свидетельского иммунитета распространяется на электронные сообщения, доступ к которым можно получить через электронный носитель информации, находящийся в фактическом владении лица. Как указывает П.В. Головненков, «согласно § 97 (абз. 1 № 1) УПК ФРГ не подлежит выемке переписка между обвиняемым и лицами, которые имеют право отказаться от дачи показаний на основании §§ 52, 53 (абз. 1 предл. 1 № 1-3b), 53a УПК ФРГ (супруг/супруга, помолвленный/-ая, лица, состоящие с обвиняемым в родстве или свойстве, священнослужители, защитники, адвокаты, налоговые консультанты, врачи, сотрудники признанных государством консультаций и т. д., а также их профессиональные помощники). Запрет на выемку распространяется согласно § 97 (абз. 1 № 2) УПК ФРГ также на записи, которые лица, перечисленные в §§ 53 (абз. 1 предл.1 № 1-3b), 53a УПК ФРГ, сделали о сообщениях, доверенных им обвиняемым, или о других обстоятельствах, на которые распространяется право

[143] Уголовно-процессуальный кодекс Федеральной Республики Германии от 12.09.1950 // Официальный сайт публикации документа. URL: http://www.gesetze-im-internet.de/englisch_stpo/index.html. (дата обращения: 10.07.2021 г.).

на отказ от дачи показаний»[144].

Представляется важным рассмотреть вопрос о распространении режима «коммерческой тайны» на электронную информацию. Так, в соответствии с п. 2 ст. 3 Закона «О коммерческой тайне»[145], информация, составляющая коммерческую тайну – это «сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны».

Очевидно, что указанные сведения могут быть распространены с помощью различных интернет-сервисов между заинтересованными лицами (между учредителями юридического лица, контрагентами договора коммерческой концессии «франчайзинг» и т. д.). Так, ч. 3 ст. 6 закона «О коммерческой тайне» предусматривает для обладателя информации, составляющей коммерческую тайну, а также для органа государственной власти, местного самоуправления, получившего такую информацию, обязанность предоставлять названную информацию по запросу органа предварительного расследования по делам, находящимся в их производстве.

Необходимо отметить, что ч. 2 ст. 6 закона «О коммерческой тайне», предусматривает для обладателя подобной информации механизм самозащиты. Как указывает К.В. Пронин: «Во всех случаях, когда обладатель коммерческой тайны считает требования государственного органа (органа местного самоуправления) о предоставлении ему тех или иных конфиденциальных

---

[144] Головненков П.В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: научно-практический комментарий и перевод текста закона. М.: Проспект, 2-е изд. 2012. – 312 с.

[145] Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 20.03.2021) «О коммерческой тайне» // URL: https://base.garant.ru/12136454/ (дата обращения: 20.07.2021 г.).

сведений незаконными и отказывается исполнить запрос, инициатор запроса, согласно части 2 статьи 6 Закона «О коммерческой тайне», наделяется правом затребовать эту информацию в судебном порядке».

Рассмотрение дела в суде дает обеим сторонам спора равные процессуальные возможности для отстаивания своей позиции, что является дополнительной правовой гарантией от злоупотреблений со стороны чиновников. Кроме того, обладатель коммерческой тайны также наделен правом на обращение в суд - он может подать иск о признании соответствующего предписания государственного органа (органа местного самоуправления) не соответствующим закону, иному нормативному правовому акту»[146]. Доступ к электронной информации, составляющей коммерческую тайну, через электронный носитель фактически лишает обладателя данной информации, механизма судебной самозащиты.

Выше уже указывалось, что в настоящее время существуют специальные приложения (программы), которые позволяют управлять банковским счетом (производить транзакции, оплачивать счета, брать кредит, осуществлять вклады, наблюдать информацию по счету и т. д.) через электронный носитель информации. Исходя из этого, через электронный носитель информации можно получить доступ к банковской тайне. Согласно ст. 26 Федерального закона «О банках и банковской деятельности»[147], справки по операциям и счетам юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также физических лиц выдаются кредитной организацией, при наличии согласия руководителя следственного органа, по делам, находящимся в их производстве.

При этом, согласно п. 3 ч. 2 ст. 38 УПК РФ, следователь уполномочен самостоятельно направлять ход расследования, принимать решение о

---

[146] Пронин К.В. Защита коммерческой тайны. М.: Издательство: Гросс-Медиа, 2006. С. 54.

[147] Федеральный закон от 02.12.1990 № 395-1 (ред. от 02.07.2021) «О банках и банковской деятельности» // URL: https://base.garant.ru/10105800/ (дата обращения: 13.07.2021 г.).

производстве следственных и иных процессуальных действий, за исключением случаев, когда в соответствии с УПК РФ требуется получение судебного решения или согласия руководителя следственного органа.

Взаимосвязанные положения п. 3 ч. 2 ст. 38 УПК РФ и ст. 26 Федерального закона «О банках и банковской деятельности» накладывают на следователя ведомственный контроль со стороны руководителя следственного органа. Исходя из этого, следователь вправе собирать сведения, попадающие под режим банковской тайны, только при наличии согласия руководителя следственного органа по возбужденному уголовному делу. Очевидно, что осмотр электронного носителя информации, который может быть произведен до возбуждения уголовного дела, и соответственного «банковского» приложения, согласия руководителя следственного органа не требует, что фактически необоснованно исключает ведомственный контроль и содержит предпосылки для нарушения режима банковской тайны.

Электронный носитель информации может содержать или открывать доступ к сведениям, составляющим государственную тайну. В соответствии со вторым абзацем ст. 2 закона «О государственной тайне»[148] под носителями сведений, составляющих государственную тайну, понимаются «материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов». Представляется что лица, обладающие доступом к информации, составляющей государственную тайну, могут обмениваться между собой электронными сообщениями, в которых может содержаться государственная тайна.

При этом, исходя из положения п. 4 ч. 2 ст. 29 УПК РФ, судебное решение необходимо получать только при производстве выемки предметов и документов, составляющих государственную тайну. Для следственного осмотра такого требования в УПК РФ не содержится. Следуя логике законодателя, можно

[148] Закон РФ от 21.07.1993 № 5485-1 (ред. от 01.07.2021) «О государственной тайне» // URL: https://base.garant.ru/10102673/ (дата обращения: 13.07.2021 г.).

предположить, что если судебное разрешение на изъятие предметов и документов уже получено, то повторное разрешение на их осмотр уже не нужно. Названный механизм позволяет сотрудникам органов предварительного расследования получать доступ к сведениям, составляющим государственную тайну, без судебного решения.

Таким образом, электронный носитель открывает доступ к информации, которая может относиться к многообразию вариаций режимов тайн, предусмотренных законодательством. Существующий в правоприменительной практике порядок получения электронной информации позволяет игнорировать законодательные гарантии защиты информации.

В качестве дополнительного аргумента в пользу ограничения права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренного ч. 2 ст. 23 Конституции РФ, необходимо рассмотреть позицию Европейского суда по правам человека. В соответствии с ч. 1 ст. 8 «Конвенции о защите прав человека и основных свобод» «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции».

Так, рассматривая жалобу о мониторинге телефонных переговоров и электронных сообщений своих сотрудников со стороны английского колледжа, ЕСПЧ раскрыл объем понятия «частная жизнь». Суд указал, «что в соответствии с прецедентной практикой Европейского Суда телефонные звонки из офисных помещений prima facie (на первый взгляд) охватываются понятиями «частная жизнь» и «корреспонденция» для целей п. 1 ст. 8 Конвенции… Логично, что электронные письма, отправленные с работы, также должны защищаться в соответствии со ст. 8 Конвенции, как и информация, полученная в ходе контроля за историей личного использования Интернета… Соответственно, Европейский Суд считает, что сбор и хранение личной информации, касающейся телефонных звонков, электронной почты и использования Интернета заявительницей без ее ведома, представляли собой вмешательство в ее право на уважение частной

жизни и корреспонденции по смыслу ст. 8 Конвенции»[149].

В ходе производства уголовно-процессуального обыска ЕСПЧ также указал, что электронные сообщения попадают под право на уважение частной жизни и корреспонденции, при этом суд не усматривает нарушение ст. 8 Конвенции, когда исследование и изъятие компьютерной информации проводится в ходе правомерного обыска (при получении судебной санкции). Однако ЕСПЧ констатирует нарушение ст. 8 Конвенции даже в случаях правомерности обыска, когда он является «масштабным и неизбирательным», соответственно «несоразмерным преследуемой цели»[150]. Как было указано выше, особо строгие требования ЕСПЧ выдвигает при производстве правомерного обыска в отношении адвоката[151].

Исходя из изложенного, можно предположить, что ЕСПЧ распространяет объем права на «уважение корреспонденции», предусмотренного ст. 8 «Конвенции о защите прав человека и основных свобод», на электронные сообщения. Дополнительно следует подчеркнуть, что ЕСПЧ применяет положение ст. 8 Конвенции не только к взаимодействиям, связанным с коммуникацией между лицами, но и на иные виды отношений, связанных с использованием компьютерных данных и информационных технологий: геолокация (GPS (Global Positioning System), электронные базы данных, перехват и контроль компьютерной информации, идентификация в сети «Интернет»[152].

Российская судебно-следственная практика содержит примеры распространения режима «тайны связи», предусмотренного ч. 2 ст. 23

---

[149] См.: Дело «Копланд (Copland) против Соединенного Королевства» (жалоба № 62617/00) Постановление ЕСПЧ от 03 апреля 2007 // URL: https://base.garant.ru/5732869/ (дата обращения: 12.12.2019).

[150] См.: Дело «Компании «Винчи Конструксьон» и 2Жэ-Тэ-Эм Жени Сивиль э Сервис» (Vinci Construction and GTM Genie Civil et Services v. France) против Франции» (жалобы № 63629/10 и 60567/10) Постановление ЕСПЧ от 02 апреля 2015 // URL: https://base.garant.ru/71202932/ (дата обращения: 18.04.2020).

[151] Такие требования см.: Дело «Юдицкая и другие (Yuditskaya and Others) против Российской Федерации» (жалоба № 5678/06) Постановление ЕСПЧ от 12 февраля 2015 // URL: https://base.garant.ru/71354692/ (дата обращения: 19.04.2020).

[152] Ефремов, А.А. Новые информационные технологии в практике Европейского суда по правам человека / А.А. Ефремов // Прецеденты Европейского суда по правам человека. – 2016. – № 6. – С. 10-15.

Конституции РФ, на электронные сообщения, доступ к которым открывается с помощью электронных носителей информации. Рассмотрим некоторые из них.

Так, в соответствии с апелляционным постановлением № 22К-455/2015 от 02.02.2015 года Приморского краевого суда[153] следователь по особо важным делам СУ СК России, желая произвести осмотр мобильных телефонов, а также электронных сообщений в программах «WhatsApp» и «Viber» возбудил перед судом ходатайство о разрешении производства осмотра мобильных телефонов супругов. В ходатайстве следователю было отказано. Суд мотивировал свой отказ тем, что «уголовно-процессуальным законом не предусмотрено получение разрешения на указанное следственное действие».

Показательный пример содержит кассационное определение от 24 мая 2012 года № 22-2225/12 Омского областного суда[154]. Согласно кассационному определению суда, адвокат подал жалобу в интересах потерпевшего на действия следователя, которые выражались в производстве выемки мобильного телефона и осмотре Смс-сообщений, без получения судебного решения. При этом адвокат указал, что осмотр телефонного аппарата включает внешний осмотр самого предмета, а не его содержания (в том числе телефонных соединений, контактов, СМС сообщений). Необходимо отметить, что мобильный телефон был выдан потерпевшим добровольно.

Отменяя решение Советского районного суда г. Омска и направляя жалобу на новое рассмотрение в этот же суд в ином составе, судебная коллегия Омского областного суда указала на то, что ст. 13 УПК РФ предусматривает ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых телеграфных и иных сообщений (к которым можно отнести и Смс-сообщения) только на основании судебного решения. Более того, тайна личной переписки гарантирована ч. 2 ст. 23 Конституции РФ. Также в ст. 8 Конвенции о защите прав человека и основных свобод указано, что каждый имеет право на

---

[153] Апелляционное постановление Приморского краевого суда от 02 февраля 2015 № 22 К-455/2015 // URL: https://sudact.ru/regular/doc/VsGt5FRTg35t/ (дата обращения: 18.04.2020).

[154] Кассационное определение от 24 мая 2012 № 22-2225/12 Омского областного суда // URL: https://sudact.ru/regular/doc/3O7EjaCooxZr/ (дата обращения: 19.04.2020).

уважение его личной и семейной жизни, его жилища и его корреспонденции. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом.

Судебной коллегией было разъяснено, что несмотря на то что глава 25 УПК РФ прямо не закрепляет обязанность следователя получать судебное разрешение на осмотр СМС-переписки, эта обязанность вытекает из других норм как уголовно-процессуального закона и положений Конституции РФ, так и из международных норм, закрепленных в вышепоименованной Конвенции, подлежащих безусловному применению в РФ.

Суд указал, что осмотр личной переписки, содержащейся в мобильном телефоне одного из участников судопроизводства с учетом природы и степени вмешательства фактически идентичен осмотру почтово-телеграфных отправлений либо телеграмм. Как отметила судебная коллегия, Советским районным судом г. Омска не учтено, что СМС-переписка имеет двухсторонний характер и содержит мысли не только потерпевшего, но и других лиц, пусть и имеющих отношение к делу, но вообще никак не уведомленных о том, что их личная переписка будет достоянием органов предварительного следствия.

Демонстрируемые примеры отражают правильное понимание сущности положения законодательства, регулирующего правовой режим тайны связи. Опираясь на вышеуказанные случаи из судебно-следственной практики, можно сделать вывод, что в сознании правоприменителя осмотр электронных сообщений через изъятый электронный носитель информации отождествляется с нарушением тайны связи, предусмотренной ч. 2 ст. 23 Конституции РФ.

К любопытному выводу можно прийти, если произвести сравнительный анализ действий сотрудника органа предварительного расследования по осмотру электронного носителя информации и действий лица, совершающего преступление, объектом которого являются конституционные права человека и гражданина на неприкосновенность частной жизни и тайны связи.

Так, если доступ к электронной информации против воли владельца

совершает лицо, не наделенное властными полномочиями, то подобные действия суд трактует как преступления против конституционных прав человека и гражданина, а также преступления против компьютерной информации.

Например, согласно приговору Волгоградского городского суда от 17.11.2016 № 1-914/2016[155], Н. был признан виновным в совершении ряда преступлений, предусмотренных ч. 1 ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ч. 1 ст. 137 УК РФ (нарушение неприкосновенности частной жизни), ч. 1 ст. 138 УК РФ (нарушение тайны переписки телефонных переговоров, почтовых, телеграфных и иных отправлений). Воспользовавшись тем, что SIM-карта К. была оформлена на него, Н. обратился с заявлением о повторном выпуске SIM-карты с абонентским номером К. После чего Н., в нарушение положений ст. 3, 9, 10 Закона «Об информации, информационных технологиях и о защите информации», согласно которому личная переписка является охраняемой законом тайной и ее получение помимо воли гражданина запрещается, не имея разрешения К., используя неустановленное устройство, подключенное к сети Интернет, осуществил неправомерный доступ к личной переписке К. в социальной сети «ВКонтакте», изменив логин и пароль от указанной страницы, чем модифицировал компьютерную информацию и блокировал к ней доступ К. Далее Н. без согласия К. разместил на ее странице «ВКонтакте» фотографию К. в обнаженном виде.

В приговоре суд указал, что доступ к электронным сообщениям лица без его разрешения нарушает тайну связи, предусмотренную ст. 23 Конституции РФ, а также рядом иных законов федерального уровня. Однако аналогичная ситуация наблюдается и при производстве следственных действий, с тем отличием, что доступ помимо воли владельца электронной информации осуществляет сотрудник органа предварительного расследования или эксперт.

Отсюда вывод, что суды оценивают деяние лиц, получивших доступ к электронным сообщениям через носитель информации (телефон, планшет,

---

[155] Приговор Волгоградского городского суда от 17 ноября 2016 г. № 1-914/2016 // URL: http://sudact.ru/regular/doc/hwzIJ69MfXmR/ (дата обращения: 22.03.2019).

компьютер) против воли владельца, как преступление, предусмотренное ст. 138 УК РФ (нарушение тайны переписки телефонных переговоров, почтовых, телеграфных и иных отправлений). Данный преступный состав закреплен законодателем в главе 19 УК РФ «Преступления против конституционных прав и свобод человека и гражданина». Соответственно видовым объектом для данного состава преступления являются «защищаемые уголовным законом конституционные права человека и гражданина»[156]. Исходя из этого, суд признает нарушение конституционного права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренного ч. 2 ст. 23 Конституции РФ, при осмотре электронных сообщений, содержащихся на электронном носители информации (или доступ к которым, открывается с помощью носителя информации).

Однако если принудительный доступ к электронным сообщениям против воли владельца электронного носителя информации осуществляет сотрудник органов предварительного расследования при производстве следственных действий без судебного разрешения, то в данном случае нарушения конституционных прав человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренную ч. 2 ст. 23 Конституции РФ суд не усматривает. В данном случае логика суда является парадоксальной, так как сотрудники органов предварительного расследования вторгаются и нарушают конституционные права человека и гражданина по аналогии (фактически при тех же обстоятельствах) с лицами, признанными виновными в совершении преступления, предусмотренного ст. 138 УК РФ (нарушение тайны переписки телефонных переговоров, почтовых, телеграфных и иных отправлений).

Очевидно, что доступ к электронным сообщениям через носитель информации должен оцениваться правоприменителем как нарушение тайны связи в независимости от субъекта, осуществляющего такой доступ.

---

[156] Жалинский А.Э., Дубовик О.Л. Учебно-практический комментарий к Уголовному кодексу Российской Федерации. М.: Издательство «Эксмо», 2006. – С.412.

Некоторые исследователи полагают, что осмотр электронных сообщений, содержащихся на электронном носителе информации, должен производиться по судебному решению. Так, Р.И. Оконенко утверждает, что «исследование компьютера необходимо осуществлять в форме обыска и только на основании судебного решения. Иное противоречит Конституции РФ, не основано на нормах УПК РФ, не согласуется с историей эволюции правовых гарантий в области неприкосновенности частной жизни, выраженной, в частности, в стандарте plain view»[157].

Рассматривая правоприменительную практику по исследованию содержания электронной информации, в частности электронных сообщений, через следственный осмотр предметов (планшета, смартфона, и т. д.) А.А. Хайдаров выдвинул умозаключение, что данная практика противоречит действующему законодательству и нарушает конституционные права граждан на тайну телефонных переговоров, переписки и иных сообщений. Автор предлагает для фиксации переписки в памяти телефона использовать следственное действие контроль и запись переговоров, предварительно получив судебное разрешение[158].

В свою очередь В.Ю. Агибалов, изучая особенности производства обыска при расследовании преступлений с использованием информационных технологий, пришел к выводу, что исследование и изъятие компьютерной информации представляет собой самостоятельное следственное действие – «копирование компьютерной информации», которое автор предложил внести в УПК РФ. В связи с введением данного следственного действия В.Ю Агибалов предложил расширить полномочия суда на предоставление разрешения для производства следственных действий непосредственно в компьютерных системам и сетях[159].

В пользу введения в УПК РФ дополнительного следственного действия и закрепления судебного надзора по осмотру и копированию компьютерной

---

[157] Оконенко Р.И. К вопросу о правомерности осмотра компьютера как следственного действия // Адвокат. 2015. № 1. С. 30.

[158] Хайдаров А.А. Указ. соч. С. 37, 39.

[159] Агибалов В.Ю. Указ. соч. С. 115, 117.

информации с электронных носителей В.Ю. Агибалов приводил следующие аргументы: «При производстве копирования компьютерной информации, как правило, осуществляется вторжение в личную жизнь гражданина, ознакомление с информацией, содержащей сведения, образующие одну из охраняемых законом тайн (банковская, врачебная, личной переписки и т. д.), и, по мнению ряда исследователей, в ней уже отражается и воспроизводится часть человеческой личности. Это список контактов, в телефонной книжке и электронной почте, содержание смс-сообщений или сообщений в интернет-пейджерах (ICQ, MIRC и т. д.), последовательность и продолжительность звонков определенным абонентам, наиболее часто набираемые номера, адреса электронных коммуникаций. Даже установленные рингтоны для звонков определенных абонентов в мобильном телефоне и для определенных событий в компьютерной системе, используемые экранные заставки уже позволяют судить об эмоциональном отношении владельца или пользователя компьютерной системы к тем или иным субъектам или явлениям»[160].

Следует согласиться, что мнение автора отражает роль и значение информационных технологий для современного человека. Как верно указывает автор, электронные носители информации, фактически концентрируют массив всесторонних данных, которые характеризуют всю жизнь человека. Скорее всего электронный носитель информации содержит гораздо больший объем частных сведений, о человеке, чем его жилище.

В ряде иностранных государств для исследования информации, содержащейся на электронном носителе, введен ведомственный и судебный контроль.

Уголовно-процессуальное законодательство Китайской Народной Республики не содержит специальных ограничений, связанных с исследованием со стороны правоохранительных органов абонентских устройств (смартфонов, компьютеров, планшетов и т. д.). Несмотря на это существует ведомственный процессуальный контроль со стороны вышестоящего органа. Так, при

[160] Агибалов В.Ю. Указ. соч. – С. 115.

необходимости производства процессуальных действий сотрудником полиции уровня провинции необходимо получить разрешения от органа уездного уровня. В свою очередь сотруднику полиции уровня уезда достаточно получить разрешение руководителя[161].

Необходимо обратить внимание на «Положение о процедуре осуществления осмотра места преступления, совершенного с применением средств информационно-цифровых технологий и проверки электронных доказательств», разработанное Министерством общественной безопасности Китая в 2005 году[162]. Согласно п. 18 данного положения, на месте происшествия допустимо производить онлай-анализ, подразумевающий прямой анализ и сбор информационных данных, производимый в условиях использования электронных систем во включенном состоянии на месте совершения противоправных действий. Как правило, использование процедуры онлайн-анализа может осуществляться только в указанных ниже случаях.

1. Экстренные случаи, при которых отказ от применения онлайн-анализа приведет к тяжелым последствиям;

2. Особые случаи, при которых отключение электронного оборудования и его изъятие является невозможным.

Исходя из рассмотренных правил, исследования электронного носителя информации при осмотре места происшествия в Китае возможно только в особых случаях.

Согласно УПК ФРГ, электронные носители информации подлежат выемке и дальнейшему исследованию по судебному решению, если изъятие необходимо

---

[161] На указанный порядок указал заместитель начальника факультета безопасности информации и сети милиции общественной безопасности Хэйлунцзянского института профессиональной подготовки офицеров МОБ КНР, Ли Вэньцзян в рамках проведенных 10-12 апреля 2018 в ДВЮИ МВД России лекционных занятий гостями из Хэйлунцзянского института МОБ КНР.

[162] 计算机犯罪现场勘验与电子证据检查规则 (公信安[2005]161号 公安部) / «Положение о процедуре осуществления осмотра места преступления, совершенного с применением средств информационно-цифровых технологий и проверки электронных доказательств» МОБ КНР 2005 / пер. Манцуров А.Ю. // URL: http://www.360doc.com/content/17/1121/23/44284862_706004600.shtml. (дата обращения: 08.07.2021 г.). (дата обращения: 15.01.2019).

произвести в случаях, не терпящих отлагательств, то сотрудник правоохранительного органа обязан подтвердить производство выемки в суде в течение трех дней[163].

Детальный анализ уголовно-процессуального законодательства США, регулирующего сбор доказательств, выраженных в электронной форме, был проведен Р.И. Оконенко. Так, в своем диссертационном исследовании автор отмечает, что в отличие от российского уголовно-процессуального права, американская модель «не делит следственные действия, проводимые с целью обнаружения предметов и документов на осмотр, обыск, выемку и их подвиды»[164]. Нарушение прав на неприкосновенность частной жизни устанавливается специальными стандартами, выработанными судебной практикой.

Данные стандарты определяют не только в каких случаях необходимо получать судебный ордер на обыска, а также какие объекты подлежат изъятию, какие конкретные действия может предпринимать сотрудник правоохранительных органов США при производстве обыска, к примеру, может ли сотрудник разрезать мягкую мебель, разбирать стену и т. д. Судебная практика США постепенно адаптировалась к сбору электронной информации за счет указанных выше стандартов неприкосновенности частной жизни.

Как указывает Р.И. Оконенко: «В настоящее время компьютер приравнивается судьями к закрытому контейнеру, поэтому для его исследования необходимо получить судебную санкцию. При обыске обычного помещения действия ограничиваются предметом поиска, однако так как природа компьютерной информации неочевидна и относительна, а интересующие правоохранительные органы сведения могут находиться в любом месте и виде, суды стали признавать право полиции на открытие любого файла для осмотра его

---

[163] Головненков П.В., Указ. соч. С. 54-55.

[164] Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук. М., 2016. С. 65.

содержания[165]… Указанный подход был применен в деле «United State sversus Williams» (2008). Практически аналогичную позицию занял Верховный суд США»[166].

Таким образом, исследование содержания компьютерной информации, содержащейся на электронных носителях, в США происходит в режиме обыска и только по судебному разрешению. При этом ордер на обыск в жилище, также распространяется и на компьютерную информацию[167].

Важным аспектом, раскрытым в диссертации Р.И. Оконенко, является вопрос об исследовании электронных носителей информации, изъятых в ходе правомерного ареста, когда для производства личного обыска нет необходимости получать судебное разрешение.

Так, продолжительное время судебные органы США сравнивали электронный носитель информации с закрытым контейнером (к примеру, с пачкой сигарет), который допустимо исследовать при личном обыске без судебного разрешения, исходя из правомерного ареста[168]. Как указывает Р.И. Оконенко: «25 июня 2014 года Верховный суд США принял революционное решение для института обыска при аресте по делу «Riley versus California»[169]… Суд посчитал неправомерным обыск сотового телефона при аресте без получения дополнительного судебного ордера по правилам уголовного судопроизводства[170].

Рассмотрим подробнее аргументы, которыми руководствовался Верховный суд США при принятии данного решения.

Судом был указано, что не всякий обыск может быть признан правомерным только потому, что проведен в рамках правомерного ареста, так как объект поиска может быть настолько большим и информативным, что его обследование

---

[165] Оконенко Р.И. Указ. соч. С. 78.

[166] Ward K.B. The plain (or not so plain) view doctrine: applying the plain view doctrine to digital seizures // University of Cincinnati Law Review. Vol. 79. Iss. 3. Art. 6. 2011. P.1180 - 1181 // Цит. по Оконенко Р.И. Указ. соч. С. 78-79.

[167] Оконенко Р.И. Указ. соч. С. 68.

[168] United States v. Finely. 477 F.3d 250. 5 th Cir. (2007) // Цит. по Оконенко Р.И. Указ. соч. С. 106.

[169] Riley v. California. 573 U.S. (2014). P. 2-4. Цит. по Оконенко Р.И. Указ. соч. С. 110.

[170] Оконенко Р.И. Указ. соч. С. 113.

выходит за рамки тех полномочий, которые предоставляются полиции в связи с арестом. Судом было отвергнута позиция представителя Соединенных Штатов, согласно которой поиск информации на мобильном телефоне фактически не различим с поиском физических объектов[171].

Опровержение позиции суд мотивировал существенным отличием в свойствах электронных носителей информации и обычных физических объектов: во-первых, цифровые устройства несравнимы с физическими объектами по объему и видам информации, которые могут в них содержаться. Во-вторых, существенное отличие связано с термином «содержать в себе». Если относительно физического объекта всегда можно сказать, что в нем хранится, то с мобильными телефонами дело обстоит несколько сложнее. Рассуждая в этом ключе, суд привел технологии типа «ICloud», позволяющие отображать на экране телефона ту информации, которая не хранится у него в памяти[172].

Следующим важным вопросом, который рассмотрел Верховный суд США, является возможность уничтожения или сокрытия доказательств. Суд указал, что, во-первых, отсутствие физического контроля владельца над мобильным телефоном до получения соответствующего ордера вполне может предотвратить возможность уничтожения данных. Во-вторых, проблема удаленного доступа к мобильному телефону может быть решена с помощью простых и дешевых технологий (к примеру, «сумок Фарадея»), которые блокируют внешние сигналы, поступающие на телефон. В-третьих, уничтожение информации с помощью удаленного доступа производится третьими лицами, а не самим арестованным[173].

Таким образом, уголовный процесс США значительно продвинулся в совершенствовании нормативной основы, регулирующей сбор доказательств, выраженных в электронной форме с учетом баланса между потребностями правоохранительных органов и прав и свобод человека и гражданина. В целом можно утверждать, что законодательство ряда государств уже учитывает особенности существования электронной информации, что объясняет появление

---

[171] Там же С. 113.
[172] Оконенко Р.И. Указ. соч. С. 113.
[173] Там же С. 111-112.

ведомственного и судебного контроля при собирании доказательств выраженных в электронной форме.

Обобщая рассмотренные тезисы, можно кратко изложить аргументы в пользу введения судебного контроля на исследование информации, содержащейся на электронном носителе.

1. Одна из особенностей собирания информации через электронный носитель заключается в том, что посредством электронного носителя следователь может получить доступ не только к информации, которая физически расположена в памяти самого устройства, но и к данным владельца, которые расположены удаленно (облачные технологии). Фактически, при следственном осмотре электронного устройства, исследуется не физический объект, а область киберпространства, доступ к которой открывается с помощью электронного носителя информации.

2. В электронных носителях информации можно обнаружить сведения, которые попадают под многообразие существующих режимов тайн (связи, адвокатская, коммерческая, государственная и т. д.).

3. Европейский суд по правам человека отождествляет сбор и исследование информации, полученной через электронный носитель, как посягательство на право уважения частной и семейной жизни, предусмотренной ст. 8 Конвенции «О защите прав человека и основных свобод».

4. Действия лица, связанные с непроцессуальным доступом к электронным сообщениям против воли владельца электронного носителя информации, суд определяет как нарушение конституционного права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренного ч. 2 ст. 23 Конституции РФ.

5. В некоторых субъектах РФ установлен судебный контроль на исследование содержания электронных сообщений через производство следственных действий в отношении электронных носителей информации.

6. Сотрудники предварительного расследования по своей инициативе получают решение суда на производство следственных действий в отношении

электронных носителей информации с целью изучения содержания электронных сообщений, понимая, что фактически будет ограничено конституционное право на тайну связи.

7. В некоторых иностранных государствах уже введены специальные нормы и гарантии, регламентирующие производство обыска электронного носителя информации и обеспечивающие защиту прав человека и гражданина.

Еще одной проблемой при получении доступа к электронной информации является вопрос о подмене обыска следственным осмотром. Подобно вскрытию любых помещений (в том числе сейфов, иных хранилищ), что допустимо только при производстве обыска, подбираются пароли компьютера при производстве осмотра. Принимая во внимание рассмотренные особенности электронной информации и её носителей, необходимо задаться вопросом о правомерности использования следственного осмотра, а не обыска.

Чтобы ответить на этот вопрос, необходимо изучить имеющиеся научные подходы по разграничению следственного осмотра и обыска. Так, А.П. Рыжаков указывает, что главное отличие осмотра от обыска и некоторых других следственных действий – при осмотре нельзя применять принуждение[174]. Однако данный критерий разграничения является не безапелляционным, так как на основании п.п. 4-5 ст. 27, ст. 29 УПК РФ суд принимает решение о производстве осмотра и обыска в жилище при отсутствии согласия проживающих в нем лиц, что является прямым принуждением. Также на основании ч. 3 ст. 177 УПК РФ и ч.ч. 1, 5, 13 ст. 181 УПК РФ при производстве осмотра и обыска допускается изъятие предметов, имеющих отношение к уголовному делу, что фактически является принуждением.

Анализируя позицию некоторых авторов можно прийти к выводу о разграничении осмотра и обыска по объекту. Так, Г.В. Костылева и Н.Е. Муженская включают в цели следственного осмотра изучение обстановки, обнаружения, фиксации, изъятия и исследования следов преступления и

---

[174] Рыжаков А.П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации. М.: «Гарант-сервис-университет», 2014. С. 635.

преступника и других вещественных доказательств[175]. Если в ч. 1 ст. 176 УПК РФ прямо говорится про следы преступления, то в ч. 1 ст. 182 УПК РФ про следы преступления нет никаких упоминаний. Разграничение следственных действий «осмотр» и «обыск» по объекту представляется довольно проблематичным. К примеру, если при производстве обыска, следователь обнаруживает следы нового преступления (пятна крови, следы борьбы и т. д.), то исходя из названного разграничивающего критерия, необходимо прекращать обыск и начинать осмотр места происшествия, что в практической деятельности будет недопустимо.

В свою очередь А.В. Смирнов и К.Б. Калиновский под осмотром понимают «непосредственное восприятие и процессуальную фиксацию участниками этого следственного действия внешних признаков объектов, к которым, как правило, имеется свободный доступ»[176]. Данная позиция представляется наиболее верной. Однако формулировка «свободный доступ» имеет ряд недостатков. Так, если авторы подразумевали свободный доступ к материальным объектам, находящимся в физическом пространстве, то следователь не может узнать содержание сведений, хранящихся на электронном носителе информации, без их воспроизведения на компьютере, что всегда будет нарушать конструкцию критерия «свободного доступа».

По данному вопросу интересно мнение Р.И. Оконенко, который предлагает понимать «свободный доступ» не с материальной точки зрения, а с абстрактно-юридической, а именно «о возможной степени вторжения органов предварительного расследования в частную жизнь человека»[177]. Данный критерий, приводя аналогию с правоприменительной практикой США, автор объясняет исходя из разумного ожидания гражданина относительно сохранности тайны его личной жизни. Подобная позиция объясняет, почему на основании ч. 5 ст. 177 УПК РФ требуется получить разрешение владельца жилища на

---

[175] Костылева Г.В., Муженская Н.Е. Руководство для следователя по осмотру места происшествия. М., 2010. С. 7-8.

[176] Смирнов А.В., Калиновский К.Б. Следственные действия в российском уголовном процессе: учеб. Пособие. СПб.: СПбГИЭУ, 2004. С. 12.

[177] Оконенко Р.И. К вопросу о правомерности осмотра компьютера как следственного действия // Адвокат. 2015. № 1. С. 29.

производство осмотра.

Учитывая разграничительный критерий, предложенный Р.И. Оконенко, можно предположить, что при производстве осмотра следователь вправе собирать информацию об объектах, которые доступны его непосредственному восприятию, поскольку только такая деятельность не нарушает разумные ожидания граждан по поводу сохранности тайны их личной жизни.

Учитывая вышеизложенное, следователь может осмотреть электронный носитель информации, к примеру, с записью общественного места камер видеонаблюдения, так как не вторгается в личную жизнь человека, а последний может разумно ожидать, что запись может быть просмотрена. Но при этом следователь не может осматривать компьютер лица (планшет, мобильный телефон, и т. д.), так как вторгается в личную жизнь человека и ограничивает право, предусмотренное ст. 23 Конституции РФ, чего последний разумно ожидать не может. К тому же, изымая электронное устройство у другого лица и осматривая содержащиеся на нем данные, следователь, исследуя информационную систему, выходит за рамки «свободного доступа» и вторгается в частную жизнь человека и гражданина, ограничивая право на неприкосновенность частной, семейной жизни, тайну связи. Также подобное вторжение наглядно прослеживается при подборе пароля, защищающего личные сведения владельца электронного носителя информации.

Основываясь на разграничительном критерии осмотра и обыска по объему прав сотрудника органа предварительного расследования на вторжение в личную жизнь гражданина, можно сделать вывод о подмене обыска, осмотром предмета (компьютера, мобильного телефона, планшета и т. д.).

Однако понимая, что для исследования информации на электронном устройстве необходимо производить обыск, уголовно-процессуальное законодательство создаёт перед следователем ограничения. Так, в настоящий момент ч. 1 ст. 182 УПК РФ предусматривает в качестве объектов обыска «какое-либо место» или «лицо». Отдельно взятый предмет как объект обыска уголовно-процессуальным законом не предусмотрен, что делает невозможным

производство обыска в отношении отдельно взятого электронного носителя информации.

Несмотря на положительные стороны разграничительного критерия «степени вторжения в частную жизнь человека», его сложно прямо реализовать в УПК РФ, так как он является достаточно абстрактным и оценочным, что может привести к его произвольному толкованию в правоприменительной практике. В уголовно-процессуальном праве должны быть закреплены точные условия выбора «осмотра» или «обыска».

Для унификации правоприменительной практики и создания дополнительных гарантий защищенности конституционных прав человека и гражданина на неприкосновенность частной жизни необходимо адаптировать уголовно-процессуальное законодательство к современным информационно-техническим общественным отношениям.

Регулирование правового режима электронной информации в уголовно-процессуальном праве обусловливается, во-первых, тем, что сотрудник органа предварительного расследования при получении данных с электронного носителя информации не может знать, с каким именно видом тайны ему предстоит столкнуться. Во-вторых, многообразием нормативно-правовых актов, регулирующих правовой режим информации. В-третьих, «отсутствием законодательной иерархии режимов конфиденциальности информации; отсутствием четких критериев отнесение информации к какому-либо виду тайн»[178].

Обозначенные в исследовании особенности электронной информации и электронных устройств, побудили законодателя внести в УПК РФ дополнительную категорию «электронный носитель информации». Однако, понятие электронного носителя информации в УПК РФ не было закреплено, что в правоприменительной практике приводит к отождествлению электронного носителя информации с обычным предметом. Для устранения данного

[178] Терещенко Л.К. Правовой режим информации: дисс. ... д-ра юрид. наук. М., 2011. С. 309.

недостатка необходимо законодательно закрепить в ст. 5 УПК РФ понятие «электронный носитель информации - предмет, используемый для записи, хранения и (или) воспроизведения информации, обрабатываемой с помощью средств вычислительной техники».

Для обеспечения возможности производства обыска в отношении электронного носителя информации данную категорию необходимо добавить в ч. 1 ст. 182 УПК РФ. Подобное изменение позволит унифицировать понимание электронного носителя информации как особого объекта следственных действий.

Одной из основных проблем в законодательном регулировании получения электронной информации является разграничения порядка доступа к ней. Было бы ошибочно закрепить в уголовно-процессуальном законодательстве требование по получению судебного разрешения для исследования информации на всех электронных носителях, которые изымаются в ходе предварительного расследования.

Решение данной проблемы видится в свойствах самого электронного носителя информации. Если устройство функционально позволяет распространять и воспроизводить информацию, передаваемую посредством электросвязи (мобильный телефон, планшет и т. д.), то необходимо получить судебное решение на производство обыска электронного носителя информации, так как в данном случае при исследовании электронных сообщений будет нарушаться неотъемлемое право человека и гражданина на «тайну связи» предусмотренное ст. 23 Конституции РФ.

Если электронный носитель информации не обладает указанным выше свойствами (к примеру, флеш-накопитель, внешний жесткий диск, оптический диск и т. д.), то в данном случае есть основания предполагать, что положения ч. 2 ст. 23 Конституции нарушены не будут. Однако будут затрагиваться права, предусмотренные ч. 1 ст. 24 Конституцией и ч. 8 ст. 9 Закона от №149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которым запрещается получать информацию о личной жизни лица помимо его воли, за исключением случаев, предусмотренных федеральными законами.

Можно предположить что, для производства обыска электронного носителя информации, не позволяющего распространять и воспроизводить информацию, передаваемую посредством электросвязи, помимо воли лица, достаточно постановления сотрудника органа предварительного расследования, что фактически и будет исключающим случаем, установленным УПК РФ.

Необходимо подчеркнуть, что если владелец электронного носителя информации разрешил получить доступ к электронной информации, то следует производить осмотр, не учитывая свойства самого электронного носителя информации. Изложенный выше подход соответствует теории дифференциации следственных действий осмотра и обыска, исходя из возможной степени вторжения органов предварительного расследования в частную жизнь человека. Названные ограничения по получению электронной информации также необходимо учитывать при производстве судебной компьютерно-технической экспертизы.

Учитывая вышеизложенное, допустимо предположить, что в ст. 182 УПК РФ необходимо добавить ч. 3.1. УПК РФ, согласно которой «обыск электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи, производится на основании судебного решения, принимаемого в порядке, установленном ст. 165 настоящего Кодекса. Если электронный носитель информации не обладает свойствами обмена и воспроизведения сведений, передаваемых посредством электросвязи, но имеется возражение владельца, то обыск производится на основании постановления следователя».

Далее ч. 2 ст. 29 УПК РФ дополнить пунктом 4.1 «о производстве обыска и (или) экспертизы в отношении электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи».

В соответствии с данной поправкой изложить ч. 1 ст. 195 УПК РФ в следующей редакции: «Признав необходимым назначение судебной экспертизы, следователь выносит об этом постановление, а в случаях, предусмотренных

пунктами 3 и 4.1 части второй статьи 29 настоящего Кодекса, возбуждает перед судом ходатайство, в котором указываются:»

В ч. 5 ст. 165 УПК РФ после слов «обыска и выемки в жилище» добавить «обыск электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи».

В ч. 1 ст. 176 УПК РФ после слов «иного помещения» необходимо добавить слова «электронного носителя информации», ч. 2 изложить в следующей редакции: «осмотр электронного носителя информации, места происшествия, документов и предметов может быть произведен до возбуждения уголовного дела». Также в ст. 176 добавить ч. 6.1. УПК РФ:«Осмотр электронного носителя информации производится только с согласия его владельца или лица, предоставляющего компьютерную информацию, в ином случае производится обыск в порядке ч. 3.1. ст. 182 настоящего Кодекса».

Изложенные выше законодательные поправки позволят унифицировать правоприменительную практику по получению электронной информации и (или) ее материальных носителей, а также создать дополнительные гарантии защиты прав и свобод человека и гражданина. Основным критерием, необходимым для получения судебного решения на производство следственных действия, направленных на исследование содержания электронного носителя информации против воли владельца, является функциональная возможность электронного носителя передавать сведения по сетям электросвязи, так как в данном случае имеется высокая вероятность, что при обыске электронного носителя

2.2. Правовое регулирование применения следственных действий электронно-технического характера

В условиях постоянно расширяющейся интеграции информационных технологий во все сферы жизнедеятельности человека важное значение в структуре электронных средств доказывания по уголовному делу занимают

следственные действия, направленные на получение электронной информации. Представляется, что к названным следственным действиям следует относить: «контроль и запись переговоров», «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», «получение информации о соединениях между абонентами и (или) абонентскими устройствами».

Следует отметить, что среди ученых существуют обоснованные позиции по выделению названных следственных действий в отдельную категорию «технико-специальные»[179] или «информационно-технологические»[180].

Особенности названных следственных действий заключаются в следующем:

1) Следователь принимает решение о производстве следственного действия, определяет его границы.

2) Техническую или исследовательскую работу по сбору и обобщению сведений осуществляют третьи лица, которые в последующем предоставляют результат следователю.

3) Следственные действия направлены на получение электронной информации или исследования свойств электронной информации (время получения, отправитель, достоверность информации и т.д.).

4) Данные следственные действия, по сути, носят негласный характер, так как проводятся скрытно от лиц, от которых ожидается получение электронной информации[181].

Представляется допустимым обозначить совокупность названных

---

[179] См.: Стельмах В.Ю. Технико-специальные следственные действий в российском уголовном процессе // Вестник Санкт-Петербурского университета МВД России. 2015. № 1. С. 54-55.

[180] См.: Шурухнов Н.Г. Процедура и содержание процессуальных информационно-технологических средств сбора доказательств, используемых в российской практики расследования преступлений, совершаемых с использование современных электронных технологий // Вопросы правоведения. 2013. № 5. С. 297.

[181] О негласных следственных действиях подробнее см., например: Зуев С.В. Негласные формы уголовного судопроизводства 1864 года и их современное развитие // Расследование преступлений: проблемы и пути их решения. 2014. № 4 (4). С. 110-117.; Семенцов В.А. К вопросу о пополнении системы следственных действий негласными познавательными приемами // Законы России: опыт, анализ, практика. 2016. № 4. С. 48-57.

следственных действий как «электронно-технические», что будет обусловливать получение именно электронной информации. Под электронно-техническими следственными действиями следует понимать совокупность следственных действий, направленных на получение электронной информации, где следователь принимает решением о производстве следственного действия, определяет его рамки, а техническую работу осуществляют третьи лица, которые и предоставляют результаты.

Однако уголовно-процессуальное регулирование электронно-технических следственных действий значительно отстает от потребностей и потенциальных возможностей правоохранительных органов по сбору электронной информации и содержит ряд существенных процессуальных недостатков.

Одной из проблем названных следственных действий является ограниченность сведений, которые они позволяют получить. Обратимся к следственному действию «контроль и запись переговоров», предусмотренному ст. 186 УПК РФ, включеннному в УПК РФ с момента его принятия в 2001 году. Данная норма претерпевала неоднократные изменения, однако поправки, внесенные в нее, не коснулись объема и качества сведений, которые допустимо получать с помощью «контроля и записи переговоров».

В соответствии с ч. 1 ст. 186 УПК РФ «допускается контроль и запись телефонных и иных переговоров». Исходя из формулировки «иные переговоры», кроме аудио информации, которая передается по каналам «телефонной» связи, данное следственное действие допустимо применять и к другим каналам электросвязи. Согласно п. 35 ст. 2 Закона «О связи» под электросвязью понимается «любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам». Данное положение подтверждается п. 14.1 ст. 5 УПК РФ, в котором указано, что «прослушивание и запись переговоров путем использования любых средств коммуникации».

По данному вопросу интересна позиция А.А. Хайдарова, который считает,

что «следователь, чтобы зафиксировать содержание переписки в памяти телефона, обязан произвести контроль и запись переговоров, предварительно получив на это судебное разрешение»[182].

Тем не менее, позиция относительно возможности получать электронные сообщения посредством «контроля и записи переговоров», является небезапелляционной.

Так, в ч. 6 ст. 186 УПК РФ говорится, что «следователь в течение всего срока производства контроля и записи телефонных и иных переговоров вправе в любое время истребовать от органа, их осуществляющего, фонограмму для осмотра и прослушивания». Исходя из закона, результатом контроля и записи является фонограмма. Согласно толковому словарю Т.Ф. Ефремовой под фонограммой понимается, «1. Запись звука (речи, музыки, пения), сделанная на пластмассовом диске, магнитной ленте, кинопленке и т. п. 2. Пластмассовый диск, магнитная лента, кинопленка и т. п. с такой записью»[183]. Таким образом, данное следственное действие направленно на контроль и запись аудио (звуковой) информации, разговора между лицами.

В пользу данной позиции можно привести мнение В.Ю. Стельмаха, который утверждает: «очевидно, что в ст. 186 УПК РФ термин «переговоры» употреблен в простом значении, в том же смысле, что и «разговор», то есть «словесный обмен сведениями, беседа». Таким образом, под переговорами следует понимать любые случаи общения людей речевым способом»[184].

Подобное понимание категории «переговоры» в соотношении с категорией «фонограмма» как результат следственного действия «контроль и запись переговоров» значительно ограничивает объект данного следственного действия и фактически делает невозможным получение мультимедийных электронных

---

[182] Хайдаров А.А. Незаконная практика фиксации личной переписки граждан на мобильных устройствах // Уголовный процесс. 2017. № 5 С. 39.

[183] Ефремова Т.Ф., Новый толково-словообразовательный словарь русского языка // URL: http://slovariki.org/tolkovyj-clovar-ozegova/38033 (дата обращения: 03.09.2019).

[184] Стельмах В.Ю. К вопросу о предмете контроля и записи телефоны переговоров как следственного действия // Деятельность правоохранительных органов в современных условиях: мат. XVIII Меж-ной науч.-практ. конф, посвященные 20-летию образования института ВСИ МВД России. 2013. С. 124.

сообщений, в том числе и «телефонной переписки».

К данной позиции дополнительно можно привести следующие обоснование. Так, уровень технического развития интегрировал телефонную связь со связью в сети «Интернет» фактически в единую систему электросвязи. Это значит, что с обычного телефона возможно позвонить на телефон, который работает через сеть «Интернет» и обратно. В настоящий момент одной из названных технологий является «IP-телефония»[185]. Одним из примеров, информационно-телекоммуникационного сервиса, использующего технологию «IP-телефонии» является «Skype».

В данном случае возникает еще одна проблема. Если по каналам телефонной связи передается электронная информация, которая преобразуется в звук, то через сеть «Интернет» передается информация, которая преобразуется в аудио, видео, изображение и т. д. Как указано в ч. 6 ст. 186 УПК РФ, следователь в ходе всего производства данного следственного действия имеет право истребовать фонограмму. Из чего следует, что результатом данного следственного действия является звуковая информация. Однако IP-телефония позволяет передавать не только звук, но и другие виды данных: видео, текст, изображение и т. д. В данном случае возникает противоречие между объектом названного следственного действия и возможностями современной электросвязи.

С одной стороны, юридическая конструкция ст. 186 УПК РФ позволяет производить данное действие по отношению ко всем видам коммуникаций проходящих по сетям электросвязи. С другой – ограничивает получение сведений, передаваемых по сетям электросвязи звуком (фонограммой), что абсурдно с точки зрения существующих в настоящий момент средств коммуникации.

В данном случае возникает вопрос: как законодатель допустил такое явное противоречие? Ответ на него видится в том, что данное следственное действие было принято для получения сведений, которые передаются через голосовые

[185] Русев Е. Применение технологии IP телефонии для малого и среднего бизнеса: преимущества, недостатки и перспективы развития // Экономическая среда. 2018. № 4. С. 18-20.

телефонные звонки, без учета других видов электросвязи, к примеру, сети «Интернет».

В пользу данного умозаключения следует привести мнение В.Ю. Стельмах о том, что «формулировка закона отражала состояние средств связи в момент его принятия, когда реально единственно существующим средством связи, переговоры по которому могли контролироваться был телефон. Кроме того, в начале двадцать первого века технологии передачи голосовых и не голосовых сообщений были совершенно различными. Одно средство связи не было способно передать и те и другие сообщения»[186].

Еще одним подтверждением данного тезиса служит момент возникновения IP-телефонии. Как указанно в работе Дэниела П. Дэрн и Пола Десмонда[187], становление IP-телефонии началось в 1996 году в США в качестве корпоративной связи. Повсеместно данный вид связи начал использоваться только в начале 2000-х годов. Один из самых известных операторов IP-телефонии «Skype» был основан только в 2003 году[188].

Исходя из приведенных данных следует, что на момент принятия УПК РФ в декабре 2001 года интеграция телефонной связи с сетью «Интернет» была еще на начальном этапе. В связи с этим рассматриваемое следственное действие не было рассчитано на интеграционные явления в области электросвязи.

Таким образом, во-первых, юридическая конструкция ст. 186 УПК РФ «контроль и запись переговоров» допускает возможность применения данного следственного действия не только к телефонной связи, но и другим видам электросвязи. Во-вторых, результатом данного следственного действия является фонограмма (звуковая информация), что ограничивает возможность получения сведений из электронно-информационной сферы, т.к. данное следственное

---

[186] Стельмах В.Ю. К вопросу о предмете контроля и записи телефонных и иных переговоров как следственного действия // Материалы XVIII Международной научно-практической конференции: «Деятельность правоохранительных органов в современных условиях». Иркутск, 2013. С. 119.

[187] Дэниел П. Дэрн, Пол Десмонд. «Позвоним через IP?» / Сети / Network world. 1997. № 8 // URL: http://www.osp.ru/nets/1997/08/142803/ (дата обращения: 24.08.2020).

[188] Данные о появлении компании «Skype» // URL:// https://www.skype.com/ru/about/ (дата обращения: 10.09.2021).

действие вводилось законодателем для получения аудио информации, которая передается по сетям телефонной связи. Из чего следует, что данное следственное действие устарело и не адаптировано к современному уровню технического развития коммуникационных средств связи, значительно сужая объем сведений, которые возможно получить и использовать при доказывании по уголовному делу.

Следующим следственным действием, направленным на получение сведений выраженных в электронной форме, является «наложение ареста на почтово-телеграфные отправления их осмотр и выемка», предусмотренное ст. 185 УПК РФ.

В 2016 году в ст. 185 УПК РФ была внесена ч. 7, согласно которой «при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка».

В соответствии с п. 10 ст. 2 ФЗ Об информации под электронным сообщением понимается «информация, переданная или полученная пользователем информационно-телекоммуникационной сети». Кроме того п. 35 ст. 2 Федерального закона «О связи» под электросвязью подразумевает любые «излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам».

Исходя из указанного выше определения, под категорию «электронные и иные сообщения» попадает широкий спектр информации, которая удовлетворяет потребностям органов, осуществляющих предварительное расследование.

Следует отметить, что среди ученых до внесения ч. 7 в ст. 185 УПК РФ не было единого мнения относительно допустимости распространения данного следственного действия на электронные сообщения. Так, Е.Р. Россинская и А.И. Усов считают, что действия по изъятию электронной почты, адресованной абоненту, попадают под выемку почтово-телеграфной корреспонденции и

должны осуществляться в соответствии со ст. 185 УПК РФ[189]. В свою очередь, А.Н. Гуев отмечает в своей работе, что «в практике возник вопрос: относятся ли правила ч. 1 ст. 185 УПК к отправлениям по электронным средствам связи в т.ч. по сетям «Интернета»? К сожалению, в ч. 1 ст. 185 УПК – пробел, поскольку такие отправления нельзя приравнять к почтово-телеграфным. Пробел надо устранять (учитывая большую распространенность таких отправлений), впредь до этого следует исходить из буквального текста ст. 185 УПК РФ»[190].

Судебная практика подтверждает мнение Е.Р. Россинской и А.И. Усова, что свидетельствует об использовании «ареста на почтово-телеграфные отправления» к электронным сообщениям до внесения ч. 7 в ст. 185 УПК РФ. Обратимся к постановлению Первореченского районного суда г. Владивостока № 3/6-248/11 от 29 декабря 2011 года[191]. Согласно постановлению 17 ноября 2011 года, в присутствии подозреваемого Н. и его защитника с целью устранения доступа заинтересованных лиц к информации, хранящейся в электронном почтовом ящике, пароль почтового ящика был изменен. Далее суд, удовлетворяя ходатайство следователя, наложил арест на электронный почтовый ящик, заключающийся в запрете доступа любых лиц без разрешения органа предварительного следствия к содержащейся в нём информации. В постановлении суд разрешил производство осмотра и выемки содержащейся в электронном почтовом ящике корреспонденции.

Необходимо отметить, что УПК РФ, в целом, и ст. 185 УПК РФ, в частности, не содержат положений относительно порядка действий следователя при модификации электронной информации в целях ограничения доступа лиц к электронной почте и процедуры ареста электронной почты (электронных сообщений).

---

[189] Россинская Е.Р. Усов А.И. Судебная компьютерная – техническая экспертиза. М.: Право и закон, 2001. С. 99.

[190] Гуев А.Н. Постатейный комментарий к Уголовно-процессуальному кодексу Российской Федерации. 2010 // Гарант: справ. правовая система // URL: http://base.garant.ru

[191] Постановлению Первореченского районного суда г. Владивостока № 3/6-248/11 от 29.12.2011 // URL: rospravosudie.com/court-pervorechenskij – rajonnyj-sud-g- vladivostoka-primorskij-kraj-s/act-102540216 (дата обращения: 23.03.2019).

Однако применение «ареста почтово-телеграфных отправлений» к электронным сообщениям является фактом, но вызывает ряд юридических противоречий. Введенное положение об осмотре и выемке электронных и иных сообщений, передаваемых по сетям электросвязи, их не устранило.

Представляется, что, если поправка была внесена в законодательные нормы, регулирующие производство следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», то предусмотренные ею предписания должны учитывать содержание, объект и форму этого следственного действия, соответствовать нормативным правовым актам, регулирующим общественные отношения в области распространения информации в сети «Интернет».

В действительности, между данными категориями возникает юридическая коллизия, которая не позволит получать электронные и иные сообщения, передаваемые по сетям электросвязи. Необходимо разобраться в причинах возникновения указанного противоречия.

Исходя из ч. 1 ст. 185 УПК РФ, объектами данного следственного действия являются: бандероли, посылки или другие почтово-телеграфные отправления, либо телеграммы или радиограммы. Электронные сообщения в качестве объекта «наложения ареста на почтово-телеграфные отправления» не указываются. Допустимо предположить, что законодатель относит электронные сообщения к категории «другие почтово-телеграфные отправления».

Рассмотрим подробнее, что понимается под другими почтово-телеграфными отправлениями. Перечень почтовых отправлений содержится в Приказе Министерства связи и массовых коммуникаций № 234 «Об утверждении правил оказании услуг почтовой связи»[192]. Согласно № 2 приказа, к ним относятся почтовая карточка, письмо, бандероль, секограмма, мелкий пакет, мешок «М», посылка. Также в пунктах 51-62 приказа предусмотрены положения, предусматривающие особенности приема и доставки (вручения) простых и

[192] Приказ Министерства связи и массовых коммуникаций от 31.07. 2014 № 234 «Об утверждении правил оказании услуг почтовой связи» (ред. от 19.11.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/70835708/ (дата обращения: 10.05.2021 г.).

заказных почтовых отправлений, пересылаемых в форме электронных документов, что фактически является электронным сообщением. Однако стоит учитывать, что в п. 51 анализируемого приказа предусмотрено, что данные электронные сообщения передаются с использованием информационной системы организации федеральной почтовой связи.

Если рассмотреть этот вопрос с позиции соотношения понятий, в соответствии с которой понятие «электронные сообщения» шире по объему и включает в себя понятие «электронные документы», передаваемые именно с использованием информационной системы организации федеральной почтовой связи, тогда законодательная поправка вписывается в текст уголовно-процессуального закона и выглядит логично. Однако если рассматривать производство этого следственного действия с позиции возможности и допустимости получать все электронные и иные сообщения, которые передаются по сетям электросвязи, то тогда возникает технико-юридическая коллизия между новым объектом данного следственного действия, формой его осуществления и смежными нормативно-правовыми актами, регулирующими отношения, возникающие в области распространения информации в сети «Интернет».

В пользу обоснования сформулированной выше научной позиции можно привести следующие аргументы. Содержание ст. 185 УПК РФ четко описывает форму производства следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка». Так, основными индивидуализирующими признаками лица, почтово-телеграфные отправления которого планируется арестовать, являются его фамилия, имя, отчество и адрес (п. 1 ч. 3 ст. 185 УПК РФ).

Указанные выше признаки индивида подходят для наложения ареста на его почтово-телеграфные отправления. Вместе с этим данные признаки не способны конкретизировать лицо, электронные сообщения которого планируется задержать, осмотреть и произвести выему.

В отличие от традиционной почты в сети «Интернет» пользователь может придумать себе любое имя, фамилию, адрес, которые не будут препятствовать

обмену электронными сообщениями и индивидуализировать его как конкретную личность. В рамках нового объекта (электронных сообщений) следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» законодателю необходимо было ввести новые индивидуализирующие признаки, например, сетевой адрес (IP-адрес), доменное имя, адрес электронной почты и т. д. Однако подобных поправок законодатель в УПК РФ не внес, чем не конкретизировал возможность его производства в отношении электронных сообщений.

Также в правовой конструкции ст. 185 УПК РФ говорится о том, что следственное действие «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» производится в учреждениях связи. Законодатель не разъясняет, что понимается под учреждениями связи, охватывает ли категория «учреждение связи» выемку электронных сообщений в сети «Интернет» и какой субъект должен выдавать электронные сообщения в сети «Интернет» для их осмотра и выемки.

Отвечая на поставленные нами выше вопросы, обратимся к научной позиции А.В. Смирнова и К.Б. Калиновского, которые утверждают, что используемый законодателем в ст. 185 УПК РФ термин «учреждение связи» вносит неясность в деятельность органов предварительного расследования, прокуратуры и суда. Сформулированное ими суждение объясняется тем, что Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи»[193] предусматривает как минимум три сходных, но разных понятия: «операторы почтовой связи», «организации почтовой связи» и «объекты почтовой связи». По смыслу ст. 185 УПК РФ наиболее верно считать, что арест исполняется оператором почтовой связи – организациями почтовой связи и индивидуальными

[193] Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» (ред. от 27.12.2019) // Гарант: справ. правовая система // URL: http://base.garant.ru/180689/ (дата обращения: 01.08.2021 г.).

предпринимателями, имеющими право на оказание услуг почтовой связи[194].

Более того, п. 1 ст. 10.1 ФЗ Об информации вводит категорию «организатор распространения информации в сети «Интернет», под которым понимается «лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет», например, «ВКонтакте», WhatsApp, Skype и т. д.

Согласно подп. 2 п. 3 ст. 10.1 ФЗ Об информации, на организатора распространения информации в сети «Интернет» возлагается следующая обязанность: текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео- или иные электронные сообщения пользователей сети «Интернет» хранить до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством РФ.

Законодатель не указывает, что именно «организатор распространения информации в сети интернет» обязан предоставлять электронные сообщения, из чего можно сделать небезапелляционное умозаключение о том, что категория «учреждение связи» охватывает категорию «организатор распространения информации в сети «Интернет».

Однако с вышеуказанным умозаключением также связаны определенные противоречия. Так, в п. 3.1. ст. 10.1 ФЗ Об информации говорится, что «организатор распространения информации в сети «Интернет» обязан предоставлять указанную в пункте 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами». Из данного положения

[194] Смирнов А.В., Калиновский К.Б. Комментарий к Уголовно-процессуальному кодексу Российской Федерации. М.: Проспект, 2009. // Гарант: справ. правовая система. (дата обращения: 01.08.2021 г.).

следует, что организаторы распространения информации в сети «Интернет» не обязаны предоставлять электронные сообщения органам, осуществляющим предварительное расследование.

Таким образом, практическое использование «наложение ареста на почтово-телеграфные отправления» по отношению к электронным сообщениям является фактом. Однако наличие подобной судебно-следственной практики является достаточно противоречивым явлением. Основная причина этого видится в том, что следственное действие сконструировано законодателем для ареста, выемки и осмотра именно почтово-телеграфных отправлений в учреждениях связи, а не электронных сообщений у организаторов распространения информации в сети Интернет. Добавление ч. 7 в ст. 185 УПК РФ породило дополнительные вопросы, так как законодатель не определил порядок и возможность наложения ареста на электронные сообщения. В ч. 7 ст. 185 УПК РФ говорится только о выемке и осмотре электронных сообщений. Также законодатель не уточнил индивидуализирующие признаки пользователя сети «Интернет» и (или) электронных сообщений, подлежащих выемке и осмотру.

Более того, до введения ч. 7 в ст. 185 УПК РФ электронные сообщения от оператора связи получали посредством производства выемки на основании ст. 183 УПК РФ с получением судебного разрешения, так как ограничивалось неотъемлемое право человека и гражданина на тайну переписки, телефонных переговоров и иных сообщений, предусмотренное ч. 2 ст. 23 Конституции РФ.

Для подтверждения данного тезиса необходимо обратиться к приговору Домодедовского городского суда № 1-5/2017 (1-581/2016;) от 16 февраля 2017 года[195], согласно которому К. был признан виновным в совершении преступления, предусмотренного ч. 5 ст. 33 ч.1 ст. 226.1 (пособничество в контрабанде культурных ценностей). Среди доказательств, подтверждающих вину К., содержится протокол выемки, исходя из которого в ООО «Майл.ру» был изъят компакт-диск с входящими и исходящими отправлениями электронного

[195] Приговору Домодедовского городского суда № 1-5/2017 (1-581/2016;) от 16 февраля 2017 // URL: https://jur24pro.ru/ugolovnye-dela/ugolovnoe-delo-1-5-2017-1-581-2016-/

почтового ящика, используемого К. Также, согласно протоколу осмотра изъятого в ООО «Майл.ру» компакт-диска, К направил с используемого им электронного почтового адреса на используемый Н. электронный почтовый адрес фотоизображения скульптур «Будда Шакьямуни» и «Цзонхава», чтобы Н. подготовила документы для незаконного вывоза в США указанных скульптур без их непосредственного осмотра.

Отдельное внесение выемки и осмотра электронных сообщений в ст. 185 УПК РФ без его дополнительной регламентации представляется нецелесообразным.

В этом контексте небезосновательным можно считать позицию А.Л. Осипенко, согласно которой «закрепленный процессуальным законодательством порядок взаимодействия следствия с учреждениями связи при наложении ареста на почтово-телеграфные отправления абсолютно неприменим к возможным мероприятиям с участием операторов связи по аресту сообщений электронной почты»[196].

Электронные сообщения – это не единственная информация, которая может иметь значения для уголовного дела. К примеру, такой информацией могут являться геолокационные[197] данные, которые указывают на передвижение электронного носителя информации в пространстве и времени, что может определить местоположения лица[198]. И это лишь один из многочисленных

---

[196] Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. 2010. № 2. С. 124.

[197] Геолокация – определение реального географического местоположения электронного устройства, например, радиопередатчика, сотового телефона или компьютера, подключенного к Интернету. Словом «геолокация» может называется как процесс определения местоположения такого объекта, так и само местоположение, установленное таким образом. Подробнее см.: Соколов А.Д., Стешкова А.С., Будникова С.А. Геолокация с использование API социальных сетей // Актуальные проблемы деятельности подразделений УИС: сб. мат. Всеркой науч.-практ. конф. Воронеж: «Научная книга», 2016. –С. 143.

[198] Об использовании геолокации подробнее см.: Васюков В.Ф. Особенности получения сведений о геолокации мобильного абонентского устройства, находящегося в пользовании скрывшегося подозреваемого, посредством общедоступных аппаратных средств и программных ресурсов // Библиотека криминалиста. 2016. № 3. С. 321-324; Соколов А.Д., Указ. соч. С. 142-146.

примеров потенциала использования сведений из электронно-информационной сферы при расследовании уголовного дела.

В данном случае не совсем понятно, почему законодатель не предусмотрел необходимость получения судебного решения для выемки и осмотра электронной информации частного характера в целом, а не только электронных сообщений.

Еще одним «информационно-технологическим» следственным действием является «получение информации о соединениях между абонентами и (или) абонентскими устройствами», содержание которого раскрывается в ст. 186.1 УПК РФ.

В литературе отмечается ряд недостатков юридической конструкции и практического использования данного следственного действия.

Так, В.Ю. Стельмах указывает, что «Статья 186.1 УПК РФ предусматривает два варианта и, соответственно, два порядка получения информации о соединениях между абонентами и (или) абонентскими устройствами – ретроспективный и перспективный. Ретроспективный вариант предусматривает получение сведений о соединениях, имевших место в прошлом, до решения о производстве следственного действия. Перспективный вариант означает получение информации о соединениях, которые состоятся в будущем, после принятия соответствующего решения следователем. Грамматический и логический способы толкования позволяют сделать однозначный вывод, что об установлении 6-месячного срока производства следственного действия закон говорит лишь тогда, когда планируется получать указанную информацию «на будущее»[199].

В практической деятельности складывается ситуация, что суды не всегда дают разрешение на производство названного следственного действия.

По данной проблеме любопытный пример приводит А.А. Цыкора: «Одним из типичных примеров является отклонение судьей Биробиджанского городского

[199] Стельмах В.Ю. Проблема процессуальной регламентации следственных действий, направленных на получение сведений, передаваемых по сетям электросвязи // Юридическая наука и правоохранительная практика. 2013. № 3. С. 111.

суда ЕАО ходатайства следователя о получении информации о соединениях между абонентами и абонентскими устройствами в рамках расследования уголовного дела о преступлении, предусмотренном ч. 4 ст. 111 УК РФ (причинение тяжкого вреда здоровью, повлекшее по неосторожности смерть потерпевшего). Следователя интересовала информация о соединениях за период, предшествующий возбуждению данного уголовного дела, указывающих на обстоятельства совершенного преступления, но его ходатайство было отклонено. Данное решение судьи городского суда было обжаловано путем инициации прокурором кассационного представления. Кассационным определением Судебной коллегии по уголовным делам судом Еврейской автономной области указанное постановление судьи об отказе в удовлетворении ходатайства следователя было отменено. Принимая это решение, судебная коллегия установила, что положениями ст. 186.1 УПК РФ не предусмотрено ограничений именно по длительности периода, за который необходимо получить соответствующую информацию об уже состоявшихся соединениях между абонентами и (или) абонентскими устройствам»[200].

Как можно увидеть из указанного примера, судебная практика в отношении поднятой проблемы достаточно противоречива. Однако существование решений по отказу со стороны суда в ретроспективном производстве следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами», свидетельствует о неточностях, допущенных в законодательной конструкции ст. 186.1 УПК РФ, что требует внесения изменений в соответствующие нормы УПК РФ.

Следующим недостатком рассматриваемого следственного действия является отсутствие конкретного срока, по которому оператор связи обязан предоставить следователю информацию о соединениях между абонентами и

[200] Кассационное определение Судебной коллегии по уголовным делам суда Еврейской автономной области / Официальный сайт суда Еврейской автономной области Дело № 22221/2011 Цит. по: Цыкора А.А. Некоторые проблемы производства следственного действия «получение информации между абонентами и (или) абонентскими устройствами // Известия ТГУ. Экономические и юридические науки. 2013. № 2-3. С. 241.

(или) абонентскими устройствами.

Так, И.А. Грошев отмечает, что «изучение уголовных дел, находящихся в производстве одного из следственных отделов, показало, что в настоящий момент участились факты не исполнения региональными операторами сотовой связи требований уголовно – процессуального законодательства Российской Федерации. Так, в рамках указанных выше уголовных дел, оператор сотовой связи «TELE2» неоднократно отказывал в предоставлении информации о соединениях между абонентами и (или) абонентскими устройствами, по которым в соответствии с уголовно процессуальным законом имелось судебное решение на разрешение в получении информации. В ходе дальнейшего изучения уголовных дел было установлено, что в ответ на запрашиваемую информацию, были направлены в следственный отдел по истечении 1-1,5 месяцев с момента направления постановлений суда в адрес указанных операторов связи»[201].

Следует отметить, что закон «О связи» не содержит требований по сроку ответа оператора связи в рамках данного следственного действия, что позволяет оператору связи необоснованно затягивать с ответом. Данное положение ведет к затягиванию сроков предварительного расследования. Подобный законодательный пробел требует устранения.

Необходимо рассмотреть основной недостаток следственного действия в рамках темы исследования, а именно, ограниченность его объекта. В п. 24.1 ст. 24 УПК РФ содержится определение рассматриваемого следственного действия, где содержится и перечень информации, который можно получить при помощи изучаемого следственного действия.

В соответствии с п. 24.1 ст. 5 УПК РФ под «получением информации о соединениях между абонентами и (или) абонентскими устройствами» понимается «получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих

[201] Грошев И.А. Еще раз к проблемам получения информации о соединениях между абонентами и (или) абонентскими устройствами // Актуальные проблемы гуманитарных и естественных наук. 2016. № 2-6. С. 138-139.

идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций».

Такие ученые как Н.А. Архипова[202] и А.В. Шампарова[203], полагают, что информация, получаемая посредством ст. 186.1., ограничивается областью телефонной связи. Однако данную позицию нельзя признать полностью обоснованной.

В настоящий момент действует постановление Правительства РФ от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»[204]. Данный нормативный правовой акт регулирует отношения между абонентом или пользователем, с одной стороны, и оператором связи, оказывающим телематические услуги связи, с другой стороны, при оказании телематических услуг связи. Из анализа данного Постановления следует, что при оказании телематических услуг связи оператор обязан обеспечить предоставление абоненту (пользователю) доступа к сети передачи данных и информационным системам информационно-телекоммуникационных сетей (включая Интернет), прием и передачу телематических электронных сообщений.

Названные положения допускают получение информации о соединениях абонента в сети «Интернет». Так же следует подчеркнуть, что оператор связи является лицом, предоставляющим доступ в сеть «Интернет».

Более того, до появления ст. 186.1 УПК РФ сотрудники органов предварительного расследования получали информацию о соединениях между абонентами и (или) абонентскими устройствами в рамках телематической связи, посредством направления запросов в соответствующие организации на основании ч. 4 ст. 21 УПК РФ.

---

[202] Архипова Н.А. Особенности тактики получения информации о соединениях между абонентами и абонентскими устройствами // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2014. № 12-1. С. 77.

[203] Шампаров А.В. Особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами // Публичное и частное право. 2014. № 1. С. 123.

[204] Постановлением Правительства РФ от 10.12.2007 № 575 «Об утверждении Правил оказания телематических услуг связи» (ред. от 30.12.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/12155536/ (дата обращения: 15.08.2021 г.).

Пример, подтверждающий указанный тезис, наглядно демонстрируется в работе Ю.Н. Соколова[205]. В феврале 2003 г. Д. с целью хищения денежных средств пользователей сети Интернет разместил сайт на информационных ресурсах ТОО «Neolabs», территориально расположенного в г. Алма-Аты Республики Казахстан. Администрирование сайта Д. осуществлял со своего домашнего компьютера, находящегося по улице Уральской в г. Екатеринбурге. Коммутированный доступ в сеть Интернет выполнялся через стационарный телефонный аппарат, установленный по его месту жительства, и через оператора связи ЗАО «Уральские мобильные сети».

На данном сайте Д. разместил заранее скопированные им из сети Интернет с неустановленных носителей фотографические изображения порнографического характера с участием малолетних и несовершеннолетних детей. Пользователи сети, желающие приобрести данную «информацию», должны были перечислить деньги путем электронных платежей на счета WebMoney (на вымышленное лицо), после чего исполнитель заказа получал пароль к FTP-серверу, содержащему порнографические материалы.

В ходе предварительного расследования было установлено, что администрирование сайта, размещенного на ресурсах ТОО «Neolabs», осуществлялось с IP-адреса № 80.78.105.62, принадлежащего ЗАО «Уральские мобильные сети». На основании судебного решения была получена информация о соединениях между абонентами и (или) абонентскими устройствами пользователя с вышеназванным IP-адресом, установлены номер карточки временного доступа, логин, пароль и номер телефона, с которого был осуществлен коммутируемый доступ в сеть Интернет, а также их владелец»[206].

В настоящее время аналогичный способ продолжается использоваться. Так, согласно приговору Урванского районного суда № 1-78/2016 от 23 июня 2016 г. среди сведений, подтверждающих вину лица, можно встретить следующие

---

[205] Соколов Ю.Н. Использование информации о соединениях между абонентами и (или) абонентскими устройствами в ходе предварительного расследования преступлений // Российский следователь. 2011. № 11. С. 20.

[206] Уголовное дело № 369909 // Архив Кировского суда г. Екатеринбурга. 2005. Цит. по: Соколов Ю.Н. Указ. соч. С. 20.

доказательства: «согласно идентификационной информации по IP-адресам по справке Кабардино-Балкарского филиала «Ростелеком» IP-адрес № X принадлежит А., проживающей по адресу Н (л.д.14)»[207]. Или другой пример – приговор Верховного суда Республики Татарстан № № 22-4290/2016 от 28 июня 2016 г. «Согласно справке, предоставленной АО Н, через IP-адрес № К доступ к сети интернет 01 февраля 2015 года в 13 часов 35 минут осуществлен с домашнего адреса X»[208].

Как верно указывают А.А. Варданян и А.А. Цыкора: «В следственной практике не редки случаи, когда потерпевший, свидетель или иное лицо по собственной инициативе получает от оператора связи сведения о детализации входящих и исходящих сигналов с принадлежащего ему абонентского устройства. Данную информацию лица готовы предоставить добровольно, так как имеют личный интерес к результатам расследования. Информация изымается следователем без получения судебного разрешения посредством выемки и осматривается»[209].

Однако через следственное действие «получение информации о соединениях между абонентами и (или) абонентскими устройствами» также получают сведения в сфере телематической связи. Так, согласно Апелляционному определению Верховного суда Республики Башкортостан № 22-2073/2016 от 15.03.2016 года, среди процессуальных действий проводимых для доказывания вины Н., проводилась «выемка в ОАО X, где была изъята информация о соединениях между абонентскими устройствами и установлено, что работа в сети Интернет осуществлялась пользователем А., проживающим по

[207] Приговор Урванского районного суда № 1-78/2016 от 23 июня 2016 // URL: https://sudact.ru/regular/doc/bpgp9HJ5eRVw/ (дата обращения: 23.09.2020).

[208] Приговор Верховного суда Республики Татарстан № 22-4290/2016 от 28 июня 2016 // URL: https://sudact.ru/regular/doc/3n1HEzIZwaLp/ (дата обращения: 23.09.2020).

[209] Варданян А.А., Цыкора А.А. Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединения между абонентами и (или) абонентскими устройствами // Известия тульского государственного университета. 2013. № 4 (Ч. 2). С. 23-24

адресу: ...»[210].

Во всех выше указанных примерах организация связи не предоставляла информацию, связанную с деятельностью абонента непосредственно на самом сайте в сети «Интернет» или отдельном интернет-сервисе. Была предоставлена информация только о характеристике доступа в сеть «Интернет» (дата, время, IP – адрес, ресурс к которому был осуществлен доступ и т. д.), и индивидуализирующих признаках самого абонента (ФИО, место жительства и т. д.).

Выше были приведены три процессуальных способа получения информации о соединениях между абонентами и (или) абонентскими устройствами, которые продолжают использоваться в практической деятельности органов предварительного расследования. На основе вышеизложенного можно констатировать, что законодателю не удалось привести правоприменительную практику к единообразию посредством введения следственного действия, предусмотренного ст. 186.1 в УПК РФ. Стоит отметить, что названное следственное действие является одним из самых трудоемких способов получения информации о соединениях, так как требует составления большего числа процессуальных документов, что значительно замедляет и осложняет ход предварительного расследования.

Сведения, получаемые посредством следственного действия «получения информации о соединениях между абонентами и (или) абонентскими устройствами», представляют собой статистические данные о характере контактов в сети телефонной связи и телекоммуникационной сети «Интернета», без содержания коммуникаций, что также является достаточно практичным при производстве по уголовному делу.

Однако необходимо отметить, что с 01.07.2018 года положение пп. 1 п. 1 ст. 64 закона «О связи» оператор связи обязан хранить и предоставлять

---

[210] Апелляционное определение № 22-2073/2016 Верховного суда Республики Башкортостан от 15 марта 2016 // URL: https://nalogcodex.ru/sud_pract/sou/apellyatsionnoe-opredelenie- verhovnogo- suda-respubliki -bashkortostan- (respublika-bashkortostan) -ot-15.03.2016-_-22-2073_2016 (дата обращения: 23.09.2020).

правоохранительным органам информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий. Аналогичная обязанность, согласно под. 1 п. 3 ст. 10.1 закона Об информации предусмотрена и для организаторов распространения информации в сети «Интернет».

Представляется, что указанные выше обязанности могут привести к утрате практической значимости следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами», так как будет возможно одновременно получать содержание всех видов мультимедийных сообщений (в том числе телефонных переговоров), передаваемых по сетям электросвязи, а также информацию о соединениях между абонентскими устройствами.

Рассматривая особенности производства «электронно-технических» следственных действий, направленных на получение информации, передаваемой посредством электросвязи, можно прийти к следующему выводу. Во-первых, телематическая, телефонная и иные виды связи, основанные на электромагнитных свойствах материи, интегрируются в единую систему электросвязи. Данный факт не был учтен законодателем при реформировании УПК РФ, что ограничило многообразие сведений, которые допустимо собирать с помощью следственных действий. Так, объект следственного действия «контроль и запись переговоров» ограничивается информацией, передаваемой лишь по телефонной связи.

Во-вторых, чрезмерная формализация «электронно-технических» следственных действий создает пробелы в возможности получать и использовать многообразие видов электронной информации, не указанной в УПК РФ. Предмет следственного действия «наложение ареста на почтово-телеграфные отправления» ограничен электронными сообщениями. Юридическая конструкция «получение информации о соединениях между абонентами и (или) абонентскими устройствами» не дает однозначного понимания о допустимости получения

статистических данных в области телематической связи, а также об их видах (геолокация, логин и пароль пользователя интерн-сервиса).

В-третьих, в УПК РФ отсутствуют нормы, регламентирующие порядок модификации электронной информации в интересах предварительного расследования, к примеру, для блокировки доступа лица к учетной записи электронной почты (наложение ареста на электронную почту). Положение о возможности производить осмотр и выемку электронных сообщений в учреждениях связи (ч. 7 ст. 185 УПК РФ) не согласуется с юридической конструкцией следственного действия «наложения ареста на почтово-телеграфные отправления», которое рассчитано именно на материальные почтово-телеграфные отправления.

2.3. Использование в доказывании результатов розыскной деятельности, осуществляемой с применением электронных средств, следователем и органом дознания

Розыскная деятельность является частью работы следователя, органа дознания. Такая деятельность осуществляется с помощью оперативно-розыскных мероприятий (ст. 6 Федерального закона «Об оперативно-розыскной деятельности») и следственных действий поискового характера. Электронные средства могут служить в данном случае вспомогательным инструментом, и порядок их применения требует законодательного закрепления в УПК РФ и других законах. Многие вопросы применения уголовно-процессуального и оперативно-розыскного законодательства нуждаются в использовании унифицированных подходов.

Уровень взаимопроникновения различных видов коммуникации с использованием электронных информационных технологий достиг настолько высокого уровня, что возникает потребность в разработке единого механизма получения сведений, передаваемых по сетям электросвязи, позволяющих установить наличие или отсутствие обстоятельств, подлежащих доказыванию по уголовному делу.

Результаты оперативно-розыскной деятельности могут быть представлены следователю, органу дознания в электронном виде. В основе данных материалов может лежать электронная оперативная (оперативно-розыскная) информация, которая является разновидностью оперативной информации, отличительной особенностью которой является то, что она содержится на электронных носителях[211].

Электронная информация как результат проведения оперативно-розыскных мероприятий. Для получения такого рода информации могут проводиться такие мероприятия, как: снятие информации с технических каналов связи, прослушивание телефонных переговоров, опрос и наблюдение (с применением технических средств фиксации), получение компьютерной информации. Не исключено, что и при проведении других ОРМ электронная информация может попасть во внимание оперативных сотрудников. Например, в ходе обследования помещений, зданий, сооружений, транспортных средств или наведения справок, но это не является их основной задачей. В любом случае электронная оперативно-розыскная информация должна иметь свой материальный носитель[212]. Именно так она может быть в дальнейшем реализована в доказывании по уголовным делам.

Электронная оперативная информация должна быть подвергнута проверке и оценке в соответствии с требованиями, предъявляемыми оперативно-розыскным и уголовно-процессуальным законодательством. Значимость такой информации, как и информации, полученной в ходе уголовно-процессуальной деятельности, при наглядном различии в источниках и средствах собирания зависит от их оценки с точки зрения относимости, достоверности и допустимости. Требование допустимости имеет отношение не к самой информации, а к ее носителю, способам получения и закрепления.

---

[211] Зуев С.В., Бахтеев Д.В, Вехов В.Б., Зазулин А.И., Пастухов П.С., Тушанова О.В. Электронные доказательства в уголовном судопроизводстве: учеб. Пособие. М.: Издательство Юрайт. 2020. С. 160.

[212] Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: теория, история, практика. № 4. 2016. С. 49.

Проблема использования результатов оперативно-розыскной деятельности в уголовном процессе либо в качестве доказательств, либо в доказывании по уголовному делу – это чисто российская проблема[213]. Законодательство ряда зарубежных стран (США и Великобритании, в меньшей степени Германии и Франции) предусматривает два порядка сбора доказательств — это производство следственных действий и проведение оперативно-розыскных мероприятий. Негласные следственные действия предусмотрены уголовно-процессуальными законами Украины, Республики Казахстан, . перечень тайных следственных действий, что и есть оперативно-розыскные мероприятия, содержит и УПК Грузии.

В рамках изложенного, достаточно любопытными представляются нормы Уголовно-процессуального кодекса Федеральной Республики Германии (далей УПК ФРГ)[214].

Так, §§100a/b УПК ФРГ позволяет производить «контроль и запись телекоммуникаций». Положения, установленные в § 100a УПК ФРГ, применяются в отношении любого вида телекоммуникации, включая не только обычные виды коммуникации по телефону и посредством телеграфии, но и передачу информации, генерированной с помощью компьютерной техники, через интернет, а также сообщения, передаваемые по факсу. Под контроль и запись телекоммуникаций подпадают лишь случаи, в которых информация контролируется и записывается в процессе её передачи. К этим случаям причисляется также «промежуточное хранение» информации на сервере оператора[215]. В остальных случаях, когда электронную информацию необходимо осмотреть непосредственно на электронном носителе информации владельца, производится выемка с получением судебного решения в порядке установленном в §§ 94-100 УПК ФРГ.

---

[213] Агутин А.В. Место оперативно-розыскной деятельности в доказывании по уголовным делам // Следователь. № 2. 2000. С. 51.

[214] Уголовно-процессуальный кодекс Федеральной Республики Германии от 12.09.1950 // Официальный сайт публикации документа. URL: http://www.gesetze-im-internet.de/englisch_stpo/index.html. (дата обращения: 10.07.2021 г.).

[215] Головненков П.В. Указ. соч. С. 57-58.

Для производства «контроля и записи телекоммуникаций» необходимо получить письменное судебное распоряжение, в случаях, не терпящих отлагательства, допустимо производить процессуальное действие с распоряжения прокурора с последующим судебным санкционированием в течение 3 дней[216]. При этом, в соответствии с §100b, в распоряжении (постановлении) о производстве «контроля и записи телекоммуникаций» указываются идентификационные данные телекоммуникационного соединения. На основании распоряжения о производстве «контроля и записи телекоммуникаций» каждое лицо, оказывающие телекоммуникационные услуги или участвующего в реализации, обязано оказать помощь сотруднику правоохранительного органа в соответствии с положением законодательства о телекоммуникации, для производства «контроля и записи телекоммуникаций. Период, в течение которого производится процессуальное действие, составляет 3 месяца с возможностью продления еще на 3 месяца.

Названная норма является достаточно прогрессивной и может использоваться при развитии российского уголовно-процессуального законодательства. Следует отметить, что российский законодательный вектор регулирования правоотношений в области электросвязи создает предпосылки для практической реализации единого уголовно-процессуального механизма получения информации, передаваемой по сетям электросвязи.

5 мая 2014 года Федеральным законом № 97-ФЗ[217] в закон Об информации были внесены дополнения, направленные на создание правового поля по взаимодействию между организаторами распространения информации в сети «Интернет» и правоохранительными органами. Законодателем в п. 3 ст. 10.1. для организатора распространения информации в сети «Интернет» была предусмотрены обязанность по хранению на территории РФ информации о

---

[216] Там же. С. 58.

[217] Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» // Российская газета. 2014. 07 мая.

фактах приема, передачи или доставки электронного сообщения в течение одного года, а также хранения содержания электронного сообщения в течение шести месяцев с момента приема, передачи или доставки.

В соответствии с п. 3.1. ст. 10.1. указанного закона взаимодействие осуществляется между организаторами распространения информации в сети «Интернет» и органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Исходя из содержания п. 4 ст. 10.1. закона Об информации организатор распространения информации в сети «Интернет» обязан обеспечивать техническую возможность органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, для проведения мероприятий, связанных с реализацией возложенных на них функций.

Дополнительные обязанности для организаторов распространения информации в сети «Интернет» были предусмотрены Федеральным законом от 7 июля 2016 года № 374-ФЗ[218]. Данные обязанности выражаются в предоставлении информации органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, необходимой для декодирования электронных сообщений.

Федеральным законом от 29 июля 2017 года № 241-ФЗ[219] в ст. 4.2. закона Об информации была введена новая подкатегория организатора распространения информации в сети «Интернет» – организатор сервиса обмена мгновенными сообщениями. Исходя из законодательного определения, данная категория охватывает лиц, организующих функционирование таких сервисов, как «Whatsapp», «Wechat», «Telegram» и других интернет-мессенджеров.

В соответствии со ст. 10.1. ч. 4.2. закона Об информации организатор

---

[218] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 08 июля.

[219] Федеральный закон от 29.07.2017 № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» // Российская газета. 2017. 04 августа.

сервиса обмена мгновенными сообщениями обязан осуществлять идентификацию пользователей сервиса обменными сообщениями по абонентскому номеру оператора подвижной радиотелефонной связи. Организатор сервиса обмена мгновенными сообщениями должен иметь возможность в течение суток ограничивать передачу электронных сообщений, содержащих информацию, распространение которой в Российской Федерации запрещено, по требованию уполномоченного федерального органа исполнительной власти.

Порядок взаимодействия между организатором распространения информации в сети «Интернет» с органом, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, определяется Постановлением правительства РФ от 31 июля 2014 года № 743[220]. Нормативно-правовой акт определяет организационные программно-технические стороны взаимодействия. Особый интерес вызывает п. 8 указанного Постановления правительства РФ, согласно которому организатор распространения информации в сети «Интернет» предоставляет удаленный доступ к системе для получения информации, предусмотренной п. 3 и 4.1. ст. 10.1. закона Об информации.

Необходимо обратить внимание на Постановление правительства РФ от 31 июля 2014 года № 759[221]. Данный нормативно-правовой акт, детализирует перечень сведений, которые обязан хранить и предоставлять организатор распространения информации в сети «Интернет» в соответствии с п. 3 закона Об

---

[220] Постановление Правительства РФ от 31.07.2014 № 743 «Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации» (ред. от 01.12.2018) // Гарант: справ. правовая система // URL: http://base.garant.ru/70709018/ (дата обращения: 15.08.2021 г.).

[221] Постановление Правительства РФ от 31.07.2014 № 759 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации» (ред. от 04.08.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/70710174/ (дата обращения: 10.05.2021 г.).

информации. Состав информации, подлежащей хранению организатором распространения информации в сети «Интернет», определяется п. 3 Постановления правительства № 759 и включает сведения не только о фактах приема, передачи, обработки электронных сообщений, но и данные о произведенных денежных операциях, а также информацию, позволяющую идентифицировать пользователя и определять его активность на интернет-сервисе. К примеру, сведения, вносимые пользователем при регистрации на интернет-сервисе (номер телефона, адрес электронной почты, сетевой адрес и др.), время и сетевой адрес авторизации пользователя и так же иные сведения, предусмотренные Постановлением правительства.

Рассмотренные нормативно-правовые акты регулируют отношения между организатором распространения информации в сети «Интернет» с органом, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации в узком поле правоотношений, возникающих в сфере телематических услуг связи. Однако для того, чтобы физически получить возможность воспользоваться интернет-сервисом, в каждом случае необходимо прибегнуть к услугам оператора связи, предоставляющего определенному лицу услуги электросвязи (тематической и (или) телефонной).

В соответствии с пп. 1 п. 1 ст. 64 Закона «О связи» оператор связи обязан хранить в течение трех лет на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки всех видов коммуникации[222],проходящих с использованием электросвязи. При этом в соответствии пп. 2 п. 1 ст. 64 Закона «О связи» содержание коммуникации, производимой с помощью электросвязи, оператор связи обязан хранить на территории Российской Федерации в течение шести месяцев.

В свою очередь в п. 5 ст. 64 Закона «О связи» предусмотрено, что «при проведении уполномоченными государственными органами следственных действий операторы связи обязаны оказывать этим органам содействие в

[222] Голосовую информацию, текстовые сообщения, изображение, звуков, видео- или иных сообщений пользователей услугами связи.

соответствии с требованиями уголовно-процессуального законодательства». Фактически это единственная норма, обязывающая оператора связи оказывать содействие в рамках уголовно-процессуального законодательства.

Таким образом, рассмотрев нормативно-правовые акты, регулирующие взаимодействие правоохранительных органов с операторами связи и организаторами распространения информации с сети «Интернет», можно сделать ряд выводов. Во-первых, обязанность по предоставлению информации правоохранительным органам со стороны операторов связи и организаторов распространения информации в сети «Интернет» закреплена в федеральном законодательстве и подзаконных нормативно-правовых актах, что свидетельствует о наличии правового поля.

Во-вторых, законодатель предусмотрел обязанность взаимодействия между операторами связи и органами предварительного расследования, а также органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. При этом обязательность взаимодействия со стороны организаторов распространения информации в сети «Интернет» была законодательно установлена только по отношению к органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации.

Если отсутствие органов, осуществляющих предварительное расследование в рамках взаимодействия с операторами связи и организаторами распространения информации в сети «Интернет» на уровне подзаконного регулирования, можно объяснить отсутствием необходимости технического взаимодействия[223], то отсутствие органов предварительного расследования в качестве субъекта взаимодействия с организаторами распространения информации в сети «Интерне» в рамках ст. 10.1. Закона Об информации является законодательным

[223] Контроль и запись переговоров может осуществляться специальными уполномоченными на то лицами из числа операторов предприятия связи или специальным оперативно-техническим подразделением органа дознания. См.: Морозова Е.В., Андровник Н.А. Тактика контроля и записи переговоров: проблемы теории и практики // Вестник уральского института экономики: управление и право. 2013. № 4. С. 17.

пробелом. При условии, что в процессе расследования уголовного дела возникает и реализуется потребность в получении сведений, которыми обладают организаторы распространения информации в рамках уголовно-процессуального законодательства.

В-третьих, перечень сведений, указанных в ст. 10.1. Закона Об информации и в п. 1 ст. 64 Закона «О связи», которые обязаны хранить и предоставлять уполномоченным органам операторы связи и организаторы распространения информации в сети «Интернет», является ограниченными.

Представляется, что, помимо указанной в нормах информации, органы, осуществляющие предварительное расследование, могут заинтересовать геолокационные данные пользователя как в ретроспективе, так и в реальном времени. Более того, многие приложения, которые используются на электронных носителях, просят разрешения у пользователя для доступа к системам устройства, позволяющим определить местоположение, что также может быть использовано в рамках предварительного расследования[224].

Важной особенностью является то, что практически каждый интернет-сервис (электронная почта, социальная сеть и т. д.) хранит всю информацию пользователей в «облаке» неограниченное количество времени. Если пользователь интернет-сервиса не предпринял действия по удалению информации, то сохраняется возможность получить доступ к этим данным. Не исключена возможность того, что у правоохранительных органов возникнет потребность получить доступ к сведениям, хранение которых не попадает под сроки, установленные федеральным законодательством.

Введенные законодателем обязательства по сохранению содержания телекоммуникаций на территории РФ со стороны операторов связи и организаторов распространения информации в сети «Интернет» обусловлены

---

[224] В средствах массовой информации неоднократно освещалась информации о том, что приложения собирают гелокационные данные. См.: Фитнес-приложение раскрыло расположение военных баз США // URL: https://www.popmech.ru/technologies/news-407982-fitnes-prilozhenie-raskrylo-raspolozhenie-voennyh-baz-ssha/ (дата обращения: 20.02.2020); См.: Приложение Uber следит за своими пользователями // URL: https://tjournal.ru/38587-byvshiy-sotrudnik-uber-obvinil-kompaniyu-v-slezhke-za-polzovatelyami (дата обращения: 20.02.2020).

проблемами взаимодействия между организаторами распространения информации в сети «Интернет», которые находятся за границей, и правоохранительными органами РФ[225].

Более того, получение электронной информации может быть обусловлено политикой частной организации. Ярким примером служит ситуация 2018 года с интернет-мессенджером «Telegram», владелец которого отказался передавать Российской Федерации ключи дешифровки сообщений[226].

Поэтому необходимо предусмотреть такой уголовно-процессуальный механизм наложения ареста на электронные сообщения или контроль электронной информации, не включая в данный механизм организатора распространения информации в сети «Интернет».

Размышляя подобным образом, важно коснуться вопроса трансграничности «киберпространства». Согласно ч. 1 ст. 2 УПК РФ, производство по уголовному делу на территории Российской Федерации независимо от места совершения преступления ведется в соответствии с УПК РФ, если международным договором Российской Федерации не установлено иное. В свою очередь ч. 2 ст. 2 определяет, что действие уголовно-процессуального закона распространяется на воздушное, морское или речное судно под флагом РФ, находящееся за пределами территории РФ, но приписанное к порту РФ. В соответствии с ч. 3 ст. 2 УПК РФ отдельные процессуальные действия, могут проводиться за пределами территории Российской Федерации, в случаях предусмотренных ст. 12 УК РФ.

Таким образом, действие уголовно-процессуального закона в пространстве определяется физическими, материальными границами или лицом, которое существует в материальном мире. Данное положение вступает в противоречие с таким явлением, как «киберпространство», так как оно не имеет материальных границ.

---

[225] Важенин В.В., Имаков Т.З. Проблемы противодействия экстремизму в сети «Интернет» // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2015. № 1. С. 21; Хайдаров А.А. Указ. соч. С. 40.

[226] Дуров не отдает ключи от Telegram. Что будет с мессенджером? // URL: https:// hitech-vesti-ruampproject.org (дата обращения: 22.02.2020).

Например, производя осмотр изъятого мобильного телефона, можно получить доступ не только к информации, которая хранится непосредственно в памяти электронного устройства, но и к информации, которая расположена на серверах удаленно в «облаке». Необходимо учитывать, что организация, владеющая и управляющая серверами, может физически находится в одном государстве, а серверы расположены совершенно в другом.

Не исключена и такая ситуация, когда лицо совершило преступление в Российской Федерации или против интересов Российской Федерации, но находится за пределами российской территории и есть необходимость исследовать электронное устройство удаленно от лица. На данное обстоятельство обращал внимание И.И. Карташов, указывая, что «УПК РФ оставляет открытым вопрос о возможности обыска в компьютерных сетях, если они находятся за пределами обыскиваемых помещений»[227].

Таким образом, достаточно сложно определить, как будут реализовываться нормы, регулирующие действие уголовно-процессуального закона в пространстве относительно «киберпространства».

На данную проблему уже было обращено внимание в международном праве. Как отмечает Э.Л. Ансельмно: «Новые особенности пространства, обусловленные Интернетом, указывают на неэффективность понятия географической территориальности в международном праве, поскольку в киберпространстве ослабевает связь с физическим местоположением… По сути, внетерриториальность создает конфликт в сфере права государств на юрисдикцию»[228].

Обосновывая свое умозаключение, автор приводит следующий пример по делу компании «Yahoo!» против Франции. На сайте компании «Yahoo!» была выставлена реликвия времен нацисткой Германии. Во Франции был подан иск

---

[227] Карташов И.И. «Цифровые доказательства» в уголовном процессе // Центральный научный вестник. 2016. № 15. С. 25.

[228] Ансельмно Э.Л. Киберпространство в международном законодательстве: опровергает ли развитие интернета принцип территориальности в международном праве? // Экономические стратегии. 2006. № 2. С 25-26.

против «Yahoo!» в связи с тем, что подобные предметы запрещено реализовывать на территории Франции. В свою очередь «Yahoo!» подал встречный иск на территории США, так как юридический адрес компании был в штате Калифорния. Французский суд указал, что компания должна исключить доступ граждан Франции к информации, расположенной на сайте. В тоже время суд США пришел к выводу, что определения национального французского суда не имеют юридической силы в отношении американских компаний, которые физически расположены на территории США. В свою очередь компания «Yahoo!» заявила, что не разрабатывала сайт для какого-то государства. Поскольку сайт не является французским, «Yahoo!» не нарушила законов как Франции, так и США[229].

На рассматриваемую проблему обращает внимание и А.Л. Осипенко, который полагает, что от разрешения вопроса о юрисдикции конкретного государства на раскрытие трансграничного преступления зависят пределы полномочий национальных оперативно-розыскных органов в сетевом информационном пространстве, а, следовательно, и допустимость осуществления действий разведывательно-поискового характера[230].

Подтверждая данное суждение, автор приводит следующий пример. В 2000 году ФБР США произвело удаленное обследование компьютеров, находящихся на территории России, которые использовались российскими хакерами в противоправных целях. Данные, полученные агентами ФБР, были использованы в качестве доказательств в судебном процессе. Однако проведение подобных мероприятий вызвало возмущение со стороны ФСБ России, так как ФБР проигнорировали необходимость обращения с запросом к правоохранительным органам России[231].

В юридической литературе рассматриваются различные точки зрения

---

[229] Ансельмно Э.Л. Указ соч. С. 30.

[230] Осипенко А.Л. О правовом регулировании действий оперативно-розыскных органов при раскрытии трансграничных преступлений в сети Интернет // Оперативник (сыщик). 2011. № 2. С. 20.

[231] Там же С. 20 .

относительно решения вопроса о юрисдикции. Их обобщение позволяет выделить несколько подходов. Согласно первому подходу, киберпространство надлежит воспринимать как общую территорию, по аналогии с открытым морем, космосом, Антарктикой. Правила по использованию киберпространства должны быть аналогичны правилам действующим в отношении общих территорий[232].

Критически оценивая данный подход, А.Л. Осипенко указывает, что вряд ли возможно сегодня всерьез обсуждать вопрос о признании киберпространства суверенной территорией с независимым внутренним правовым регулированием… последствия противоправных действий наступают не только в «киберпространстве», но и физическом мире, затрагивая интересы, защищаемые национальным законодательством конкретного государства. Исходя из этого, право на осуществление уголовного преследования должно распространяться на сетевые события, которые являются территориально неопределенными, но имеющие последствия на территории конкретного государства[233].

Общественно-опасные деяния, совершенные на физически существующих «общих» международных территориях, также могут привести к реальным негативным результатам для определенного государства, что соотносится с деятельностью в киберпространстве.

Второй подход можно обобщить в необходимость определения юрисдикции государства, исходя из места совершения преступления или наступления последствий общественно-опасного деяния[234].

Названный аспект достаточно сложно реализовать на практике. Несмотря на то, что существуют технологии, которые позволяют достаточно точно определить, с какой территории произошел выход в сеть «Интернет» с целью совершения преступления[235], есть общедоступные VPN-программы,

---

[232] Ансельмно Э.Л. Указ соч. С. 25.

[233] Осипенко А.Л. Указ. соч. С. 21.

[234] Осипенко А.Л. Указ. соч. С. 21-22.; Искевич И.С., Кочеткова М.Н., Попов А.М. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект // Проблемы правоохранительной деятельности. 2016. № 2. С. 56-57.

[235] Там же С. 56.

позволяющие скрыть источник выхода или намеренно указать неверный территориальный адрес.

Не исключена и такая ситуация, когда «проникновение» в компьютерную сеть банка Германии с целью совершения преступления совершает гражданин Франции, который перемещается по территории Китая. В данном случае представляется проблематичным определить место совершения преступления.

Определение юрисдикции по общественно-опасным последствиям, также может представлять значительные трудности. Например, к юрисдикции какой страны можно отнести расследование преступления, связанного с использованием вируса «Wanna Cry», который заразил компьютеры в более чем 70 странах мира?

Третий подход заключается в том, что юрисдикция государства и правомерность получения доказательств в «киберпространстве» определяется международными договорами и нормативно-правовыми актами. Данная модель реализуется практически и рассматривается в научной среде как основной вектор правового регулирования[236].

На сегодняшний день действует Конвенция о преступности в сфере компьютерной информации ETS №185 от 23 ноября 2001 года[237]. Международный документ содержит нормы, подлежащие имплементации в национальное законодательство участников конвенции. Нормы конвенции определяют совокупность составов преступлений, а также перечень процессуальных мероприятий, направленных на трансграничное получение компьютерной информации, в качестве доказательства по уголовному делу.

Международное сотрудничество определяется главой III названной конвенции. Статья 32 регулирует трансграничный доступ к охраняемой законом информации. В соответствии с п. а ст. 32 Конвенции сторона-участник имеет

---

[236] Осипенко А.Л. Указ. соч. С. 23; Искевич И.С. Указ. соч. С. 57; Карташов И.И. Указ. соч. С. 57.

[237] Конвенция о преступности в сфере компьютерной информации ETS от 23.11.2001 № 185 (г. Будапешт) // Гарант: справ. правовая система // URL: http://base.garant.ru/4089723/ (дата обращения: 13.08.2021 г.).

право без согласия другого государства получать доступ к общедоступным компьютерным данным, а согласно п. b ст. 32 Конвенции сторона-участник имеет право без согласия другого государства-участника «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».

На основании ст. 27 взаимодействие государств-участников названной конвенции осуществляется через направление запросов о взаимной помощи, компетентному органу, который определяется государством-участником конвенции. Статья 35 обязывает создать контактный центр, который будет работать 24 часа в сутки 7 дней в неделю для оказания неотложной помощи при расследовании уголовного дела. Изложенное позволяет сделать вывод, что государствам-участникам необходимо получать разрешение о производстве трансграничных следственных действий.

В настоящий момент участниками данной конвенции являются не только страны Европы, но и другие государства, к примеру, США, Израиль, Япония, Канада и др. (общее количество участников 56). Российская Федерация стала участником Конвенции в 2005 году, но уже в 2008 году вышла из Конвенции (Распоряжение Президента РФ № 144-рп от 22 марта 2008).

Следует согласиться, что присоединение к названной конвенции сказалось бы положительно на возможности российских правоохранительных органов производить трансграничные следственные действия, однако не разрешит все поставленные проблемы в рамках российского уголовно-процессуального закона.

Во-первых, направление запроса о правовой помощи в порядке ст. 453 УПК РФ является сложным процессуальным действием, которое производится с участие высшего руководства органов исполнительной и судебной власти Российской Федерации. Более того, направление запроса о правовой помощи и исполнение данного запроса иностранным государством может занимать достаточно длительное время.

Представляется, что достаточно сложно реализовать международный механизм, позволяющий получать электронные доказательства по каждому уголовному делу, которое находится в производстве. Следует предположить что необоснованно будет инициировать запрос о международной правовой помощи, например, в США, для предоставления электронной переписки пользователя интернет-сервиса, когда отсутствует согласие лица, имеющего полномочия на раскрытие данных, а сама электронная информация хранится удаленно в «облаке». При этом сам интернет-сервис или лицо могут физически находиться в иностранном государстве.

Исходя из этого допустимыми являются действия, направленные на получение электронной информации с использованием возможностей национальной правоохранительной системы, когда электронное устройство уже изъято или существует техническая возможность произвести процессуальные действия, направленные на получение электронной информации «дистанционно», с учетом соблюдения прав и безопасности третьих лиц.

Во-вторых, исполнение Конвенции «О преступности в сфере компьютерной информации» может быть обусловлено геополитической обстановкой, которая в настоящий момент является неблагоприятной для Российской Федерации.

В-третьих, как уже отмечалось выше, получение электронной информации может быть обусловлено политикой частной организации.

Таким образом, международный механизм трансграничного получения электронной информации юридически сконструирован так, что в большинстве случаев необходимо получать согласие страны-участника Конвенции «О преступности в сфере компьютерной информации». Подобное обстоятельство является негативной стороной международного регулирования действия уголовно-процессуального закона в «киберпространстве», так как потребность в получении электронной информации при производстве по уголовному делу является повсеместной, а взаимодействие в рамках международной правовой помощи будет значительно замедлять производство по уголовному делу.

Поэтому следует предусмотреть возможность производства следственных

действий в рамках уголовно-процессуального закона Российской Федерации. Пользователи сети «Интернет» не знают и не интересуются физическим местонахождением интернет-сервиса, которым они пользуются. Поэтому в настоящее время невозможно установить объем юрисдикции конкретного государства в определенной области «киберпространства».

Исходя из этого, «киберпространство» необходимо рассматривать с точки зрения режима общих международных территорий. Однако при этом необходимо учитывать, что производство процессуальных действий в «киберпространстве» может затрагивать права и интересы, а также аппаратно-программные средства граждан и организаций, которые могут находиться в любой точке планеты.

Таким образом, необходимо определить возможную степень «проникновения» в информационно-телекоммуникационную сеть (социальную сеть, базы данных и т. д.), с учетом интересов третьих лиц (государства, распространителя информации в сети «Интернет»), понимая, что «киберпространство» обладает режимом общих международных территорий.

В ст. 2 Конвенции об открытом море от 29 апреля 1958 года и ст. 3 договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, от 27 января 1967 года, определяется свобода доступа и использования международных территорий при условии обеспечения международного мира и безопасности.

Механизм получения информации через изъятый электронный носитель является распространенным явлением в уголовно-процессуальной деятельности (США, Канада, Россия, Бельгия и т. д.). Более того, к примеру, в Бельгии предусмотрена уголовная ответственность за отказ в сотрудничестве при производстве «электронного обыска»[238].

Основываясь на имеющейся практике, можно прийти к выводу, что существующий механизм сбора информации через изъятый электронный

[238] Сергеев М.С. Правовые основы применения электронной информации и электронных носителей информации в уголовном судопроизводстве: дисс. … кан. юрид. наук. Казань, 2018. С. 93-114.

носитель не вызывает противоречий в международных отношениях, так как обеспечивает соблюдение международного мира и безопасности при производстве трансграничных действий в «киберпространстве».

Скорее всего, данная ситуация обусловлена тем, что доступ через изъятое электронное устройство, производится только к определенной области «киберпространства», которая относится к конкретному лицу. В случаях, когда может возникнуть необходимость проведения трансграничных следственных действий без изъятого электронного носителя информации (удаленный обыск), необходимо учитывать область «киберпространства», которая будет затрагиваться при производстве трансграничных следственных действий.

Представляется верным, что объектом трансграничных следственных действий может выступать только индивидуально-определенная область «киберпространства», которая привязана к лицу посредством данных, позволяющих его идентифицировать (сетевой адрес, электронная почта и т. д.). Если производство по уголовному делу ведется в отношении неустановленного лица, то допустимо производить трансграничные следственные действия по идентификационным данным пользователя, при наличии достаточных сведений, указывающих на то, что идентификационные данные относятся к лицу, совершившему преступление.

При этом допустимо выходить за пределы киберпространства, привязанному к физической памяти электронного носителя информации, если имеются достаточные данные полагать, что могут быть обнаружены сведения, имеющие отношение к уголовному делу. Данный принцип производства трансграничных следственных действий можно обозначать как «электронное домино».

Например, в ходе производства «дистанционного обыска» компьютера у следователя возникает предположение, что чертежи созданного взрывного устройства или переписки между соучастниками преступления содержатся в «облачном сервисе» (Яндекс, Google диск, WhatsApp Web). При наличии технической возможности допустимо исследовать область киберпространства,

даже если есть необходимость преодолеть защиту профиля «облачного хранилища». Исследование киберпространства может вестись и в обратном направлении, начиная с «облачного сервиса».

Недопустимо производить трансграничные следственные действия в тех случаях, когда может создаться угроза безопасности какого-либо государства. К примеру, интернет-сервис, который используется гражданами на территории конкретного государства (национальный интернет-банк, госуслуги и т. д.). В данном случае следственное действие необходимо произвести в рамках международной правовой помощи.

Таким образом, уголовно-процессуальная юрисдикция государства в «киберпространстве» в настоящий момент не получила должного регулирования. Прежде чем приступать к разработке законопроекта по соответствующему изменению территориального действия уголовно-процессуального законодательства, необходимы дополнительные исследования обозначенной проблемы. Систематизация существующих научных теорий, позволит определить основной вектор совершенствования действия уголовно-процессуального законодательства в «киберпространстве». Среди существующих теорий наиболее практичной представляется позиция, что по своим юридическим свойства «киберпространство» наиболее похоже на общие международные территории. При производстве трансграничных следственных действий необходимо руководствоваться положением ст. 2 УПК РФ и обозначенным принципом «электронного домино».

На основе выявленных недостатков в производстве «информационно-технологических» следственных действий предлагается из ст. 185 УПК РФ исключить ч. 7, а п. 14.1. ст. 14.1. УПК РФ изложить в следующей редакции: «контроль электросвязи – мониторинг голосовой информации, изображения, звука, видео-, иных форм телекоммуникации пользователей электросвязи, получение содержания телекоммуникации, в установленных федеральным законом случаях, от операторов связи и организаторов распространения информации в сети «Интернет», арест телекоммуникаций».

Дополнить ст. 2 Федерального закона от 07 июля 2003 года «О связи» № 126-ФЗ п. 29.1 следующего содержания: «телекоммуникация – прием, передача, доставка и (или) обработка голосовой информации, изображения, звука, видео-, и иных форм электронной информации пользователей электросвязи».

Часть 5 ст. 165 УПК РФ изложить в следующей редакции: «В исключительных случаях, когда производство осмотра жилища, обыска и выемки в жилище, обыск электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи, личного обыска, контроля электросвязи, а также выемки заложенной или сданной на хранение в ломбард вещи, наложение ареста на имущество, указанное в части первой статьи 104.1 Уголовного кодекса Российской Федерации, не терпит отлагательства, указанные следственные действия могут быть произведены на основании постановления следователя или дознавателя без получения судебного решения. В этом случае следователь или дознаватель не позднее 3 суток с момента начала производства следственного действия уведомляет судью и прокурора о производстве следственного действия. К уведомлению прилагаются копии постановления о производстве следственного действия и протокола следственного действия для проверки законности решения о его производстве. Получив указанное уведомление, судья в срок, предусмотренный частью второй настоящей статьи, проверяет законность произведенного следственного действия и выносит постановление о его законности или незаконности. В случае, если судья признает произведенное следственное действие незаконным, все доказательства, полученные в ходе такого следственного действия, признаются недопустимыми в соответствии со статьей 75 настоящего Кодекса».

Статью 186 УПК РФ изложить в следующей редакции:

«Статья 186. Контроль электросвязи

1. При наличии достаточных оснований полагать, что сведения, передаваемые подозреваемым, обвиняемым и другими лицам посредством электросвязи могут иметь значение для уголовного дела, допускается

производство контроля данных сведений в порядке, установленном статьей 165 настоящего Кодекса.

2. При наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких родственников, родственников, близких лиц получение, исследование и запись телекоммуникации допускается по письменному заявлению указанных лиц, а при отсутствии такого заявления – на основании судебного решения.

3. В ходатайстве следователя о производстве контроля электросвязи:

1) уголовное дело, при производстве которого необходимо применение данной меры;

2) основания, по которым производится данное следственное действие;

3) фамилия, имя и отчество лица, телефонные номер, адрес электронной почты, доменное имя, а так же иную информацию позволяющую идентифицировать пользователя электросвязи:

4) период осуществления контроля электросвязи;

5) действия по контролю электросвязи или их совокупность, необходимые в рамках контроля электросвязи: мониторинг телекоммуникации, получение телекоммуникации от операторов связи и (или) организаторов распространения информации в сети «Интернет», наложение ареста на телекоммуникации.

6) наименование органа, которому поручается техническое осуществление контроля электросвязи.

4. Постановление о производстве контроля электросвязи направляется в соответствующий орган.

5. В рамках одного постановления допустимо производить как одно действие по контролю электросвязи, так и их совокупность: мониторинг телекоммуникации, получение телекоммуникации от операторов связи и (или) организаторов распространения информации в сети «Интернет», наложение ареста на телекоммуникации.

6. Контроль электросвязи может быть установлен на срок до 6 месяцев. Ретроспективный период получения содержания телекоммуникации от оператора

связи и (или) организатора распространения информации в сети «Интернет» определяется федеральным законодательством. Контроль электросвязи прекращается по постановлению следователя, с обязательным уведомлением об этом суда, принявшего решение о наложении ареста, и прокурора, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу. При завершении производства контроля электросвязи возобновляется доступ пользователя к функциональным возможностям коммуникационного интернет-сервиса путем восстановления данных авторизации.

7. Арест телекоммуникаций состоит в ограничении доступа к электронным сообщениям пользователя электросвязи путем модификации данных авторизации, необходимых для получения доступа к функциональным возможностям коммуникационного интернет-сервиса. Модификацию данных авторизации пользователя коммуникационного интернет-сервиса производит организация, исполняющая постановление о контроле электросвязи. Организация, исполняющая постановление о контроле электросвязи, предоставляет следователю данные для авторизации в коммуникационном интернет-сервисе в качестве пользователя, в отношении которого был произведен арест телекоммуникаций, для последующего осмотра содержания электронных сообщений.

8. Следователь вправе самостоятельно произвести арест телекоммуникаций пользователя электросвязи путем модификации данных авторизации, необходимых для получения доступа к функциональным возможностям коммуникационного интернет-сервиса. Модификация данных авторизации производится в присутствии понятых. Порядок модификации данных авторизации фиксируется в протоколе.

9. Следователь в течение всего срока производства контроля электросвязи вправе в любое время произвести осмотр электронных сообщений (документа) и (или) истребовать от органа, осуществляющего контроль электросвязи, электронный носитель информации, содержащий телекоммуникацию

пользователя электросвязи, для осмотра. Электронный носитель информации передается следователю в опечатанном виде с сопроводительным письмом, в котором должны быть указаны даты и время начала и окончания записи телекоммуникации и краткие характеристики использованных при этом технических средств.

10. О результатах осмотра электронных сообщений (документа) и (или) электронного носителя информации, содержащего телекоммуникацию пользователя электросвязи, следователь с участием специалиста (при необходимости) составляет протокол, в котором должна быть дословно изложена та часть телекоммуникации, которая, по мнению следователя, имеет отношение к данному уголовному делу. Лица, участвующие в осмотре электронного носителя информации, содержащего телекоммуникацию пользователя электросвязи, вправе в том же протоколе или отдельно изложить свои замечания к протоколу.

11. Электронный носитель информации, содержащий телекоммуникацию пользователя электросвязи, приобщается к материалам уголовного дела на основании постановления следователя как вещественное доказательство и хранится в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования телекоммуникации пользователя электросвязи посторонними лицами и обеспечивающих ее сохранность и техническую пригодность для повторного прослушивания, в том числе, в судебном заседании».

Необходимо дать несколько пояснений относительно законопроекта. В предлагаемом следственном действии используются категории, понятие которых не содержится в УПК РФ: коммуникационный интернет-сервис, авторизация, модификация. Ряд указанных категорий содержится в Постановлении Правительства РФ от 31.07.2014 № 759. В соответствии с п. 2 нормативно-правового акта под авторизацией понимается «внесение зарегистрированным пользователем сети «Интернет» информации в коммуникационный интернет-сервис, необходимой для получения доступа к функциональным возможностям указанного коммуникационного интернет-сервиса».

Под коммуникационным интернет-сервисом понимается «информационная

система и (или) программа для электронных вычислительных машин, которая предназначена и (или) используется для приема, передачи и (или) обработки электронных сообщений пользователей сети «Интернет» в целях обмена электронными сообщениями между пользователями сети «Интернет», в том числе для передачи электронных сообщений неопределенному кругу лиц». Данная категория вбирает все существующие сервисы, позволяющие обмениваться электронными сообщениями: «Whatsapp», «Telegram», «Вконтакте» и другие.

Понятие модификация компьютерной информации используется в ч. 1 ст. 272 УК РФ, но его содержание не раскрывается. Понятие модификации информации содержится в «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации»[239]. Согласно документу, под модификацией компьютерной информации следует понимать «внесение изменений в компьютерную информацию (или ее параметры)».

Важным аспектом является то, что объем дефиниции телекоммуникация сформулирован так, что в него входит многообразие данных, которые передаются посредством электросвязи, в том числе и геолокационные данные.

Как было указано выше, многие организаторы распространения информации находятся за пределами территории Российской Федерации и из-за политической обстановки могут отказаться от сотрудничества с российскими правоохранительными органами, не взирая на нормы российского федерального законодательства.

По данной причине в законопроекте были предусмотрены механизмы получения телекоммуникации пользователя электросвязи без взаимодействия с организатором распространения информации в сети «Интернет» через арест телекоммуникаций и мониторинг телекоммуникации. Любопытно, что, к

[239] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» // Гарант: справ. правовая система // URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (дата обращения: 10.07.2021 г.).

примеру, § 100i УПК ФРГ допускает использовать технические средства (пеленгатора IMSI)[240] «для установления идентификационного номера прибора (IMEI) и идентификатора абонента (IMSI), а также местонахождения мобильного телефона с целью исследования обстоятельств дела или установления местонахождения обвиняемого»[241]. Скорее всего, названные технические средства в рамках контроля электросвязи могут использовать Бюро специальных технических мероприятий МВД России.

В рамках рассмотренного законодательного регулирования взаимодействия правоохранительных органов с операторами связи и организаторами распространения информации в сети «Интернет», а также предлагаемой уголовно-процессуальной новеллой по «контролю электросвязи», необходимо рассмотреть такое следственное действие, как получение информации между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ).

Один из вопросов, который касается данного следственного действия, состоит в целесообразности его существования. Сведения, на получение которых оно направлено, полностью дублируются ст. 64 Закона «О связи» и ст. 10.1. Закона Об информации, а также подзаконными нормативно-правовыми актами. Поэтому оставление в УПК следственног действия «получение информации между абонентами и (или) абонентскими устройствами» что не имеет практического значения, так как указанную информацию возможно будет получать с помощью «контроля электросвязи».

В юридической литературе на данную проблему уже обращалось внимание. Так, В.Ф. Васюков, указывая на смежность следственных действий, предусмотренных ст. 186.1. и ч. 7 ст. 185 УПК РФ, сделал следующий вывод: «Представляется, что с 01.07.2017 года следователям придется проводить два эти следственные действия одновременно, чтобы сформировать единый комплекс

---

[240] Устройство, используемое для перехвата сигнала мобильного телефона. Подробнее см.: Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy // URL: https://papers.ssrn.com/sol3/ papers.cfm? abstract_id=2437678 (дата обращения: 10.04.2020).

[241] Головненков П.В.. Указ. соч. – С. 58.

информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображения, звуков, видео и иных сообщений пользователей сотовой связи. В итоге это может привести к тому, что положения ст. 186.1. УПК РФ о возможности получения статистических сведений применяться не будут. Логично предположить, что использование в практике смежных процедур приведет к поглощению меньших по объему и значению юридических норм большими»[242].

Любопытную модель юридическую регулирования предлагает в своем диссертационном исследовании И.А. Зазулин. Автор находит необходимым исключить из ст. 185 УПК РФ ч. 7 и внести изменения в ст. 186.1. УПК РФ и изложить норму в новой редакции: «получение информации между абонентами и (или) абонентскими устройствами, а также информации, содержащейся в сообщениях, передаваемых посредством сервисов электронной почты, обмена мгновенными сообщениями или иным подобным образом»[243].

Исходя из законопроекта, И.А. Зазулин предлагает получать содержание электронных сообщений, которое обязаны хранить операторы связи и организаторы распространения информации в сети «Интернет» на основании ст. 10.1. Закона Об информации и ст. 64 Закона «связи», посредством ст. 186.1. УПК РФ. Однако в законопроекте не учтено, что операторы связи обязаны хранить голосовую информацию, передаваемую посредством телефонной связи. При этом порядок производства в разработанном следственном действии во многом схож с порядком производства «контроля и записи переговоров», в тоже время внесение каких-либо изменений в ст. 186 УПК РФ И.А. Зазулин не предлагает.

Следственное действие «получение информации о соединениях между абонентами и (или) абонентскими устройствами» может быть использовано для подготовки производства ареста телекоммуникаций. К примеру, следователем с помощью ст. 186.1. УПК РФ может быть получена информация, которая вносится

---

[242] Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. 2016. № 10. С. 66.

[243] Зазулин, А.И. Правовые и методологические основы использования использования цифровой информации в доказывании по уголовному делу: дисс. … кан. юрид. наук. Екатеринбург, 2018. С. 247-249.

пользователем коммуникационного интернет-сервиса при авторизации и в последующем модифицирована для наложения ареста телекоммуникаций посредством ст. 186 УПК РФ «контроля электросвязи».

В УПК ФРГ наряду с нормами, регулирующими «контроль телекоммуникаций» (§§100a/b УПК ФРГ), существует норма §100g «Информация о телекоммуникационных соединениях», которая по своей форме аналогична следственному действию «получение информации о соединениях между абонентами и (или) абонентскими устройствами». Как указывает П.В. Головненков: «Данная норма позволяет получать информацию о связи (например, номер абонентской карты, местонахождение, телефонный номер или идентификационные данные, в особенности идентификационный номер мобильного телефона и динамические IP-адреса компьютеров, исходящей и входящей точки соединения, время начала и окончания соединения, а также описание полученных телекоммуникационных услуг)»[244].

Видится, что исключение следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами» из УПК РФ преждевременно. Представляется значимым исправить недостатки уголовно-процессуальной конструкции ст. 186.1. УПК РФ, выявленные в ходе исследования. К основынм из них относятся: отсутствие сроков по предоставлению информации следователю, отсутствие законодательного закрепленного права получать ретроспективную информацию, конструкция следственного действия не достаточно ясно указывает на право получения сведений из области телематической связи.

Учитывая вышеизложенное, предлагается изложить п. 24.1 ст. 5 УПК РФ в следующей редакции: получение информации о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационными соединениями - получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), а также телекоммуникационных

[244] Головненков П.В. Указ. соч. С. 58.

соединениях номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций, сетевом адресе, доменном имя, идентификатор пользователя сети «Интернет», логин, пароль и других данные».

С учетом сказанного предлагается изложить ст. 186.1. УПК РФ в следующей редакции:

«Статья 186.1. Получение информации о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях.

1. При наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном ст. 165 настоящего Кодекса.

2. В ходатайстве следователя о производстве следственного действия, касающегося получения информации о соединениях между абонентами и (или) абонентскими, устройствами, а также телекоммуникационных соединениях указываются:

1) уголовное дело, при производстве которого необходимо выполнить данное следственное действие;

2) основания, по которым производится данное следственное действие;

3) период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия;

4) наименование организации, от которой необходимо получить указанную информацию.

3. В случае принятия судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях, его копия направляется следователем в соответствующую осуществляющую услуги связи организацию, руководитель

которой обязан предоставить указанную информацию, зафиксированную на любом материальном носителе информации. Указанная информация предоставляется в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств, а также иные идентификационные данные о пользователях сети «Интернет» и телекоммуникационных соединениях.

4. Получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях может быть установлено на срок до шести месяцев и неограниченном ретроспективном периоде. Соответствующая осуществляющая услуги связи организация и (или) организатор распространения информации в сети «Интернет» обязаны направить необходимую информацию не позднее 10 суток с момента получения постановление суда о производстве следственного действия. Соответствующая осуществляющая услуги связи организация и (или) организатор распространения информации в сети «Интернет» в течение всего срока производства данного следственного действия обязаны предоставлять следователю указанную информацию по мере ее поступления, но не реже одного раза в неделю.

5. Следователь осматривает представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях, с участием специалиста (при необходимости), о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов, сетевой адрес, доменное имя, идентификатор пользователя сети «Интернет», логин, пароль и другие данные). Лица, присутствовавшие при составлении протокола, вправе в том же протоколе или отдельно от него изложить свои замечания.

6. Представленные документы, содержащие информацию о соединениях

между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях, приобщаются к материалам уголовного дела в полном объеме на основании постановления следователя как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

7. Если необходимость в производстве данного следственного действия отпадает, его производство прекращается по постановлению следователя, но не позднее окончания предварительного расследования по уголовному делу.

ЗАКЛЮЧЕНИЕ

Основными научными положениями и выводами, сделанными в результате проведенного диссертационного исследования, являются следующие:

1. Первый этап интеграции информационных технологий в уголовное судопроизводство условно можно обозначить как процесс внедрения информационных технологий в уголовный процесс и утверждение данного направления науки уголовного процесса как приоритетного. Данный этап сопровождается нормативным закреплением информационных технологий и смежных категорий в УПК РФ, другие нормативные правовые акты, а также появлением первых научных трудов в названной сфере.

Следующим этапом интеграции информационных технологий в уголовное судопроизводство является широкое использование информационных технологий, переход от фрагментарного использования электронной информации к полноформатному электронному производству по уголовным делам. Представляется, что именно на данном этапе развития находится российское уголовное судопроизводство.

В перспективе, по прогнозам современной инженерной науки, человечество переступит порог девятой информационной революции и последующим этапом развития уголовного судопроизводства станет появление и использование в уголовном процессе информации с учетом иных способов ее передачи, обработки и представления. Электронная информация перестанет быть все объемлемым неисчерпаемым ресурсом, на смену его придут более продвинутые технологии.

2. Электронные средства, используемые в доказывании на досудебных стадиях уголовного процесса, – это совокупность уголовно-процессуальных и аппаратно-программных средств направленных на собирание, проверку и оценку доказательств, выраженных в электронном виде, а также обеспечивающих производство следственных действий.

Современное уголовно-процессуального доказывание, осуществляемое на досудебных стадиях уголовного судопроизводства, переживает период перехода

от фрагментарного использования электронной информации к полноценному производству по уголовным делам в электронном формате. Под электронной информацией следует понимать сведения (сообщения, данные) передача, обработка, воспроизведение которых осуществляется посредством электронных аппаратно-программных средств.

Понятие электронной информации вбирает в себя цифровую и аналоговую информацию, передаваемую посредством электронной связи, законодательно закреплено, в том ее преимущество.

3. Электронная информация не подчиняется классическим правилам отражения следов, основанного на взаимодействия следообразующего и следовоспринимающего материального объекта. Процесс отражения электронно-цифровой информации обусловлен переводом аналоговой информации в дискретный код и наоборот (или без «оцифровки», если речь идет об аналоговой электронике) с использованием программно-аппаратных средств. Таким образом, восприятие компьютерной информации происходит с помощью множества аппаратно-программных посредников между электронной информацией и органами чувств человека (субъекта доказывания).

4. К свойствам электронной информации можно отнести следующее:

– электронная информация соединяет в себе физический, логический, семантический уровни её существования. Физический и логический уровень существования информации являются гибкими атрибутами по отношению к семантическому уровню, так как изменения на указанных уровнях существования электронно-цифровой информации может не влиять на семантический уровень;

– электронная информация не может существовать без физического носителя, однако важно понимать, что физический носитель является крайне условным, так как электронная информация может быть сохранена на различные формы физических носителей (оптическом, электромагнитном и т. д.), в том числе находящихся в разных пространственных промежутках;

– электронную информацию возможно копировать неограниченное количество раз. При этом копия будет тождественна оригиналу;

– наблюдение электронной информации всегда происходит опосредовано, так как человек способен воспринимать органами чувств и понимать значение электронной информации только при посредничестве аппаратно-программных средств.

5. Наличие многочисленных аппаратно-программных посредников между электронной информацией и органами чувств человека не является основанием для априорного скептического отношения к достоверности электронной информации, так как аппаратно-программные средства функционируют по детерминированным физическим и программным алгоритмам.

Электронная информация существует в искусственно-созданной человеком среде (киберпространстве), и легко поддается изменению (удалению, модификации и т. д.). При производстве каких-либо манипуляций относительно электронной информации, необходимо вести речь об умышленном изменении электронной информации. В каждом конкретном случае субъекту доказыванию необходимо решить вопрос о необходимости проверки достоверности доказательств исходя из фактических обстоятельств дела.

Анализ правоприменительной практики показывает, что электронная информация используется для проверки других доказательств. Суд не подвергает сомнению достоверность электронной информации, даже в случаях, когда электронная информация была скопирована и предоставлена участником уголовного судопроизводства.

6. Рассматривая положение электронной информации среди источников уголовно-процессуальных доказательств, было выделено 4 основных научных подхода:

– электронную информацию необходимо приобщать к материалам уголовного дела в качестве закрепленных в ч. 2 ст. 74 УПК РФ источников уголовно-процессуальных доказательств: вещественных доказательств или иных документов;

– электронную информацию необходимо выделить как самостоятельный подвид вещественных доказательств и предусмотреть дополнительные поправки в УПК РФ;

– электронную информацию необходимо выделить в качестве самостоятельного источника уголовно-процессуальных доказательств;

– необходимо отказаться от исчерпывающего перечня источника уголовно-процессуальных доказательств.

Детальный анализ норм УПК РФ, регулирующий источники уголовно-процессуальных доказательств, научной литературы, правоприменительной практики, а также результатов социологического исследования сотрудников органов предварительного следствия, позволяет утверждать, что существующая система источников доказательств полностью охватывает все существующие формы электронной информации и позволяет приобщать ее к материалам уголовного дела в качестве «вещественных доказательств» или «иных документов».

Более того, выделение электронной информации (электронные доказательства) в качестве отдельного источника доказательств, наряду с иными документами может привести к коллизии среди существующих видов уголовно-процессуальных доказательств.

Юридическая конструкция категории «вещественных доказательств» позволяет относить компьютерную информацию к данному источнику по законодательным признакам. Подобное правовое явление представляет собой юридическую фикцию, так как компьютерная информация не имеет «вещественного» воплощения.

Проведенный теоретический анализ законодательного подхода по отнесению электронной информации к «вещественному доказательству» показывает небезапелляционность решения законодателя. Обозначенные свойства электронной информации позволяют утверждать, что её целесообразно относить именно к «иным документам».

7. Электронная информация отличается от «вещественных доказательств»

по следующим критериям.

1) по механизму образования. Для вещественных доказательств характерно механическое отражения структуры следообразующего объекта в структуре следовоспринимающем или существование отдельного материального объекта. Электронная информация сохраняется, обрабатывается, передается и воспроизводится в понятный для человека вид на основе электромагнитных физических свойств метрии с помощью аппаратно-программных средств.

2) по признаку восприятия. Вещественные доказательства воспринимаются органами чувств непосредственно. Электронная информация представляется в понятную для человека форму с помощью программно-аппаратных средств. Поэтому её восприятие всегда происходит опосредованно.

3) по содержанию доказательственной информации. В вещественном доказательстве юридически значимым представляется структура материального объекта. Для электронной информации значение для уголовного дела имеет информационное содержание электронного носителя информации, а не сам материальный объект.

Следует констатировать, что отнесения электронной информации к вещественным доказательствам является юридической фикцией и возможно только из-за уголовно-процессуальной конструкции норм о вещественных доказательствах.

По всей видимости, единственным разграничительным признаком между электронной информацией и «иными документами» является законодательное понятие «документа», где одним из признаков является наличие реквизитов, позволяющих идентифицировать документ. В исследовании было указано, что у электронного документа не всегда имеются идентифицирующие реквизиты.

8. Рассматривая особенности собирания, проверки и оценки доказательств с помощью электронных средств был выявлен ряд проблем.

Во-первых, телематическая, телефонная и иные виды связи, основанные на электромагнитных свойствах материи, интегрируются в единую систему электросвязи. Данный факт не был учтен законодателем при реформировании

УПК РФ, что ограничило многообразие сведений, которые допустимо собирать с помощью следственных действий. Объект следственного действия «контроль и запись переговоров» ограничивается информацией, передаваемой по телефонной связи.

Законодательная формулировка следственного действия получение информации о соединениях между абонентами и (или) абонентскими устройствами не вносит достаточной ясности о возможности получать сведения в рамках телематических услуг связи. Рассмотренные следственные действия не позволяют собирать геолокационные данные, а также иные формы электронной информации, которые прямо не указаны в УПК РФ.

Во-вторых, законодатель установил правоотношения, регулирующие порядок предоставления электронной информации субъектами, осуществляющими распространения информации в сетях электросвязи с правоохранительными органам, но связанные с данным процессом поправки, введенные в УПК РФ, содержат ряд технико-юридических недостатков, которые значительно затруднят их использовать в практической деятельности органов предварительного расследования.

Так, ч. 7 ст. 185 УПК РФ, предусматривает осмотр и выемку электронных сообщений. Однако юридическая конструкция данной нормы предназначалась для наложения ареста, осмотра и выемки «физических» почтово-телеграфных отправлений в учреждениях связи, а не электронных сообщений. Положения ст. 185 УПК РФ фактически не адаптировано для производства выемки и осмотра электронных сообщений.

Законодательство предусматривает обязанность предоставления информации, передаваемой по сетям электросвязи, при производстве следственных действий со стороны оператора связи. Для организатора распространения информации в сети «Интернет» такой обязанности не предусмотрено.

В-третьих, ряд поправок, введенных в УПК РФ, содержит недостатки, которые отражаются в практической деятельности. Дополняя ст. 185 УПК РФ ч.

7, законодатель не уточнил порядок производства ареста электронных сообщений, что является востребованной процедурой в практической деятельности. Юридическая конструкция следственного действия получение информации о соединениях между абонентами и (или) абонентскими устройствами не содержит положения о сроках предоставления информации следователю, также отсутствует законодательно закрепленное право получать ретроспективную информацию.

9. В соответствии со ст. 164.1 УПК РФ устанавливается императивное требование на участие специалиста при изъятии электронных носителей информации, что является анахронизмом, так как современные информационные технологии в большинстве случаев настолько просты в обращении, что не требуют специальных знаний. Требование об участии понятых в следственных действиях широко раскрыты в ст. 170 УПК РФ и в дополнительной регламентации в 164.1. УПК РФ не нуждается. Более того, процесс копирования информации с одного электронного носителя на другой фиксируется объективно и не нуждается в удостоверении со стороны понятых. Для разрешения названного недостатка предлагается авторская редакция ст. 164.1 УПК РФ.

10. Основными способами исследования содержания электронной информации, доступ к которой производится через изъятый электронный носитель, являются: осмотр предметов и назначение компьютерно-технической экспертизы. При производстве названных следственных действий без судебного решения исследуются и приобщаются к материалам уголовного дела частные электронные сообщения владельцев (пользователей) электронных носителей информации.

В данном случае можно утверждать, что тайна связи распространяется только на данные, которые были доверены лицом определенной организации или должностному лицу. Если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля. Данное положение согласуется с рассмотренной в

исследовании позицией Конституционного суда РФ, а также установленным порядком производства следственных действий в отношении электронных носителей информации, исключающих судебный контроль.

11. В исследовании обосновывается точка зрения, что названный механизм сбора электронной информации через электронные носители ограничивает право человека и гражданина на тайну связи и неприкосновенность частной жизни, предусмотренное ст. 23 Конституции РФ.

12. Для создания дополнительных гарантий защиты права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений были разработаны законодательные поправки, направленные на установление судебного контроля, на производство следственных действий в отношении электронных носителей информации. Основным критерием, необходимым для получения судебного решения на производство следственных действия, направленных на исследование содержания электронного носителя информации против воли владельца, является функциональная возможность электронного носителя передавать сведения по сетям электросвязи, так как в данном случае имеется высокая вероятность, что при обыске электронного носителя будет обнаружена информация, попадающая под действия режима тайны связи.

13. Обосновывается, что в ряде случаев происходит подмена обыска следственным осмотром при производстве следственных действий в отношении электронного носителя информации. Следует отметить, что УПК РФ не содержит четких разграничений между следственным осмотром и обыском. В условиях существования современных информационно-телекоммуникационных технологий проблема разграничения между названными следственными действиями является особенно актуальной. Анализ точек зрения, представленных в юридической литературе, позволяет прийти к выводу, что разграничительным критерием между следственным осмотром и обыском является степень вторжения органов предварительного расследования в частную жизнь человека, исходя из разумных ожиданий гражданина относительно сохранности тайны его личной жизни.

Основываясь на указанных абстрактно-юридических критериях, следователь может осмотреть электронный носитель информации, к примеру, с записью общественного места камер видеонаблюдения, так как не вторгается в личную жизнь человека, а последний может разумно ожидать, что запись может быть просмотрена. Но при этом следователь не может осматривать информационное содержание компьютера (планшет, мобильный телефон, и т. д.) против воли владельца, так как вторгается в личную жизнь человека, чего последний разумно ожидать не может. Подобное вторжение наглядно прослеживается при подборе пароля, защищающего личные сведения владельца электронного носителя информации.

Понимая, что для исследования информации, содержащейся на электронном устройстве, необходимо производить обыск, уголовно-процессуальное законодательство создаёт перед следователем ограничения. Так, в настоящий момент, ч. 1 ст. 182 УПК РФ предусматривает в качестве объектов обыска «какое-либо место» или «лицо».

Названный разграничительный критерий является абстрактным и оценочным для внедрения в уголовно-процессуальное законодательство, но должен стать руководящим принципом при его реформировании. Для унификации правоприменительной практики были разработаны поправки в УПК РФ, позволяющие точно определить, в каких случаях необходимо производить обыск электронного носителя, а в каких осмотр.

14. В целях совершенствования механизма получения электронной информации, передаваемых посредством электросвязи, было предложено исключить ч. 7 из ст. 185 УПК РФ. Заменить следственное действие «контроль и запись переговоров» (ст. 186 УПК РФ) на «контроль электросвязи».

Под контролем электросвязи следует понимать мониторинг голосовой информации, изображения, звука, видео-, иных форм телекоммуникации пользователей электросвязи, получение содержания телекоммуникации, в установленных федеральным законом случаях, от операторов связи и организаторов распространения информации в сети «Интернет», арест

телекоммуникаций». В свою очередь, под телекоммуникацией понимается прием, передача, доставка и (или) обработка голосовой информации, изображения, звука, видео-, и иных видов электронной информации пользователей электросвязи.

В конструкции следственного действия «контроль электросвязи» был детально проработан порядок мониторинга, получения и арест телекоммуникаций. Таким образом, объектом названного следственного действия являются все существующие формы коммуникации и данных пользователей в сфере электросвязи.

15. В ряде случаев следственные действия, направленные на собирание электронной информации, носят трансграничный характер. Международный механизм трансграничного получения электронной информации юридически сконструирован так, что в большинстве случаев необходимо получать согласие страны участника Конвенции «О преступности в сфере компьютерной информации». Подобное обстоятельство является негативной стороной международного регулирования действия уголовно-процессуального закона в «киберпространстве», так как потребность на получение электронной информации при производстве по уголовному делу является повсеместной, а взаимодействие в рамках международно-правовой помощи требует большого количество времени.

Так, «киберпространство» необходимо рассматривать с точки зрения режима общих международных территорий. Однако при этом необходимо учитывать, что производство процессуальных действий в «киберпространстве» может затрагивать права и интересы, а также аппаратно-программные средства граждан и организаций, которые могут находиться в любой точке планеты Земля.

Объектом трансграничных следственных действий может выступать только индивидуально-определенная область «киберпространства», которая привязана к лицу посредством данных, которые позволяют его идентифицировать (сетевой адрес, электронная почта и т. д.). Если производство по уголовному делу ведется в отношении неустановленного лица, то допустимо производить трансграничные

следственные действия по идентификационным данным пользователя в «киберпространстве» при наличии достаточных сведений, указывающих на то, что идентификационные данные относятся к лицу, совершившему преступление. При этом допустимо выходить за пределы «киберпространства», привязанного к физической памяти электронного носителя информации, если имеются достаточные данные полагать, что могут быть обнаружены сведения, имеющие отношение к уголовному делу. Данный принцип производства трансграничных следственных действий, можно обозначать как «электронное домино».

Недопустимо производить трансграничные следственные действия в тех случаях, когда может создаться угроза безопасности какого-либо государства. К примеру, интернет-сервис, который используется гражданами и на территории конкретного государства (национальный интернет-банк, госуслуги и т. д.). В данном случае, следственное действие необходимо произвести в рамках международной правовой помощи.

Изложенные выводы позволят достичь значительного прогресса по использованию электронной информации в доказывании на досудебных стадиях уголовного процесса.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативно-правовые акты и иные официальные документы

1. Конвенция о защите прав человека и основных свобод (ред. от 24.06.2013) // КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_29160/ (дата обращения: 13.07.2021 г.).

2. Конвенция о преступности в сфере компьютерной информации ETS от 23.11.2001 № 185 (г. Будапешт) // Гарант: справ. правовая система // URL: http://base.garant.ru/4089723/ (дата обращения: 13.08.2021 г.).

3. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Бюллетень международных договоров. 2009. № 6.

4. Конституция Российской Федерации, принята 12 декабря 1993 г. Всенародным голосованием (ред. от 14.03.2020 г.) // КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 13.07.2021 г.).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) // Гарант: справ. правовая система // URL: https://base.garant.ru/10108000/ (дата обращения: 13.08.2021 г.).

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) // Гарант: справ. правовая система // URL: https://base.garant.ru/12125178/ (дата обращения: 01.08.2021 г.).

7. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (ред. от 02.07.2021) // Гарант: справ. правовая система // URL: http://base.garant.ru/186117/ (дата обращения: 01.08.2021 г.).

8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 02.07.2021) // Гарант: справ. правовая система // Гарант: справ. правовая система // URL: http://base.garant.ru/12148555/ (дата обращения: 01.08.2021 г.).

9. Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» (ред. от 27.12.2019) // Гарант: справ. правовая система // URL: http://base.garant.ru/180689/ (дата обращения: 01.08.2021 г.).

10. Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов» (ред. от 08.06.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/103526/ (дата обращения: 20.06.2021 г.).

11. Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (ред. от 31.07.2020) // Гарант: справ. правовая система // Гарант: справ. правовая система // URL: https://base.garant.ru/12126961/ (дата обращения: 20.06.2021 г.).

12. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 12.07.2021) // Гарант: справ. правовая система // URL: https://base.garant.ru/10104229/ (дата обращения: 20.06.2021 г.).

13. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 20.03.2021) «О коммерческой тайне» // Гарант: справ. правовая система // URL: https://base.garant.ru/12136454/ (дата обращения: 20.07.2021 г.).

14. Федеральный закон от 02.12.1990 № 395-1 (ред. от 02.07.2021) «О банках и банковской деятельности» // Гарант: справ. правовая система // URL: https://base.garant.ru/10105800/ (дата обращения: 13.07.2021 г.).

15. Закон РФ от 21.07.1993 № 5485-1 (ред. от 01.07.2021) «О государственной тайне» // Гарант: справ. правовая система // URL: https://base.garant.ru/10102673/ (дата обращения: 13.07.2021 г.).

16. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. № 149. 2016.

17. Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по

вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» // Российская газета. 2014. 07 мая.

18. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 08 июля.

19. Федеральный закон от 29.07.2017 № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» // Российская газета. 2017. 04 августа.

20. Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 2012. 03. декабря.

21. Федеральный закон от 01.07.2010 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2010. 07 июля.

22. Федеральный закон от 28.07.2012 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2012. 01 августа.

23. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 01.07.2021) «Об электронной подписи» // Гарант: справ. правовая система // URL: http://base.garant.ru/12184522/ (дата обращения: 11.07.2021 г.).

24. Федеральным закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности» // Российская газета. 2016. 08 июля.

25. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер

противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 11 июля.

26. Постановления Правительства РФ от 09.12.2014 № 1342 «О порядке оказания услуг телефонной связи» (ред. от 18.01.2021) // Консультант плюс: справ. правовая система // Консультант плюс: справ. правовая система // URL: http:// www.consultant.ru/document/cons_doc_LAW_172117/ (дата обращения: 15.08.2021 г.).

27. Постановлением Правительства РФ от 10.12.2007 № 575 «Об утверждении Правил оказания телематических услуг связи» (ред. от 30.12.2020) // Гарант: справ. правовая система // Гарант: справ. правовая система // URL: http://base.garant.ru/12155536/ (дата обращения: 15.08.2021 г.).

28. Постановление Правительства РФ от 31.07.2014 № 743 «Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации» (ред. от 01.12.2018) // Гарант: справ. правовая система // URL: http://base.garant.ru/70709018/ (дата обращения: 15.08.2021 г.).

29. Постановление Правительства РФ от 31.07.2014 № 759 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации» (ред. от 04.08.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/70710174/ (дата обращения: 10.05.2021 г.).

30. Постановление Правительства РФ от 27.08.2005 № 538 «Об

утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» (ред. от 17.04.2021) // Консультант плюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_55326/ (дата обращения: 15.05.2021 г.).

31. Приказ Министерства связи и массовых коммуникаций от 31.07. 2014 № 234 «Об утверждении правил оказании услуг почтовой связи» (ред. от 19.11.2020) // Гарант: справ. правовая система // URL: http://base.garant.ru/70835708/ (дата обращения: 10.05.2021 г.).

32. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» // Гарант: справ. правовая система // URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (дата обращения: 10.07.2021 г.).

33. Уголовно-процессуальный кодекс Федеральной Республики Германии от 12.09.1950 // Официальный сайт публикации документа. URL: http://www.gesetze-im-internet.de/englisch_stpo/index.html. (дата обращения: 10.07.2021 г.).

II. Монографии, учебные пособия

34. Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография / В.Ю. Агибалов. – М.: Юрлитинформ, 2012. –152 с.

35. Балакшин, В.С. Доказательства в Российском уголовном процессе: понятие, сущность, классификация: монография / В.С. Балакшин. – Екатеринбург: Изд-во УрГЮА, 2015. – 112 с.

36. Белкин, А.Р. Теория доказывания: научно-методическое пособие / А.Р. Белкин. – М.: Издательство НОРМА, 1999. – 429 с.

37. Бурдинский, И.Н. Системы счисления и арифметика ЭВМ / И.Н. Бурдинский. – Хабаровск: Изд-во Тихоокеан. гос. ун-та. 2008. – 79 с.

38. Вехов, В.Б. Расследование преступлений в сфере компьютерной

информации и электронных средств платежа: учебное пособие для вузов / В.Б. Вехов, С.В. Зуев. – М.: Издательство Юрайт. 2021. – 243 с.

39. Гаврилов, Б.Я. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей / Б.Я. Гаврилов. – М.: Проспект, 2017. – 160 с.

40. Головненков, П.В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: научно-практический комментарий и перевод текста закона / П.В. Головненков. – М.: Проспект, 2-е изд. 2012. – 312 с.

41. Громов, Н.А. Доказательства их виды и доказывание в уголовном процессе: учебно-практическое пособие / Н.А. Громов, С.А. Зайцева, А.Н. Гущин. – М.: Приор-издат, 2006. – 80 с.

42. Даль, В.И. Толковый словарь живого великоросского языка / В.И. Даль. – М.: Русский язык, 1955. – Т. 4. – 684 с.

43. Жалинский, А.Э. Учебно-практический комментарий к Уголовному кодексу Российской Федерации / А.Э. Жалинского, О.Л. Дубовик – М.: Издательство «Эксмо», 2006. – 1088 с.

44. Зинатулли, З.З. Уголовно-процессуальное доказывание / З.З. Зинатулли – Ижевск: Детектив-Информ, 2003. – 255 с

45. Зуев, С.В. IT-справочник следователя / С.В. Зуев – М.: Юрлитинформ, 2019. – 232 с.

46. Зуев, С.В. Информационные технологии в уголовном процессе зарубежных стран: монография / Д.В. Бахтеев, В.А. Задорожная, А.И. Зазулин, В.К. Захарова, П.С. Пастухов, Ю.В. Стрелкова – М.: Юрлитинформ, 2020. – 216 с.

47. Зуев, С.В. Основы оперативно-розыскной деятельности: учебное пособие для вузов / С.В. Зуев. – М.: Издательство Юрайт. 2020. – 191 с.

48. Зуев, С.В. Основы теории электронных доказательств: монография / А.Н. Балашов, И.Н. Балашов, Д.В. Бахтеев, К.Л. Брановицкий, В.Б. Вехов, В.Н. Григорьев, В.В. Долганичев, А.И. Зазулин, О.А. Зайцев, С.В. Зуев, О.А. Максимов, М.О. Медведева, Д.В. Овсянников, О.В. Овчинникова, П.С. Пастухов, О.В. Тушканова – М.: Юрлитинформ, 2019. – 383 с.

49. Зуев, С.В. Развитие информационных технологий в уголовном судопроизводстве: монография / В.С. Балакшин, В.Б. Вехов, В.Н. Григорьев, А.И. Зазулин, О.А. Зайцев, С.В. Зуев, М.О. Медведева, Е.В. Никинит, О.В. Овчинникова, П.С. Пастухов, В.А. Родиыилина, И.В. Смолькова, В.Ю. Стельмах, А.А. Шаевич – М.: Юрлитинформ, 2018. – 248 с.

50. Зуев, С.В. Уголовный процесс: учебник / С.В. Зуев, К.И. Сутягин. – Челябинск: Издательский Центр ЮУрГУ, 2016. – 563 с.

51. Зуев, С.В. Цифровизация судопроизводства: научно-практический (постатейный) комментарий правовых актов / К.Л. Брановицкий, В.Н. Григорьев, С.П. Грубцова, О.А. Зайцев, А.И. Зазулин, С.В. Зуев, П.С. Пастухов, М.О. Медведева, В.С. Черкасов. – М.: Юрлитинформ, 2020. – 320 с.

52. Зуев, С.В. Электронные доказательства в уголовном судопроизводстве: учеб. пособие / С.В. Зуев, Д.В. Бахтеев, В.Б. Вехов, А.И. Зазулин, П.С. Пастухов, О.В. Тушанова – М.: Издательство Юрайт. 2020. – 193 с.

53. Кокорев, Л.Д. Уголовный процесс: доказательства и доказывание / Л.Д. Кокорев, Л.Д. Кузнецов. – Воронеж. Изд-во Воронеж. ун-та. 1995. – 272 с.

54. Лазарева, В.А. Доказывание в уголовном процессе: учебно-практическое пособие / В.А. Лазарева. – М.: Высшее образование, 2009. – 343 с.

55. Лебедев, В.М. Научно-практический комментарий к Уголовно-процессуальному кодексу Российской Федерации / В.М. Лебедев, В.А. Давыдов. – М.: Издательская группа ИНФРА-М, 2014. – 1056 с.

56. Опадчий, Ю.Ф. Аналоговая и цифровая электроника / Ю.Ф. Опадчий, О.П. Глудкин, А.И. Гуров. – М.: Горячая Линия-Телеком, 2005. – 768 с.

57. Орлов, Ю.К. Проблемы теории доказательств в уголовном процессе / Ю.К. Орлов. – М. : Юристъ, 2009. – 175 с.

58. Подосинов, А.В. Латинско-русский и русско-латинский словарь / А.В. Подосинов – М.: ФЛИНТА, 2014. – 744 с.

59. Пронин, К.В. Защита коммерческой тайны / К.В. Пронин. – М.: Издательство: Гросс-Медиа, 2006. – 144 с.

60. Романов, Б.Н. Теория электрической связи. Сообщения, сигналы,

помехи, их математические модели: учеб. пособие / Б.Н. Романов, С.В. Краснов. – Ульяновск: Ульяновский гос. технический ун-т, 2008. – 127 с.

61. Россинская, Е.Р. Судебная компьютерная – техническая экспертиза / Е.Р. Россинская, А.И. Усов. М.: Право и закон, 2001. 414 с.

62. Рыжаков, А.П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / А.П. Рыжаков. – М.: «Гарант-сервис-университет», 2014. – 1289 с.

63. Смирнов, А.В. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / А.В. Смирнов, К.Б. Калиновский. – М.: Проспект, 2009. – 992 с.

64. Смирнов, А.В. Следственные действия в российском уголовном процессе: учеб. пособие / А.В. Смирнов, К.Б. Калиновский. – СПб.: СПбГИЭУ, 2004. – 73 с.

65. Соколов Ю.Н. Информационные технологии в уголовном судопроизводстве: монография / Ю. Н. Соколов. - Екатеринбург : Телекоммуникационное Право, 2010. – 418 с.

66. Стельмах, В.Ю. Производство следственных действий, направленных на получение и использование компьютерной информации / В.Ю. Стельмах, О.М. Ефремова, В.Ф. Васюков. – М, 2021. – 480 с.

67. Строгович, М.С. Курс советского уголовного процесса: Основные положения науки советского уголовного процесса / М.С. Строгович. – Т.1. – М.: Издательство «Наука», 1968. – 470 с.

68. Томин, В.Т. Уголовный процесс: актуальные проблемы теории и практики / В.Т. Томин. – М.: Издательство Юрайт, 2009. – 376 с.

69. Федотов, Н.Н. Форнзика – компьютерная криминалистика / Н.Н. Федотов. – М.: Юридический мир, 2007. – 432 с.

70. Хохлов, Ю.Е. Глоссарий по информационному обществу / Е.Ю. Хохлов, М.А. Банчук, О.Н. Вершинская, Р.У. Елизарова, Т.В. Ершова, Когаловский М.Р., Мендкович А.С., Паринов С.И., Смолян Г.Л., Стырин Е.М., Черешкин Д.С., Шаповшник С.Ю. – М.: Институт развития информационного общества, 2009. –

160 с.

71. Шейфер, С.А. Доказательства и доказывание по уголовным делам. / С.А. Шейфер – М.: Издательство Норма. 2020. – 240 с.

72. Юнг, У. Аналоговая электроника / У. Юнг. – Бостон, Оксфорд, 2002. – 1145 с.

73. Croydon, M.S. Electronic evidence / Ed. by M.S. Croydon. – 3rd ed. Lexis Nexis: Butter worths Law, 2012. – 934 p.

74. Gercke, M. Understanding cybercrime: a guide for developing countries / M. Gercke. – ITU, 2011. – 493 p.

75. Shipley, Todd. G. Investigating internet crimes: an introducing to solving internet crimes in cyberspace / Todd. G Shipley, A. Bowker 2014. – USA: Elsevier. – 496 p.

III. Научные статьи

76. Азаров, В.А. Действительно ли объективная истина – цель доказывания в уголовном судопроизводстве? / В.А. Азаров // Библиотека криминалиста. – 2012. - № 4. - С. 7-10.

77. Александров, А.С. О надежности «электронных доказательств» в уголовном процессе / А.С. Александров, С.И. Кувычков // Библиотека криминалиста. – 2013. – № 5. – С. 76-84.

78. Андреева, О.И., Правовое регулирование уголовно-процессуальных отношений в цифровую эпоху / О.И. Андреева, О.А. Зайцев // Вестник Томского государственного университета. – 2020. – № 455. – С. 190-198.

79. 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. 99-105.

80. Ансельмно, Э.Л. Киберпространство в международном законодательстве: опровергает ли развитие интернета принцип территориальности в международном праве? / Э.Л. Ансельмно // Экономические стратегии. – 2006. – № 2. – С. 24-31.

81. Антонов, И.А. Работа следователя: противоречия процессуального положения, решаемых задач и ответственности / И.А. Антонов // Российский следователь. – 2019. – № 7. – С. 15 - 19.

82. Архипова, Н.А. Особенности тактики получения информации о соединениях между абонентами и абонентскими устройствами / Н.А. Архипова // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2014. – № 12-1. – С. 76-78.

83. Асанов, Р.Ш. Проблема обеспечения прав личности при действующей форме производства контроля и записи переговоров / Р.Ш. Асанов // Труды Академии управления МВД России. – 2019. – № 4. – С. 33-39.

84. Багавиева, Э.А. Об основаниях применения получения информации о соединениях между абонентами и (или) абонентскими устройствами / Э.А. Багавиева // Бизнес. Образование. Право. – 2019. – № 2 (47). – С. 296-301.

85. Баранов, А.М. Электронные доказательства: иллюзия уголовного процесса XXI В. / А.М. Баранов // Уголовная юстиция. – 2019. - № 13. – С. 64-69.

86. Беспалов, М.Б. Маленький вопрос большой доступности или о возможностях использования видеоконференц-связи в судах Российской Федерации / М.Б. Беспалов // Вестник Екатерининского университета. – 2014. – № 4. – С. 67-73.

87. Бикмиев, Р.Г., Бурганов, Р.С. Выемка и осмотр электронных устройств / Р.Г. Бикмиев, Р.С. Бурганов // Уголовное право. – 2018. – № 1. – С. 125-131.

88. Бондаренко, А.А. Изъятие электронных носителей информации при расследовании уголовных дел экономической и общеуголовной направленности, а также по соединенным уголовным делам / А.А. Бондаренко // Законодательство и практика. – 2019. – № 1. – С. 36-40.

89. Быков, В.М. Понятие компьютерной информации как объекта преступлений / В.М. Быков, В.Н. Черкасов // Законность. – 2013. – № 12. – С. 37-40.

90. Важенин, В.В. Проблемы противодействия экстремизму в сети «Интернет» / В.В. Важенин, Т.З. Имаков // Преступность в сфере

информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2015. – № 1. – С. 19-26.

91. Варданян, А.А. Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединения между абонентами и (или) абонентскими устройствами / А.А. Варданян, А.А. Цыкора // Известия тульского государственного университета. – 2013. – № 4 (Ч. 2).– С. 21-26.

92. Васюков, В.Ф. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В.Ф. Васюков, А.В. Булыжкин // Российский следователь. – 2016. – № 6. – С. 3-8.

93. Васюков, В.Ф. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел / В.Ф. Васюков, С.Е. Семенова // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3. – С. 203-209.

94. Васюков, В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации / В.Ф. Васюков // Уголовный процесс. – 2016. – № 10. – С. 64-67.

95. Васюков, В.Ф. Особенности получения сведений о геолокации мобильного абонентского устройства, находящегося в пользовании скрывшегося подозреваемого, посредством общедоступных аппаратных средств и программных ресурсов / В.Ф. Васюков // Библиотека криминалиста. – 2016. – № 3. – С. 321-324.

96. Вехов, В.Б. Работа с электронными доказательствами в условиях изменяющегося уголовно-процессуального законодательства / В.Б. Вехов // Российский следователь. – 2013. – № 10. – С. 22-24.

97. Вехов, В.Б. Электронные доказательства: проблемы теории и практики / В.Б. Вехов // Правопорядок: теория, история, практика. – № 4. – 2016. – С. 46-49.

98. Воскобитова, Л.А. Уголовное судопроизводства и цифровые

технологии: проблемы совместимости / Л.А. Воскобитова // Lex Russia (Русский закон). – 2019. - № 5. – С. 91-104.

99. Виноградова, К.А., Изъятие и осмотр мобильных телефонов и находящейся на них электронной информации по преступлениям, совершенным военнослужащими / К.А. Виноградова, Л.А. Савина // Вестник военного права. – 2019. – № 2. – С. 55-58.

100. Гаас, Н.Н. Осмотр изъятого мобильного устройства: проблемы правоприменения / Н.Н. Гаас // Вестник Уральского юридического института МВД России. – 2019. – № 4 (24). – С. 28-32.

101. Гаврилов, Б.Я. Получение доказательств и информации с электронных носителей: вопросы законодательного регулирования и правоприменения / Б.Я. Гаврилов // Уголовное судопроизводство: проблемы теории и практики. –2018. – № 3. – С. 32-36.

102. Галкин, Д.В. Об использовании зеркала Гезелла в ходе допроса несовершеннолетнего / Д.В. Галкин // Труды академии МВД республики Таджикистан. – № 3. – 2015. – С. 60-62.

103. Головко, Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция / Л.В. Головко // Вестник экономической безопасности: юридические науки. – 2019. - № 1. – С. 15-25.

104. Гмырко, В.П., Парадоксы доказательственного права / В.П. Гмырко, И.А. Зинченко // Библиотека криминалиста. – 2014. – № 2. – С. 9-17.

105. Григорьев, В.Н. Тенденции и проблемы развития законодательств в области информационных технологий, регулирующего уголовное судопроизводство / В.Н. Григорьев // Академическая мысль. – 2019. – № 3 (8) – С. 56-61.

106. Григорьев, В.Н., Об электронных носителях информации в уголовном судопроизводстве / В.Н. Григорьев, О.А. Максимов // Вестник Нижегородского ун-та им. Н.И. Лобачевского. – 2019. – № 3. – С. 65-71.

107. Гришин, А.В., Актуальные проблемы совершенствования уголовно-процессуального права в Российской Федерации / А.В. Гришин, О.Г. Селютина //

Закон и право. – 2020. – № 9. – С. 61-62.

108. Гришин, А.В., Некоторый проблемы внедрения понятия «электронные доказательства» в процессуальное законодательство / А.В. Гришин, А.И. Пахомова // Актуальные проблемы права, государства и экономики: сборник статей Всероссийской конференции и межведомственного круглового стола. Орел. – 2020. – С. 45-48.

109. Грошев, И.А. Еще раз к проблемам получения информации о соединениях между абонентами и (или) абонентскими устройствами / И.А. Грошев // Актуальные проблемы гуманитарных и естественных наук. – 2016. – № 2-6. – С. 138-142.

110. Давлетов, А.А. Право адвоката применять технические средства при производстве следственных действий / А.А. Давлетов // Адвокатская практика. – 2020. - № 2. – С. 44-48.

111. Данилов, А.И. Классификация следственных действий / А.И. Данилов // Юридический факт. – 2019. – № 80. – С. 26-27.

112. Денисов, Е.А. Проблемы изъятия криминалистически значимой информации у компании, предоставляющей услуги социальной сети / Е.А. Денисов // Вестник Московского университета МВД России. – 2018. – № 2. – С. 101-104.

113. Деришев, Ю.В. Всесторонность, полнота и объективность исследования обстоятельств как принцип современного уголовного судопроизводства / Ю.В. Деришев, Т.Г. Олиференко // Ввестник омской юридической академии. – 2016. - № 1. – 56-60.

114. Диденко, К.В. Документы вещественные доказательства и «иные документы»: проблемы разграничения / К.В. Диденко // Проблемы в российском законодательстве. – 2008. – № 2. – С. 291-292.

115. Дикарев, И.С. Система сдержек и противовесов в досудебном производстве по уголовным делам / И.С. Дикарев // Журнал российского права. – 2018. – № 3. – С. 76-83.

116. Долгополов, Н.В. «Электронный нос» – новое направление индустрии

безопасности / Н.В. Долгополов, М.Ю. Яблоков // Мир и безопасность. – 2007. – № 3. – С. 54-59.

117. Доля, Е.А. Проверка доказательств в российском уголовном процессе (стадия предварительного расследования) / Е.А. Доля // Правоведение. 1994. – № 1. – С. 27-28.

118. Дубоносов, Е.С., Анализ перспектив развития отечественной системы следственных действий / Е.С. Дубоносов, В.Н. Яшин // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 1. – С. 71-81.

119. Ефремов, А.А. Новые информационные технологии в практике Европейского суда по правам человека / А.А. Ефремов // Прецеденты Европейского суда по правам человека. – 2016. – № 6. – С. 10-15.

120. Ефремова, М.А. К вопросу о понятии компьютерной информации / М.А. Ефремова // Российская юстиция. – 2012. – № 7. – С. 50-52.

121. Зазулин, А.И. Компьютерная информацию в уголовном процессе: сущность и способы закрепления как доказательства по уголовному делу / А.И. Зазулин // Бизнес в законе: экономико-юридический журнал. – 2015. – № 6. – С. 130-133.

122. Зайцев, О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации / А.С. Александров, О.И. Андреева, О.А. Зайцев // Вестник Томского государсвенного университета. – 2019. – № 488. – С. 199-207.

123. Зигура, Н.А. Разграничения компьютерной информации и «иных» документов / Н.А. Зигура // Вестник Южно-уральского государственного университета. Серия: право. – 2008. – № 8. – С. 53-56.

124. Зинатуллин, З.З. Проблемы уголовно-процессуального доказывания в свете достижений научно-технического прогресса / З.З. Зинатуллин, Т.З. Зинатуллин // Судебная власть и уголовный процесс. – 2020 - № 3 – С. 33-37.

125. Зуев, С.В. Негласные формы уголовного судопроизводства 1864 года и их современное развитие / С.В. Зуев // Расследование преступлений: проблемы

и пути их решения. – 2014. – № 4 (4). – С. 110-117.

126. Зуев, С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы / С.В. Зуев // Сибирский юридический вестник. – 2018. – № 4. – С. 118-122.

127. Искевич, И.С. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект / И.С. Искевич, М.Н. Кочеткова, А.М. Попов // Проблемы правоохранительной деятельности. – 2016. – № 2. – С. 54-58.

128. Караваев, Н.Л. Феномен информатизации: терминологический анализ понятия / Н.Л. Караев // Информатизация образования и науки. – 2014. – № 4(24). – С. 3-14.

129. Карась, И.З. Экономический и правовой режим информационных ресурсов / И.З. Карась // Право и информатика. - М.: Изд-во Моск. ун-та, 1990 – С. 40-59.

130. Карташов, И.И. «Цифровые доказательства» в уголовном процессе / И.И. Карташов // Центральный научный вестник. – 2016. – № 15. – С. 23-25.

131. Ким, А.В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации / А.В. Ким // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2019. – №1. – С. 151-156.

132. Ключко, В.И. Квантовые технологии как основа квантового компьютера / В.И. Ключко, Н.В. Кушнир, Д.С. Шелехань // Научные труды КубГТУ. – 2017. – № 3. – С. 136-140.

133. Кравец, Е.Г. Результаты анализа проекта федерального закона «О внесении дополнений в уголовно-процессуальный кодекс российской федерации (в части производства предварительного расследования с применением систем видеоконференц-связи)» / Е.Г. Кравец, И.В. Казначей // Современные проблемы науки и образования. – 2015. – № 2. – С. 663-670.

134. Крюкова, Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной

практики / Т.С. Крюкова // Использование информационных технологий в уголовном судопроизводстве: проблемы теории и практики. – 2016. – № 4. – С. 61-63.

135. Кузнецова, С.М. Реализация конституционного права на тайну переписки, телефонных переговоров и иных сообщений при осмотре сотового телефона в ходе производства по уголовному делу / С.М. Кузнецова // Вестник Дальневосточного юридического института МВД России. – 2018. – № 2 (43). – С. 39-43.

136. Лупинская, П.А. Общее и особенное в правилах о доказательствах и доказывании в УПК РФ и ГПК РФ / П.А. Лупинская // Lex russica (русский закон). – 2005. - № 4. – С. 707-718.

137. Маринкин, Д.Н. Цифровые доказательства в уголовном судопроизводстве / Д.Н. Маринкин, В.А. Костарева // Вестник Пермского института ФСИН России. – 2019. – № 1 (32). – С. 33-36.

138. Масленникова, Л.Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу / Л.Н. Масленникова, Т.Ю. Вилкова // Вестник Пермского университета. Юридические науки. – 2019. - № 46. – С. 728-751.

139. Мещеряков, В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста. – 2013. – № 5. – С. 265-270.

140. Морозова, Е.В. Тактика контроля и записи переговоров: проблемы теории и практики / Е.В. Морозова, Н.А. Андровник // Вестник уральского института экономики: управление и право. – 2013. – № 4. – С. 16-22.

141. Новиков, С.А. Допрос с использованием систем видеоконференц-связи: завтрашний день российского предварительного расследования / С.А. Новиков // Российский следователь. – 2014. – № 1. – С. 2-6.

142. Овчинникова, О.В. Собирание электронных доказательств размещенных в сети интернет / О.В. Овчинникова // Правопорядок: история, теория и практика. – 2016. – № 4. – С. 67-70.

143. Оконенко, Р.И. К вопросу о правомерности осмотра компьютера как

следственного действия // Адвокат. 2015. – № 1. – С. 27-30.

144. Осипенко, А.Л. О правовом регулировании действий оперативно-розыскных органов при раскрытии трансграничных преступлений в сети Интернет / А.Л. Осипенко // Оперативник (сыщик). – 2011. – № 2. – С. 18-23.

145. Осипенко, А.Л. Особенности расследования сетевых компьютерных преступлений / А.Л. Осипенко // Российский юридический журнал. – 2010. – № 2. – С. 121-126.

146. Осипенко, А.Н. Правовое регулирование и тактические особенности изъятия электронных носителей информации / А.Н. Осипенко, А.И. Гайдан // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 156-163.

147. Осипенко, А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы существования / А.Л. Осипенко // Вестник ВИ МВД России. – 2016. – № 3. – С. 83-90.

148. Пастухов, П.С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств / П.С. Пастухов // Общество и право. – 2015. – № 1. – С. 192-196.

149. Пастухов, П.С. Проблемы законодательного регулирования использования электронной информации в качестве доказательств по уголовному делу / П.С. Пастухов // «Черные дыры» в Российском законодательстве. – 2015. – № 3. – С. 127-130.

150. Пастухов, П.С. Электронное вещественное доказательство в уголовном судопроизводстве / П.С. Пастухов // Вестник ТГУ. – 2015. – № 396. – С. 149-153.

151. Родивилина, В.А., Изъятие и осмотр мобильного телефона как электронного носителя информации / В.А. Родивилина, Н.Н. Цуканов // Вестник Восточно-Сибирского института МВД России. – 2019. – № 4 – С. 107-114.

152. Россинский, С.Б. Собирание доказательств как «первый» этап доказывания по уголовному делу / С.Б. Россинский // Юридический вестник Самарского университета. – 2020. – Т. 6. – № 3. – С. 101-103

153. Семенцов, В.А. К вопросу о пополнении системы следственных

действий негласными познавательными приемами / В.А. Семенцова // Законы России: опыт, анализ, практика. – 2016. – № 4. – С. 48-57.

154. Семенцов, В.А. Цифровизация отечественного уголовного судопроизводства: эволюционный подход / В.А. Семенцова // Юридический весстник Кубанского государственного университета. – 2019. –№ 1. – С. 52-56.

155. Серетенцев, Д.Н. Применение цифровых средств фиксации в раскрытии и расследовании преступлений / Д.Н. Серетенцев, Н.С. Киреева // Научный вестинк Орловского юридического института МВД России им. В.В. Лукъянова. – 2017 - № 1. – С. 80-83.

156. Скобелин, С.Н. Использование специальных знаний при работе с электронными следами / С.Н. Скобелин // Российский следователь. – 2014. – № 20. – С. 31-33.

157. Соколов, А.Д. Геолокация с использование API социальных сетей / А.Д. Соколов, А.С. Стешкова, С.А. Будников: сборник материалов Всероссийской научно-практической конференции // Актуальные проблемы деятельности подразделений УИС: сб. мат. Всер-кой науч.-практ. конф. Воронеж: «Научная книга», 2016. – С. 143-146.

158. Соколов, Ю.Н. Использование информации о соединениях между абонентами и (или) абонентскими устройствами в ходе предварительного расследования преступлений / Ю.Н. Соколов // Российский следователь. – 2011. – № 11. – С. 18-21.

159. Сотников, К.И. Тактика осмотра страниц интернет-сайтов / К.И. Сотников // Вестник криминалистики. – 2015. – № 2 (54). – С. 48-53.

160. Старичков, М.В. Электронные носители как источники криминалистически значимой информации / М.В. Старичков, В.А, Антонов // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Вып. 3-4. Иркутск: ФГКОУ ВПО «ВСИ МВД России», 2013. – С. 123-127.

161. Стельмах, В.Ю. К вопросу о предмете контроля и записи телефоны переговоров как следственного действия / В.Ю. Стельмах // Деятельность правоохранительных органов в современных условиях: мат. XVIII Меж-ной

науч.-практ. конф, посвященные 20-летию образования института ВСИ МВД России. – 2013. – С. 119-122.

162. Стельмах, В.Ю. К вопросу о предмете контроля и записи телефонных и иных переговоров как следственного действия / В.Ю. Стельмах // Материалы XVIII Международной научно-практической конференции: «Деятельность правоохранительных органов в современных условиях» – Иркутск, – 2013. – С. 119-122.

163. Стельмах, В.Ю. Проблема процессуальной регламентации следственных действий, направленных на получение сведений, передаваемых по сетям электросвязи / В.Ю. Стельмах // Юридическая наука и правоохранительная практика. – 2013. – № 3. – С. 108-113.

164. Стельмах, В.Ю. Технико-специальные следственные действий в российском уголовном процессе / В.Ю. Стельмах // Вестник Санкт-Петербурского университета МВД России. – 2015. – № 1. – С. 54-60.

165. Стив, Ш. Основные типы абонентских телефонных линий и услуг / Ш. Стив // URL: https://www.osp.ru/lan/1996/02/131926 (дата обращения 13.03.2021 г.).

166. Сухова, Ж.В. Понятие информационных технологий: сущность и классификация / Ж.В. Сухова // инновационные научные исследования: теория, методология, практика. – 2016. – № 6. – С. 72-75.

167. Тарабан, Н.А. Информация о телефонных соединениях как доказательство в уголовном судопроизводстве и источник криминалистически значимой информации при раскрытии преступлений против личности / Н.А. Тарабанов // Российский следователь. – 2014. – № 17. С. 5-9.

168. Тушев, А.А. Информация как основа всех видов доказательств в уголовном процессе / А.А. Тушев, Н.А. Назаров // Общество и право. – 2012. – № 3. – С. 195-197.

169. Федотов, И.С. Электронные носители информации «вещественные доказательства» или «иные документы»? / И.С. Федотов, П.Г. Смагина // Вестник ВГУ. – 2014. – № 3. – С. 191-199.

170. Хайдаров, А.А. Незаконная практика фиксации личной переписки граждан на мобильных устройствах / А.А. Хайдаров // Уголовный процесс. – 2017. – № 5 – С. 36-41.

171. Химичева, О.В. Цифровизация как тренд развития современного уголовного процесса / О.В. Химичева, А.В. Андреев // Вестник Московского университета МВД России. – 2020. – № 3. – С. 21-23.

172. Цыкора, А.А. Некоторые проблемы производства следственного действия «получение информации между абонентами и (или) абонентскими устройствами / А.А. Цыкора // Известия ТГУ. Экономические и юридические науки. – 2013. – № 2-3. – С. 239-244.

173. Черкасов, В.С. Видеоконференц-связь в следственных действиях: как правильно использовать и что поменять в УПК / К.В. Авдонин, В.С. Черкасов // Уголовный процесс. – 2018. – № 7. – С. 46-53.

174. Черных, И.И. Использование видеоконференц-связи в арбитражном процессе / И.И. Черных // Законы России: опыт, анализ, практика. – 2011. – № 10. – С. 154-159.

175. Шампаров, А.В. Особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами / А.В. Шампарова // Публичное и частное право. – 2014. – № 1. – С. 121-128.

176. Шадрин, В.С. Обеспечение прав личности и современные тенденции в российском судопроизводстве / В.С. Шадрин // Закон и власть. – 2021. - № 3. – С. 39-43.

177. Шурухнов, Н.Г. Процедура и содержание процессуальных информационно-технологических средств сбора доказательств, используемых в российской практики расследования преступлений, совершаемых с использование современных электронных технологий / Н.Г. Шурухнов // Вопросы правоведения. – 2013. – № 5. – С. 294-315.

178. Adam, M.G. The iphone meets the fourth amendment / M.G. Adam // UCLA Law Review. – 2008. – Vol. 27. – Pp. 27-58.

179. Doris, K.O.M. The vulnerability of cyberspace – the cyber crime / K.O.M.

Doris // Journal of Forensic science and criminal investigation. – 2017. – 21 February. – Pp. 31-39.

180. Ward, K.B. The plain (or not so plain) view doctrine: applying the plain view doctrine to digital seizures / K.B. Ward // University of Cincinnati Law Review. – 2011. –Vol. 79. Iss. 3. Art. 6. – Pp 1163-1187.

IV. Диссертации и авторефераты диссертации

181. Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дисс. ... канд. юрид. наук: 12.00.09 / Агибалов Владимир Юрьевич – Воронеж, 2010. – 28 с.

182. Архипова, Е.А. Применение видеоконференцсвязи в уголовном судопроизводстве России и зарубежных стран (сравнительно-правовое исследование): дисс. ... канд. юрид. наук: 12.00.09 / Архипова Екатерина Александровна – М., 2013. – 198 с.

183. Батурин Ю.М. Теоретические проблемы компьютерного права: автореф. дисс. … док. юрид. наук: 12.00.01 / Батурин Юрий Михайлович Волгоград, – М., 1991. – 39 с.

184. Вехов, В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дисс. … канд. юрид. наук: 12.00.09. / Вехов Виталий Борисович – Волгоград, 1995. – 276 с.

185. Вехов, В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дисс. … докт. юрид. наук: 12.00.09 / Вехов Виталий Борисович – Волгоград, 2008. – 561 с.

186. Григорьев, О.Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дисс. … кан. юрид. наук: 12.00.09 / Григорьев Олег Геннадьевич – Тюмень, 2003. – 221 с.

187. Зазулин, А.И. Правовые и методологические основы использования использования цифровой информации в доказывании по уголовному делу: дисс.

… кан. юрид. наук: 12.00.09 / Зазулин Анатолий Игоревич – Екатеринбург, 2018. – 251 с.

188. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … кан. юрид. наук: 12.00.09 / Зигура Надежда Анатльевна – Челябинск, 2010. – 234 с.

189. Клементьев, А.С. Телекоммуникационное обеспечение уголовного процесса: дис. ... канд. юрид. наук: 12.00.09 / Клементьев Александ Станиславович – Владимир. 2007. – 175 с.

190. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети интернет: дисс. … канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. – М., 2018. – 199 с.

191. Краснова, Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: дисс. ... канд.юрид. наук: 12.00.09 / Краснова Людмила Борисовна – Воронеж, 2005. – 202 с.

192. Оконенко, Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук: 12.00.09 / Оконенко Роман Иванович – М., 2016. – 156 с.

193. Пастухов, П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дисс. … д-ра юрид. наук: 12.00.09 / Пастухов Павел Сысоевич. – М., 2015. – 64 с.

194. Россинский, С.Б. Модернизация уголовно-процессуального доказывания в условиях информационного общества: дисс. … д-ра юрид. наук: 12.00.09 / Россинский Сергей Борисович. – М., 2016. – 525 с.

195. Рыбин, А.В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты: дисс. ... канд. юрид. наук: 12.00.09 / Рыбин Александр Владимирович – Краснодар, 2005. – 192 с.

196. Сергеев, М.С. Правовые основы применения электронной

информации и электронных носителей информации в уголовном судопроизводстве: дисс. … кан. юрид. наук: 12.00.09 / Сергееви Максим Сергеевич – Казань, 2018. – 322 с.

197. Терещенко, Л.К. Правовой режим информации: дисс. ... д-ра юрид. наук: 12.00.14 / Терещенко Людмила Константиновна – М., 2011. – 415 с.

198. Устинов, А.В. Взаимодействия органов предварительного следствия Российской Федерации с уполномоченными субъектами иностранных государств в целях получения доказательств по уголовному делу: автореф. дис. ...канд. юрид. наук: 12.00.09 / Устинов Алексей Витальевич – М., 2012. – 26 с.

V. Правоприменительная практика

199. Дело «Копланд (Copland) против Соединенного Королевства» (жалоба № 62617/00) Постановление ЕСПЧ от 03.04.2007 // URL: https://base.garant.ru/5732869/

200. Дело «Визер и компания «Бикос бетейлигунген ГмбХ» (Wieser and Bicos Beteiligungen GmbH) против Австрии» (жалоба № 74336/01) Постановление ЕСПЧ от 16 октября 2007 // URL: https://base.garant.ru/5693183/

201. Дело «Колесниченко (Kolesnichenko) против Российской Федерации» (жалоба № 19856/04) Постановление ЕСПЧ от 09.04.2009 // URL: https://base.garant.ru/12173569/

202. Дело «Юдицкая и другие (Yuditskaya and Others) против Российской Федерации» (жалоба № 5678/06) Постановление ЕСПЧ от 12 февраля 2015 // URL: https://base.garant.ru/71354692/

203. Дело «Компании «Винчи Конструксьон» и 2Жэ-Тэ-Эм Жени Сивиль э Сервис» (Vinci Construction and GTM Genie Civil et Services v. France) против Франции» (жалобы № 63629/10 и 60567/10) Постановление ЕСПЧ от 02 апреля 2015 // URL: https://base.garant.ru/71202932/

204. Определение Конституционного Суда РФ от 08 апреля 2010 № 433-О «Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Николая Алексеевича на нарушение его конституционных прав частью первой статьи 176

и частью первой статьи 285 Уголовно-процессуального кодекса Российской Федерации» // URL: https://base.garant.ru/1794804/

205. Определение Конституционного суда РФ от 12 мая 2012 года № 814-О «Об отказе в принятии к рассмотрению жалобы гражданина Аносова Игоря Викторовича на нарушение его конституционных прав статьями 74, 75 и 81 Уголовно-процессуального кодекса Российской Федерации» // URL: http://www.garant.ru/products/ipo/prime/doc/70089288/

206. Определение Конституционного Суда РФ от 26 января 2017 № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации» // URL: https://ukrfkod.ru/pract/opredelenie-konstitutsionnogo-suda-rf-ot-26012017-n-29-o/

207. Определение Конституционного суда РФ от 25 января 2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно- процессуального кодекса Российской Федерации // СПС «Консультант плюс» // URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-25012018-n-189-o/

208. Официальный отзыв Верховного Суда РФ от 07 апреля 2011 № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» // URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=87058

209. Постановление Пленума Верховного Суда РФ от 30.06.2015 № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» // URL: https://www.vsrf.ru/documents/own/8439/

210. Постановлению Первореченского районного суда г. Владивостока № 3/6-248/11 от 29.12.2011 // URL: rospravosudie.com.

211. Апелляционное определение Верховного суда РФ от 04 июня 2013

года № 41-АПУ13-13сп // URL: https: //www.garant.ru/products/ipo/prime/doc/70304792/

212. Кассационное определение от 24 мая 2012 № 22-2225/12 Омского областного суда // URL: https://sudact.ru/regular/doc/3O7EjaCooxZr/

213. Апелляционное определение № 22-2073/2016 Верховного суда Республики Башкортостан от 15 марта 2016 // URL: https://nalogcodex.ru/sud_pract/sou/apellyatsionnoe-opredelenie-verhovnogo-suda-respubliki-bashkortostan-(respublika-bashkortostan)-ot-15.03.2016-_-22-2073_2016

214. Апелляционное определение суда Ненецкого автономного округа по делу № 22-27/2015 от 13 апреля 2015 // URL: https://sudact.ru/regular/doc/UpBwjgpnx4Yx/

215. Апелляционное постановление Приморского краевого суда № 22-5674/15 от 24 сентября 2015 // URL: https://sudact.ru/regular/doc/mcLt94ndnd0/

216. Апелляционное постановление Приморского краевого суда от 02 февраля 2015 № 22 К-455/2015 // URL: https://sudact.ru/regular/doc/VsGt5FRTg35t/

217. Апелляционное постановление Пермского краевого суда от 27 июня 2017 по делу № 22–3815/2017 // URL: https://sudact.ru/regular/doc/TZ4dDIjtG3xQ/

218. Апелляционное постановление Соликамским городского суда № 10-83/2017 Пермского края от 17 октября 2017 // URL: https://sudact.ru/regular/doc/0xG9qjZhfxxQ/

219. Приговору Домодедовского городского суда № 1-5/2017 (1-581/2016;) от 16 февраля 2017 // URL: https://jur24pro.ru/ugolovnye-dela/ugolovnoe-delo-1-5-2017-1-581-2016-/

220. Приговор Волгоградского городского суда от 17 ноября 2016 № 1-914/2016 // URL: https://sudact.ru/regular/doc/hwzIJ69MfXmR/

221. Приговор Урванского районного суда № 1-78/2016 от 23 июня 2016 // URL: https://sudact.ru/regular/doc/bpgp9HJ5eRVw/

222. Приговор Железнодорожного районного суда г. Пензы от 4.08.2016 №1-198/2016 // URL: https://rospravosudie.com.

223. Приговор Ангарского городского суда № 1-394/2016 от 10 мая 2016 //

URL: https://sudact.ru/regular/doc/DOJO7LMgjlYj/

224. Приговор Курганского городского суда № 1-480/2013 от 25.12. 2013 // URL: https://sudact.ru/regular/doc/pgWaScvpEb12/

225. Приговор Октябрьского районного суда г. Екатеринбурга 1-310/2014 от 02 февраля 2015 // URL: https://sudact.ru/regular/doc/g14oYbyVVFbB/

226. Приговор Воркутинского городского суда № 1-362/2017 от 03.11.2017 // URL: https://sudact.ru/regular/doc/65iTmvghAqmv/

227. Приговор Ясногорского районного суда от 1.02..2016 № 1–1/2016 // URL: // https://sudact.ru/regular/doc/GwUF4hU8L2Hp/

228. Приговор Верховного суда Республики Татарстан № 22-4290/2016 от 28 июня 2016 // URL: https://sudact.ru/regular/doc/3n1HEzIZwaLp/

229. Уголовное дело № 1-113/17 // Архив Центрального районного суда г. Хабаровска.

VI. Информационные, аналитические, статистические и иные материалы, материалы на иностранном языке, электронные ресурсы

230. Статистика преступлений, совершаемых при помощи компьютерных и телекоммуникационных технологий за 2015-2020 год / ГИАЦ МВД России; Состояние преступности в Российской Федерации // URL: https://xn--b1aew.xn--p1ai/search/

231. Neuralink нейроинтерфейс для чтения мыслей и управления компьютерами // URL: https://www.popmech.ru/science/493952-neuralink-neyrointerfeys-dlya-chteniya-mysley -i-upravleniya-kompyuterami/#part0.

232. Политическая дороговизна IP-телефонии // URL: https://www.osp.ru/lan/1996/02/131926.

233. Полный охват цифровым телевидением территории Дальнего Востока обойдется в 7 миллиардов рублей // URL: https://www.dvnovosti.ru/khab/2018/02/27/79502/

234. Вирус «Wanna cry» заразил десятки тысяч компьютеров по всему миру // URL: https://www.1tv.ru/news/2017-05-13/325201

235. Заключение комитета Государственной Думы по государственному строительству и законодательству от 21 октября 2016 года по проекту федерального закона № 764131-6 // URL: https:// http://sozd.parlament.gov.ru/ bill/764131-6.

236. Законопроект от 05 апреля 2018 № 434998-7 // URL: https://lawmon.ru/ law/ 434998-7. html

237. Характеристики и возможности современной IP-телефонии // URL: http://www.victel54.ru/ip_tel/about/

238. Дэниел П. Дэрн, Пол Десмонд. «Позвоним через IP?» / Сети / Network world. 1997. № 8 // URL: http://www.osp.ru/nets/1997/08/142803/

239. Данные о появлении компании «Skape» // URL: https://www.skype.com/ ru/about/

240. Типовой закон об электронной торговле // URL: https://www.uncitral.org/pdf/ russian/texts/electcom/ 05-89452_Ebook.pdf

231. Фитнес-приложение раскрыло расположение военных баз США // URL: https://www.popmech.ru/technologies/news-407982-fitnes-prilozhenie-raskrylo-raspolozhenie-voennyh-baz-ssha/

232. Приложение Uber следит за своими пользователями // URL: https://tjournal.ru/38587-byvshiy-sotrudnik-uber-obvinil-kompaniyu-v-slezhke-za-polzovatelyami.

233. Дуров не отдает ключи от Telegram. Что будет с мессенджером? // URL: https:// hitech-vesti-ruampproject.org.

234. ГОСТ 33707-2016 «Информационные технологии. Словарь» / введен в действие Приказом Росстандарта от 22.09.2016 № 1189-ст. // URL: https://docs.cntd.ru/ document/ 1200139532.

235. Энциклопедия «Кругосвет» // URL: http://www. krugosvet.ru

236. Толковый словарь русского языка В.В. Лопатин. // URL: http://www.вокабула.рф (дата обращения: 20.01.2021 г.).

237. 计算机犯罪现场勘验与电子证据检查规则 (公信安[2005]161号 公安部) / «Положение о процедуре осуществления осмотра места преступления,

совершенного с применением средств информационно-цифровых технологий и проверки электронных доказательств» МОБ КНР 2005 / пер. Манцуров А.Ю. // URL: http://www.360doc.com/content/17/1121/23/44284862_706004600.shtml.

Приложение 1

РЕЗУЛЬТАТЫ АНТЕТИРОВАНИЯ
118 следователей (26 МВД РФ, 92 СК РФ)

1. Привлекается ли Вами специалист для изъятия электронного носителя информации?

да, так как его отсутствие влечет недопустимость доказательств	70,3% (83)
да, но только в тех случаях, когда действительно нужны специальные познания, а не из-за того что это влечет недопустимость доказательств	22,9% (27)
нет, отсутствие специалиста не влечет недопустимость доказательств	5,1% (6)
затрудняюсь ответить (или свой вариант)	1,70% (2)

2. Привлекается ли Вами специалист для копирования информации с электронных носителей?

да, так как его отсутствие влечет недопустимость доказательств	68,6% (81)
да, но только в тех случаях, когда действительно нужны специальные познания, а не из-за того что это влечет недопустимость доказательств	22,9% (27)
нет, отсутствие специалиста не влечет недопустимость доказательств	4,25% (5)
затрудняюсь ответить (или свой вариант)	4,25% (5)

3. Как вы оцениваете требование ч. 9.1. ст. 182 и ч. 3.1. ст. 183 УПК РФ, предусматривающее обязательное участие специалиста при изъятии электронного носителя информации и копировании с него информации?

отрицательно, так как процесс изъятия электронных носителей и копирования с них информации в большинстве случае не требует специальных познаний	50% (59)
положительно	42,4% (50)
затрудняюсь ответить (или свой вариант)	7,6% (9)

4. Как Вы считаете, есть необходимость по исключению из УПК РФ требования по обязательному участию специалиста при изъятии электронных

носителей и копировании с них информации, а необходимость участие специалиста оставить на усмотрение следователя?

Да	74,6% (88)
Нет	14,4% (14)
затрудняюсь ответить (или свой вариант)	5% (6)

5. При производстве осмотра предметов (смартфона, планшета, ноутбука и т. д.) или назначения судебной экспертизы, с целью исследовать и приобщить к материалам уголовного дела содержания электронных сообщений, Вами получается отдельное судебное решение?

да, так как подобная информация попадает под тайну связи	17% (20)
нет, подобных требовании УПК РФ не содержит	81,3% (96)
затрудняюсь ответить (или свой вариант)	1,7 (2)

6. По Вашему **субъективному** мнению, электронные сообщения, доступ к которым производится, посредством оконечного оборудования пользователя (смартфон, ноутбук и т. д.), при расследовании уголовного дела, попадают под действие режима тайны связи?

Да	41,5% (49)
Нет	58,5% (69)

7. Склоны ли Вы при оценке доказательств, считать полученную электронно-цифровую информацию (-аудио -видеозапись, изображение, сайт в сети «Интернет» и т. д.) как недостоверную?

да, так как в электронно-цифровую информацию можно легко внести изменения	28% (33)
нет, так как подобная информация формируется по детерминированным аппаратно-программным алгоритмам	65,1% (77)
затрудняюсь ответить (или свой вариант)	6,9% (8)

8. Подвергаете ли Вы дополнительной проверки электронно-цифровую информацию (к примеру, назначаете компьютерно-техническую экспертизу и т. д.) собранную, в рамках следственных действий, в том числе полученную от участников уголовного судопроизводства (свидетеля, потерпевшего, подозреваемого и т. д.)?

да, во всех случая производится дополнительная проверка достоверности (аутентичности)	12% (14)
да, но только в тех случаях когда, когда информация получена от участника уголовного судопроизводства	3,6% (4)
да, но только в отдельно взятых случаях, когда есть сомнение в достоверности электронно-цифровой информации, что зависит от	76,2% (90)

конкретных обстоятельств уголовного дела	
нет	6,8% (8)
затрудняюсь ответить (или свой вариант)	1,7 (2)

9. Вы когда-нибудь использовали в своей деятельности систему видеоконференц-связи?

да (допрос, очная ставка, продления стражи)	11% (13)
нет	88,1% (104)
затрудняюсь ответить (или свой вариант)	0,9% (1)

10. Как вы считаете, потенциально, при каких процессуальных действиях допустимо использовать видеоконференц-связь (**нужное подчеркнуть)?**

Да (допрос, очная ставка, предъявление для опознания)	87,3% (103)
использовать нельзя	11% (13)
затрудняюсь ответить (или свой вариант)	1,7% (2)

11. Есть ли необходимость по внедрению видеоконференц-связи в уголовное досудебное производство?

Да	81,4% (96)
Нет	17,7% (21)
затрудняюсь ответить (или свой вариант)	0,9% (1)

12. Производили ли Вы когда-нибудь арест электронных сообщений?

Да	6,7% (8)
Нет	92,4% (109)
затрудняюсь ответить (или свой вариант)	0,9% (1)

13. Как вы считаете, действующие уголовно-процессуальные механизмы по собиранию электронно-цифровой информации нуждаются в совершенствовании?

Да	87,3% (103)
Нет	11% (13)
затрудняюсь ответить (или свой вариант)	1,7 (2)

14. Как вы считаете, необходимо ли в УПК РФ предусмотреть универсальное следственное действие, направленное на получение информации из «киберпространства», которое объединит в себе такие возможности как: арест электронных сообщений (или области «киберпространства», к примеру, аккаунта в соц. сети); контроль (перехват), мониторинг, сообщений передаваемых по электросвязи (классическая телефонная, телематическая (интернет) связь, электронные сообщения, геолокация и т. д.), получение содержания электронных сообщений от интернет-сервисов («Whatsapp», «Вконтакте», «Одноклассники» и т. д.)?

Да	91,5% (108)
Нет	7,6% (9)
затрудняюсь ответить (или свой вариант)	0,9% (1)

15. В качестве какого вида доказательств Вы приобщаете к материалам уголовного дела электронно-цифровую информацию, которая находится на материальном носители?

Вещественные доказательства	82,1% (97)
Иные документы	15,3% (18)
затрудняюсь ответить (или свой вариант)	2,6% (3)

16. Как Вы считаете, достаточно ли в ч. 2 ст. 74 УПК РФ видов (источников) доказательств для приобщения к материалам уголовного дела различных форм электронно-цифровой информации?

да, виды доказательств, содержавшиеся в ч. 2 ст. 74 УПК РФ, в полной мере позволяют приобщать электронно-цифровую информацию к материалам уголовного дела	67,7% (80
нет, электронно-цифровая информация имеет особую природу и необходимо предусмотреть новый источник уголовно-процессуальных доказательств	31,4% (37)
31,4% (37)	0,9% (1)

17. Как Вы считаете, есть ли необходимость дополнить УПК РФ новым объектом следственных действий электронно-цифровой информацией (компьютерной информацией)?

Да	64,4% (76)
Нет	33,9% (40)
затрудняюсь ответить (или свой вариант)	1,7% (2)

Приложение 2

РЕЗУЛЬТАТЫ АНТЕТИРОВАНИЯ
418 сотрудников органов предварительного расследования
207 следователей МВД РФ, 96 дознавателей МВД РФ, 115 следователей СК РФ

1. Возникает ли у Вас потребность в использовании в качестве доказательств по уголовному делу сведений из электронно-информационной сферы (переписку из социальных сетей, геолокационные данные, видеозвонки и т. д.)?

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	166	107	78	351
Нет	41	8	18	67
	80,20%	93%	81,25%	84%
	19,80%	7%	19,75%	16%

2. Как Вы считаете, должны ли в условиях современного научно–технического прогресса общества, в качестве доказательств обширно и повсеместно использоваться сведения из электронно-информационной сферы (переписка из социальных сетей, геолокационные данные, видеозвонки и т. д.)?

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	171	114	91	376
Нет	36	1	5	42
	80,60%	99,13%	94,80%	89,95%
	19,40%	0,87%	5,20%	10,05%

3. Знаете ли Вы, при помощи каких следственных действий возможно получать сведения из электронно-информационной сферы (переписку из социальных сетей, геолокационные данные, видеозвонки и т. д.)?

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	143	106	76	325
Нет	64	9	20	93
	68,75%	92,20%	79,20%	77,70%
	31,25%	7,80%	20,80%	22,30%

4. Как Вы считаете, уголовно-процессуальное законодательство позволяет в достаточных объемах получать сведения из электронно–информационной сферы?

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	64	72	32	169
Нет	143	43	64	249
	31,25%	62,60%	33,30%	40,30%
	68,75%	37,40%	66,70%	59,70%

5. Возникала ли у Вас потребность, в использовании программно-аппаратных средств или киберпространства (сети «Интернет») при производстве следственных действий (к примеру, допроса через «Skype», «Viber», производство следственного эксперимента в социальных сетях и т. п.)

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	81	67	34	182
Нет	126	48	62	236
	39,13%	58,26%	34,42%	43,54%
	60,87%	41,74%	60,58%	56,46%

6. Как Вы считаете, есть ли необходимость реформирования уголовно-процессуального законодательства в целях создания юридических условий для получения и использования в качестве доказательств, сведений из электронно–информационной сферы в уголовном досудебном производстве?

	Следователи		Дознаватели МВД	Общее
	МВД	СК		
Да	158	95	91	344
Нет	49	20	5	74
	76,30%	82,60%	94,80%	82,30%
	23,70%	17,40%	5,20%	17,70%

Приложение 3

Проект федерального закона «О внесении изменений в статьи 5, 29, 164, 164.1, 176, 182, 183, 186, 186.1, 187, 191, 195 Уголовно-процессуального кодекса Российской Федерации, а также дополнении Уголовно-процессуального кодекса Российской Федерации статьей 164.2»

Внести в Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ, принятый Государственной Думой Федерального Собрания Российской Федерации 22.11.2001 следующие изменения:

1) Изложить пункт 14.1. статьи 5 в следующей редакции:

«14.1) контроль электросвязи – мониторинг голосовой информации, изображения, звука, видео-, иных форм телекоммуникации пользователей электросвязи, получение содержания телекоммуникации, в установленных федеральным законом случаях, от операторов связи и организаторов распространения информации в сети «Интернет», арест телекоммуникаций».

2) часть 2 статьи 29 дополнить пунктом 4.1 следующего содержания

«4.1) О производстве обыска и (или) экспертизы в отношении электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи».

3) часть 5 статьи 165 изложить в следующей редакции: В исключительных случаях, когда производство осмотра жилища, обыска и выемки в жилище, обыска электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемые посредством электросвязи, личного обыска, а также выемки заложенной… (далее по тексту закона)».

4) часть 2 статьи 164.1. УПК РФ изложить в следующей редакции: «Следователь в ходе производства следственного действия вправе осуществить изъятие электронных носителей информации и копирование с них информации. Изъятие электронных носителей информации осуществляется с соблюдением ограничений установленных ч. 1 ст. 164.1. УПК РФ. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные

носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются изъятые электронные носители информации или электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия».

Часть 3 ст. 164.1. УПК РФ изложить в следующей редакции:

«По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации, с изымаемых электронных носителей информации осуществляется копирование информации. Копирование информации осуществляется на другие электронные носители информации, которые могут быть предоставлены законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Копирование информации не осуществляется при наличии обстоятельств, указанных в пункте 3 части первой настоящей статьи. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись».

5) часть 1 статью 176 изложить в следующей редакции:

«1. Осмотр места происшествия, местности, жилища, иного помещения, электронного носителя информации, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела».

7) Статью 176 дополнить частью 6.1.:

«6.1. Осмотр электронного носителя информации производится только с согласия его владельца или лица, предоставляющего компьютерную

информацию, в ином случае производится обыск в порядке ч. 3.1. ст. 182 настоящего Кодекса».

6) Статью 182 дополнить частью 3.1. следующего содержания:

«3.1. обыск электронного носителя информации, функционально предназначенного для обмена и воспроизведения сведений, передаваемых посредством электросвязи, производится на основании судебного решения, принимаемого в порядке, установленном ст. 165 настоящего Кодекса. Если электронный носитель информации не обладает свойствами обмена и воспроизведения сведений, передаваемых посредством электросвязи, но имеется возражение владельца, то обыск производится на основании постановления следователя».

7) Исключить часть 9.1. из статьи 182 и часть 3.1. из статьи 183.

8) Исключить из часть 7 из статьи 185.

9) Статью 186 УПК РФ изложить в следующей редакции:

«Статья 186. Контроль электросвязи

1. При наличии достаточных оснований полагать, что сведения, передаваемые подозреваемым, обвиняемым и другими лицам посредством электросвязи могут иметь значение для уголовного дела, допускается производство контроля данных сведений в порядке, установленном статьей 165 настоящего Кодекса.

2. При наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких родственников, родственников, близких лиц получение, исследование и запись телекоммуникации допускается по письменному заявлению указанных лиц, а при отсутствии такого заявления - на основании судебного решения.

3. В ходатайстве следователя о производстве контроля электросвязи:

1) уголовное дело, при производстве которого необходимо применение данной меры;

2) основания, по которым производится данное следственное действие;

3) фамилия, имя и отчество лица, телефонные номер, адрес электронной почты, доменное имя, а так же иную информацию позволяющую идентифицировать пользователя электросвязи:

4) период осуществления контроля электросвязи;

5) действия по контролю электросвязи или их совокупность, необходимых в рамках контроля электросвязи: мониторинг телекоммуникации, получение телекоммуникации от операторов связи и (или) организаторов распространения информации в сети «Интернет», наложение ареста на телекоммуникации.

6) наименование органа, которому поручается техническое осуществление контроля электросвязи.

4. Постановление о производстве контроля электросвязи направляется в соответствующий орган.

5. В рамках одного постановления допустимо производить, как одно действие по контролю электросвязи, так и их совокупность: мониторинг телекоммуникации, получение телекоммуникации от операторов связи и (или) организаторов распространения информации в сети «Интернет», наложение ареста на телекоммуникации.

6. Контроль электросвязи может быть установлен до 6 месяцев. Ретроспективный период получения содержания телекоммуникации от оператора связи и (или) организатора распространения информации в сети «Интернет» определяется федеральным законодательством. Контроль электросвязи прекращается по постановлению следователя, с обязательным уведомлением об этом суда, принявшего решение о наложении ареста, и прокурора, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу. При завершении производства контроля электросвязи, возобновляется доступ пользователя к функциональным возможностям коммуникационного интернет-сервиса путем восстановления данных авторизации.

7. Арест телекоммуникаций состоит в ограничении доступа к электронным сообщениям пользователя электросвязи, путем модификации данных

авторизации, необходимых для получения доступа к функциональным возможностям коммуникационного интернет-сервиса. Модификацию данных авторизации пользователя коммуникационного интернет-сервиса производит организация, исполняющие постановление о контроле электросвязи. Организация, исполняющая постановление о контроле электросвязи предоставляет следователю данные для авторизации в коммуникационном интернет-сервисе в качестве пользователя, в отношении которого был произведен арест телекоммуникаций, для последующего осмотра содержания электронных сообщений.

8. Следователь вправе самостоятельно произвести арест телекоммуникаций пользователя электросвязи путем модификации данных авторизации, необходимых для получения доступа к функциональным возможностям коммуникационного интернет-сервиса. Модификация данных авторизации, производится в присутствии понятых. Порядок модификации данных авторизации фиксируется в протоколе.

9. Следователь в течение всего срока производства контроля электросвязи вправе в любое время произвести осмотр электронных сообщений (документа) и (или) истребовать от органа, осуществляющего контроль электросвязи, электронный носитель информации, содержащий телекоммуникацию пользователя электросвязи, для осмотра. Электронный носитель информации передается следователю в опечатанном виде с сопроводительным письмом, в котором должны быть указаны даты и время начала и окончания записи телекоммуникации и краткие характеристики использованных при этом технических средств.

10. О результатах осмотр электронных сообщений (документа) и (или) электронного носителя информации, содержащего телекоммуникацию пользователя электросвязи, следователь с участием специалиста (при необходимости), составляет протокол, в котором должна быть дословно изложена та часть телекоммуникации, которая, по мнению следователя, имеет отношение к данному уголовному делу. Лица, участвующие в осмотре электронного носителя

информации, содержащего телекоммуникацию пользователя электросвязи, вправе в том же протоколе или отдельно изложить свои замечания к протоколу.

11. Электронный носитель информации, содержащий телекоммуникацию пользователя электросвязи приобщается к материалам уголовного дела на основании постановления следователя как вещественное доказательство и хранится в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования телекоммуникации пользователя электросвязи посторонними лицами и обеспечивающих ее сохранность и техническую пригодность для повторного прослушивания, в том числе в судебном заседании».

10) Статью 186.1. изложить в следующей редакции:

«Статья 186.1. Получение информации о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях.

1. При наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном статьей 165 настоящего Кодекса.

2. В ходатайстве следователя о производстве следственного действия, касающегося получения информации о соединениях между абонентами и (или) абонентскими, устройствами, а также телекоммуникационных соединениях указываются:

1) уголовное дело, при производстве которого необходимо выполнить данное следственное действие;

2) основания, по которым производится данное следственное действие;

3) период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия;

4) наименование организации, от которой необходимо получить указанную информацию.

3. В случае принятия судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а также о телекоммуникационных соединениях, его копия направляется следователем в соответствующую осуществляющую услуги связи организацию, руководитель которой обязан предоставить указанную информацию, зафиксированную на любом материальном носителе информации. Указанная информация предоставляется в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств, а также иные идентификационные данные о пользователях сети «Интернет» и телекоммуникационных соединениях.

4. Получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях может быть установлено на срок до шести месяцев и неограниченном ретроспективном периоде. Соответствующая осуществляющая услуги связи организация и (или) организатор распространения информации в сети «Интернет» обязаны направить необходимую информацию не позднее 10 суток с момента получения постановление суда о производстве следственного действия. Соответствующая осуществляющая услуги связи организация и (или) организатор распространения информации в сети «Интернет» в течение всего срока производства данного следственного действия обязаны предоставлять следователю указанную информацию по мере ее поступления, но не реже одного раза в неделю.

5. Следователь осматривает представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях с участием специалиста (при необходимости), о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов, сетевой адрес, доменное имя, идентификатор пользователя сети «Интернет»,

логин, пароль и другие данные). Лица, присутствовавшие при составлении протокола, вправе в том же протоколе или отдельно от него изложить свои замечания.

6. Представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, а также телекоммуникационных соединениях, приобщаются к материалам уголовного дела в полном объеме на основании постановления следователя как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

7. Если необходимость в производстве данного следственного действия отпадает, его производство прекращается по постановлению следователя, но не позднее окончания предварительного расследования по уголовному делу.

11) Изложить часть 1 статьи 195 в следующей редакции:

«1. Признав необходимым назначение судебной экспертизы, следователь выносит об этом постановление, а в случаях, предусмотренных пунктами 3 и 4.1 части второй статьи 29 настоящего Кодекса, возбуждает перед судом ходатайство, в котором указываются:».