Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

«Южно-Уральский государственный университет
(национальный исследовательский университет)»

ЮРИДИЧЕСКИЙ ИНСТИТУТ

Кафедра «Правоохранительная деятельность и национальная безопасность»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.02. 2015.164. ВКР

Руководитель работы,
_____С.В. Зуев
_____2020 г.

Автор работы,
Студент группы Ю-516
_____В.А. Спиридонова
_____2020 г.

Нормоконтролер,
Преподаватель
_____Н.В. Агаркова
_____2020 г.

Челябинск

2020

АННОТАЦИЯ

Спиридонова В.А. Выпускная квалификационная работа «Информационные технологии в деятельности правоохранительных органов»: ФГАОУ ВО «ЮУрГУ (НИУ)», Ю-516, 106 с., библиогр. список – 80 наим., прил. 5.

Объектом исследования являются общественные отношения, возникающие в сфере применения информационных технологий при осуществлении правоохранительной деятельности.

Предметом исследования является законодательство Российской Федерации, определяющее возможности и закономерности пользования информационными технологиями сотрудниками правоохранительных органов.

Цель выпускной квалификационной работы состоит в изучении и анализе действующего законодательства в сфере использования информационных технологий, а также разработке предложений направленных на усовершенствование практической деятельности сотрудников правоохранительных органов.

В работе освещены понятия «информация» и «информационные технологии», применение и использование информационных технологий в деятельности правоохранительных органов, отражена актуальность такого использования и позитивные последствия использования информационных технологий в правоохранительной деятельности.

Результаты работы имеют практическую значимость, содержат выводы и предложения автора по проблемам, связанным с применением ииспользованием информационных технологий и анализа практики такого применения. Результаты исследования могут быть полезны при разработке программ обучения юристов, а также в преподавании предметов «Тактико-специальная подготовка», «Правоохранительные органы», «Уголовно-процессуально право», «Административный процесс».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В XXI веке информационные технологии в жизни человека и, в целом, общества занимают первостепенное место. Век информатизации и технологического прорыва охватывает практически все сферы жизни, так, например, сфера услуг, медицина, экономика, культура, социальное развитие населения.

Следует отметить, что актуальность выпускной квалификационнойработы обусловлена большим количеством людей, использующих телекоммуникационные системы для решения каких-либо задач или проблем. Данное заявление можно утвердить результатами выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей[1](далее – обследование ИКТ), проводимого Федеральной службы государственной статистики Российской Федерации в 2018 году среди населения в возрасте 15 лет и старше. Так, 74,3 % респондентов считают, что являются активными пользователями информационно-телекоммуникационной сети «Интернет», 32,3 % –используют сеть «Интернет» только для заказов товаров и (или) получения услуг, а 0,4 % – вовсе не пользуются сетью «Интернет» по соображениям безопасности. При этом необходимо отметить, что использование информационных технологий не ограничивается какими-либо возрастными пределами, в рамках обследования ИКТ также было установлено, что самыми активными пользователями сети «Интернет» являются граждане в возрасте 30-34 лет (12,3 %), 25-29 лет (11,7 %) и 60-69 лет (11,0 %), а самыми

[1] Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей. Официальный сайт Федеральной службы государственной статистики Российской Федерации [Электронный ресурс]. Режим доступа. URL: https://gks.ru/free_doc/new_site/business/it/fed_nabl-croc/index.html (дата обращения 01.03.2020)

неактивными пользователями сети «Интернет» считается население в возрасте 70-79 лет (2,8 %) и старше 80 лет (0,8 %).

Говоря о возможностях и способах получения информации необходимо упомянуть и о праве на её анализ, сбор и хранение. Согласно части 1, статьи 8 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ[1](далее – ФЗ «Об информации, информационных технологиях и о защите информации») физические и юридические лица вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законодательствомРоссийской Федерации. Данная норма, в том числе, позволяет гражданам защищать свои права и свободы всеми способами, не запрещенными законом, что регламентировано частью 2, статьи 45 Конституции Российской Федерации, например, направлять в правоохранительные органы заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях в электронной форме.

Не смотря на государственное регулирование данных вопросов, в законодательстве, всё-таки, имеются значительные пробелы в сфере использования информационных технологий. Законодательно и практически недоработаны формы и способы получения электронных документов, необходимых для осуществления правоохранительной деятельности, а также отсутствуют способы внедрения в гражданское общество пользования электронными ресурсами, что обуславливает факт исследования темы в рамках данной выпускной квалификационной работы.

Цель выпускной квалификационнойработы состоит в изучении и анализе действующего законодательства в сфере использования информационных технологий, а также разработке предложений

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

направленных на усовершенствование практической деятельности сотрудников правоохранительных органов.

Объект – общественные отношения, возникающие в сфере применения информационных технологий при осуществлении правоохранительной деятельности.

Предметом исследования является законодательство Российской Федерации, определяющее возможности и закономерности пользования информационными технологиями сотрудниками правоохранительных органов.

Достижению поставленной цели способствует решение следующих основных задач: проанализировать и определить такие понятия как «информация», «информационные технологии»; исследовать действующее законодательство, регулирующее использование информационных технологий; исследовать имеющийся практический опыт применения информационных технологий в деятельности правоохранительных органов; изучить основания и условия применения информационных технологий в правоохранительной деятельности; определить законодательные пробелы и практические проблемы использования информационных технологий;изучить и проанализировать зарубежный опыт применения информационных технологий при раскрытии и расследовании преступлений; разработать рекомендации по совершенствованию механизма применения информационных технологий при осуществлении правоохранительной деятельности.

В основу исследования положены методы системно-правового анализа положений закона, новейших научных достижений с использованием сравнительно-правового метода научного познания и практической действительности, анкетирования и анализа статистических сведений.

Теоретической основой исследования послужили работы таких авторов, как И.А. Мизин, И.Н. Синицын, Б.Г. Доступов, С.В. Зуев, А.К. Айламазян, В.К. Захарова, В.Д. Курушин и другие.

Значимость и новизна данной работы заключается в том, что были предложены законопроект о внесении изменений и дополнений в Уголовно-процессуальный кодекс Российской Федерации, а также способы внедрения использования гражданским обществом информационных технологий в целях обеспечения прав и свобод.

Структура выпускной квалификационной работы определена характером исследуемых в ней вопросов. Работа состоит из введения, двух глав, включающихпять параграфов, заключения, библиографического списка и приложений.

1 ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Информация и информационные технологии в современной сфере телекоммуникационных отношений

Прежде чем приступить к формированию понятия «информация» в правовом аспекте, по мнению автора, необходимо прибегнуть к лингвистико-теоритическому анализу данного понятия.

Общество нашего времени можно справедливо назвать информационным. Сейчас важно владеть информацией, передовые и развитые страны такие, как Япония, Китай и Сингапур, обладают важнейшим ресурсом – людьми, которые могут преобразовывать и интегрировать различные активы в более сложные виды информации: поисковые и вычислительные системы, новейшие компьютерные разработки и цифровые устройства.

Хоть общество сегодняшнего дня и считается информационным, подавляющее большинство людей не могут дать разъяснение понятию «информация». По наблюдениям И.В. Лысак люди понимают слово «информация» больше на интуитивном уровне, однако не могут объяснить чем же всё-таки является информация[1]. В переводе с латинского языка informātiō, то есть информация, переводится как разъяснение, представление, понимание чего-либо. По мнению С.И. Ожегова информация представляется сведениями об окружающем мире и протекающих в нём процессах, воспринимаемыми человеком или специальным устройством[2]. Таким образом, в обыденном понимании информация воспринимается как синоним

[1] Лысак И.В. Информация как общенаучное и философское понятие: основные подходы к определению // Философские проблемы информационных технологий и киберпространства. 2015. № 2. С. 9–26.

[2] Ожегов С.И. Толковый словарь русского языка / под ред. Н.Ю. Шведова. 4-е изд. М.: Азбуковник, 2000. С. 24.

словам: сведения, сообщение, факт, данные, суждение, то есть, информация позволяет человеку быть осведомленным в чём-либо.

По настоящий момент ведутся дискуссии и в различных сферах науки в определении понятия «информация», а терминология данного понятия так и не нашла своего точного и единого определения. До сих пор многие ученые спорят, из чего состоит информация, имеет ли она какое-либо материальное или когнитивное представление. Прежде всего, это обусловлено тем, что «информация» сама по себе имеет первородное представление наряду с понятиями «энергия» и «материя», если пытаться объяснить данное понятие производными от него словами смысл и трактовка может изменить своё истинное значение, а также ввести в заблуждение иными неопределенными понятиями.

Вообще, в науке определены несколько подходов к пониманию термина «информация». Первоначальным подходом считается математический, введенный основоположником кибернетики, К. Шенноном, который считал, что информация непрерывно связана с энтропией (неопределенными и непредсказуемыми явлениями), и считается единицей снятия системных неопределённостей. Таким образом, чем больше человек принимает и обрабатывает информацию о какой-либо системе, тем более она становиться понятной и предсказуемой[1]. Однако данный подход к определению информации как условной единицы не давал представление о её сущности. Необходимо отметить, что К. Шеннон впервые определил информацию как массив информации, то есть придал ей количественное значение и ввел понятие «бит», которое до сих используется в компьютерных системах для определения и обозначения количества информации.

Противоположным мнением о сущности информации обладал американский ученый Н. Винер, который считал, что «информация есть

[1] Борисенко А.А. О сущности информации // Фундаментальные исследования. 2005. №7. С. 32–33.

информация, а не материя или энергия»[1]. Таким образом, сформировался семантический подход к пониманию информации, согласно которому информация не что иное, как содержание внешних процессов окружающего мира, но при этом количество информации не имеет никакого значения.

Анализируя оба подхода к пониманию информации, справедливо будет заметить мнение С.В. Зуева, что теории К. Шеннона и Н. Винера пришли к оппозиционному противостоянию: К. Шеннон утверждал, что информация уменьшает незнание, а Н. Винер предполагал, что информация наоборот увеличивает знание. Однако оба этих подхода не раскрывали сущность понятия, подразумевая под информацией «нечто», связанное и влияющее на меру энтропии или знания[2].

По истечении времени ученые неоднократно возвращались к определению понятия «информация» с целью определить её сущность и значение. Научное общество больше отталкивалось от мнения Н. Винера, что информация не имеет какого-либо своего субстанционального значения, не является ни энергией, ни материей, то есть, информация является третьей силой, которая независима от двух других. Так и появилась субстанциональная теория информации. Основоположниками данной теории стали Т. Стоинер, В.А. Гадасин, Л. Берталанфи. Л. Берталанфи утверждал, что информация по своей сущности должна восприниматься как энергия, то есть как физическая величина[3], а Т. Стоинер предполагал, что информация существует сама по себе и не нуждается в том, что бы её обрабатывали или интерпретировали, она присутствует в окружающем мире независимо от носителя или протекающих процессов[4].Российский исследователь В.А.

---

[1] Винер Н. Кибернетика или управление и связь в животном и машине; или Кибернетика и общество. 2-е издание. М., Главная редакция изданий для зарубежных стран, 1983. С. 46.

[2] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 12.

[3]Берталанфи Л. Общая теория систем: Критический обзор // Исследования по общей теории систем: Сборник переводов / под ред. Э.Г. Юдина. М.: Прогресс, 1969. С. 23–82.

[4]Стоинер Т. К новой теории информации. Информационная революция: наука, экономика, технология: рефератив. сборник / под ред. А.И. Ракитова. М., 1993. С. 42–48.

Гадасин, в свою очередь, определял, что информация не имеет никакого вещественного представления, она также нематериальна как мыслительные процессы человека, выражающиеся в идеях, словах, мыслях[1]. Однако источники воспроизведения информации или её носители могут быть предметами материального мира, то есть сам человек, технические средства и иное.

Данный подход всё ещё не удовлетворял научное сообщество, потому что информация не обрела материального значения, её нельзя было как-либо подтвердить или опровергнуть с помощью научных способ или экспериментов, информация до сих пор определялась как «нечто», что нельзя почувствовать или увидеть.

Следующим подходом к информации считается функциональный подход, который, в свою очередь, стал основополагающим элементом развития синергетической теории информации. Сторонники данной теории, такие как Д.С. Чернавский и Е.А. Седов, считали, что информация – это исключительное свойство самоорганизуемых и саморегулирующих систем, в которых информационные процессы используются как функции[2]. При этом ученые подчеркивали, что те самые системы, в которых функционируют информационные процессы, исключительно являются биологическими и социальными. Например, П.В. Копнин полагал, что информация не является атрибутом материи, она принадлежит не всем её формам и видам. Информация касается отдельных видов отражения. Если рефлекс связан с мозгом, то информация – со сложнодинамической системой управления[3].

Одновременно с функциональным подходом развивался атрибутивный подход к информации, который предполагал, что информация присуща всем системам, не только саморегулирующим, и существует не как исключительное свойство, а как атрибут, то есть имманентное свойство.

---

[1]Гадасин А.В. Концепция триад понятие «информация» как субстанции // Ежегодник ВНИИПВТИ: сб. науч. трудов. Минск, 2007. С. 186–190.

[2] Седов Е.А. Эволюция и информация. М.: Наука, 1976. С.19.

[3]Копин П.В. Введение в марксистскую гносеологию. Киев: Наукова Думка, 1966. С. 47.

С. Идальго справедливо отметил, что информация является не вещью или материей, а соотношением физический вещей[1]. Таким образом, атрибутивный подход отражал, что объекты материального мира накладывают друг на друга отпечаток информационного следа, который возникает вследствие их взаимодействия. Данный информационный след может быть как видимым, там и невидимым. Например, взаимодействие человека с персональным компьютером: напечатанный человеком текст на персональном компьютере – видимый след, изучение человеком уже напечатанной научной литературы в электронном формате – невидимый след.

Исходя из содержания вышеперечисленных подходов, можно сделать вывод о том, что информация остается достаточно сложной категорией, которая и в настоящее время не исследована полностью. Не смотря на это, информация занимает первостепенное место в различных сферах современного общества. Встречается в экономике, медицине, прикладных науках, социальных отношениях. Не исключением является юриспруденция.

Согласно пункту 1, части 2 ФЗ «Об информации, информационных технологиях и о защите информации», по мнению законодателя, информация – сведения (сообщения, данные) независимо от формы их представления. Очевидно, что в нормативно-правовом акте отражается бытовое понимание информации, что не всегда позволяет эффективно регулировать общественные отношения. Также законодатель закрепил два базовых вида информации: общедоступная и закрытая информация.

Общедоступная информация представляет собой сведения, которые стали известны неопределенному кругу лиц посредством использования сети «Интернет». Например, Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8-ФЗ регулирует отношения,

[1] Идальго С. Как информация управляет миром. М., 2016. С. 8

связанные с распространением и получением информации о деятельности государственных органов и органов местного самоуправления[1]. Согласно данному нормативно-правовому акту государственные органы и органы местного самоуправления обязаны предоставлять информацию о своей деятельности путем различными способами, в том числе посредством сети «Интернет». Как пример общедоступнойинформации выступает информация, полученная посредством распространения её средствами массовой информации. Так, согласно статье 2 Закона Российской Федерации «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 массовая информация является предназначенной для неограниченного круга лиц в виде печатных, аудио-, аудиовизуальных и иных сообщений и материалов[2].

Однако существует информация, которая не подлежит распространению. Например, государственная тайна, то есть военные, внешнеполитические, экономические разведывательные, контрразведывательные и оперативные сведениязащищаемые государством, разглашение которых может нанести ущерб Российской Федерации[3], илиперсональные данные – прямо или косвенно относящиеся к конкретному физическому лицу сведения, распространение которых может причинить ущерб данному лицу[4]. Таким образом, персональные данные и государственная тайна относятся к видам закрытой информации.

У каждого человека имеется право на свободный поиск, получение, передачу, произведение и распространение информации любым законным способом, данное положение закрепляется частью 4, статьи 29 Конституции Российской Федерации. Необходимо заметить, что там, где есть право, есть и

---

[1] Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8-ФЗ // Собрание законодательства РФ. 2009. № 7. Ст. 776.

[2] Закон Российской Федерации «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 // Российская газета. 1992. 08 февраля.

[3] Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1 // Собрание законодательства РФ. 1997. № 41. Ст. 8220–8235.

[4] Федеральный закон «О персональных данных» от 27 июля 2007 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31. Ст. 3451.

ответственность. Например, Уголовный кодекс Российской Федерации (далее – УК РФ)закрепляет ряд санкций за нарушение получения и распространения информации: статья 137 «Нарушение неприкосновенности частной жизни», статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», статья 140 «Отказ в предоставлении гражданину информации», статья 146 «Нарушение авторских и смежных прав», статья 283 «Разглашение государственной тайны», Статья 307 «Заведомо ложные показание, заключение эксперта, специалиста или неправильный перевод», статья 308 «Отказ свидетеля или потерпевшего от дачи показаний», статья 310 «Разглашение данных предварительного расследования». Также защита информации встречается и в процессуальном праве, например, тайная предварительного следствия, предусмотренная статьей 161 Уголовно-процессуального кодекса Российской Федерации, которая устанавливает, что сведения, ставшие известными в ходе предварительного следствия, не подлежат распространению, за исключением случаев, если следователем или дознавателем разрешено такое распространение в конкретном информационном объеме. Помимо уголовной ответственности за незаконные получение и распространение информации предусмотрена и административная ответственность. Глава 13 Кодекса Российской Федерации об административных правонарушениях предусматривает ответственность за административные правонарушения в области связи и информации. Например, статья 13.12 «Нарушение правил защиты информации», статья 13.13 «Незаконная деятельность в области защиты информации», статья 13.14 «Разглашение информации с ограниченным доступом», статья 13.15 «Злоупотребление свободой массовой информации».

Таким образом, можно сделать вывод о том, информация не имеет какого-либо материального представления, она может быть отражена только на конкретном носителе, то есть для совершения действий с информацией необходим материально-определенный объект, который способен её хранить,

обрабатывать и, конечно, передавать. Соответственно, такими объектами являются информационные технологии.Понятие «информационные технологии» также как и понятие «информация», трактуется по-разному. Так, А.К. Айламазян[1] считает, что под информационными технологиями стоит понимать как совокупность методов и средств реализации информационных процессов в различных областях человеческой деятельности. Б.П. Саущкин[2] считает, что информационные технологии представляют собой движение технологической материи, то есть прогрессивная и управляемая человеком природно-социальная совокупность процессов целенаправленного изменения различных форм информации в системах техники. Такие ученые, как И.А. Мизин, И.Н. Синицын, Б.Г. Доступов[3] считают, что все-таки информационные технологии – это всего лишь совокупность различных средств, которые необходимы для выполнения информационных процессов. По мнению автора, для понимания сущности информационных технологий необходимо синтезировать вышеперечисленные мнения ученых и понимать как совокупность методов и средств, которые на основе технических процессов способны хранить, обрабатывать, передавать, изменять, получать, собирать информацию, работающие при помощимеханической силы человека. Законодатель также закрепил понятие «информационные технологии», согласно пункту 2, части 1, статьи 2 ФЗ «Об информации, информационных технологиях и о защите информации» информационные технологии –это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

---

[1]Айламазян А.К.Информатика и теория развития. М.: Наука, 1989. С. 15.

[2]Саушкин Б.П. Наукоёмкие технологии – основа технологического суверенитета страны. Липецк: ЛГТУ, 1997. С. 7.

[3]Мизин И.А. Развитие определений «информатика» и «информационные технологии» / И.А. Мизин, И.Н. Синицын, Б.Г. Доступов; под ред. И.А. Мизина. М.: ИПИ АН СССР, 1991. С. 12.

Человек как носитель информации может воспринимать её аналоговое представление, то есть воспринимать информацию исходя из своих физических возможностей (зрение, слух, обоняние, осязание и другое), и также переводить её в цифровое представление. Данное преобразование информации возможно с помощью современных информационных технологий, которые преобразуют информацию, полученную человеком с помощью его органов чувств, в цифровую информацию, то есть совокупность электрических сигналов[1]. К таким видам информационных технологий можно отнести, например, персональный компьютер, различные виды гаджетов (мобильные телефоны, планшетный компьютер, смарт-часы, компактные персональные компьютеры). Помимо самого гаджета и его операционной системыв состав входят следующие вспомогательные элементы: 1) отвечающие за ввод информации: клавиатура, мышь, считывающая головка оптического привода, слот для USB-средств, сканер, микрофон, видеокамера, сенсорный экран; 2) отвечающие за вывод информации: принтер, монитор (экран), акустические системы; 3) отвечающие за вычислительные процессы: процессор, материнская плата, графический процессор; 4) отвечающие за хранение информации: оперативно-запоминающее устройство, flash-память.

Помимо вышеперечисленного существуют системы, способствующие оперировать информацией. Например, информационно-телекоммуникационная сеть «Интернет» представляет собой всемирную систему многотысячных объединенных научных, корпоративных, правительственных и домашних компьютерных систем, способных хранить, обрабатывать и передавать информацию. Основной принцип возможности передачи, хранения и обработки информации различных систем заключается в маршрутизации пакетов данных с помощью протокола IP (сетевой протокол). Сетевой протокол выступает как «единый язык», используемый

[1]Умняшкин С.В. Основы теории цифровой обработки сигналов. М., 2016. С. 120.

всеми системами для успешного использования информации, или как порядок цифровой передачи информации между узлами информационно-телекоммуникационной сети.

Подводя итог необходимо отметить, что на сегодняшний день научное сообщество так и не может отнести информацию к какому-либо виду материи, однако информационные технологии с помощью механической силы человека могут предать информации материальный облик, то есть закрепить на каком-либо материальном носителе, который сможет её хранить, обрабатывать и передавать.

1.2 Нормативно-правовая база регулирования информации иинформационных технологий в правоохранительных органах

Впервые внимание законодателя к проблеме регулирования информацией и её распространением было обращено в период существования Российской Советской Федеративной Социалистической Республики. В 1991 году был разработан проект закона «Об ответственности за правонарушения при работе с информацией»[1], в котором устанавливались уголовная, административная, гражданско-правовая и дисциплинарная виды ответственности за нарушение правил работы с информацией, однако данный закон так и не был принят. Далее Указом Президента Российской Федерации от 28 июня 1993 г. № 966 была утверждена Концепция правовой информатизации России[2], которая заключалась в процессе создания оптимальных условий максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с

[1]Курушин В.Д. Компьютерные преступления и информационная безопасность. М.: Новый Юрист, 1998. С. 51.

[2] Указ Президента Российской Федерации «О Концепции правовой информатизации России» от 28 июня 1993 г. № 966 // Собрание актов Президента и Правительства Российской Федерации. 1993. № 27. Ст. 2521.

применением прогрессивных технологий. Главными задачами данной Концепции выступали: информационно-правовое обеспечение внутренней деятельности органов государства, информационно-правовое обеспечение внешних по отношению к государственным органам субъектов (в том числе физических лиц), сохранение и структурирование информационно-правового поля. Последующее развитие прогрессивных информационных технологий привело законодателя к разработке и принятию нормативно-правового акта, закрепляющего основные фундаментальные понятия в сфере информатизации и порядок обращения информации. Данным актом был Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ[1], который на данный момент утратил силу. Также можно утверждать, что данный федеральный закон является основой для действующего в настоящее время ФЗ «Об информации, информационных технологиях и о защите информации», который был усовершенствован путем внесения таких понятий как «информационные технологии», «информационно-телекоммуникационная система», «предоставление информации», «распространение информации», «электронное сообщение», «единая система идентификации и аутентификации» и другое.

Ретроспективный анализ законодательства в сфере информации и информационных технологий позволяет сделать вывод о том, что совместно с развитием самих технологий развивается и законодательство Российской Федерации в этой области. Тем не менее, закрепление норм и правил использования информации и информационных технологий наблюдается не только в общей теории права, но и в различных отраслях российского права.

Основополагающим нормативным документом всё жеявляется Конституция Российской Федерации, которая закрепляет ряд положений,

[1] Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ (утратил силу) // Собрании законодательства РФ. 1995. № 8. Ст. 609.

которые отражают информационные права. Так,предусмотрены права на неприкосновенность частной жизни, на личную и семейную тайну, на защиту своей чести и своего доброго имени (часть 1, статья 23); право обращаться лично, также направлять коллективные и индивидуальные обращения в государственные органы и органы местного самоуправления (статья 33); право на получение достоверной информации о состоянии окружающей среды (статья 42);право на ознакомление с документами и материалами, затрагивающими права и свободы гражданина, а органы государственной власти, органы местного самоуправления и их должностные лица имеют обязательство обеспечить возможность такого ознакомления (часть 2, статья 24); никто не вправе собирать, хранить, использовать и распространять информацию о частной жизни лица без его согласия (часть 1, статья 24), право на получение информации о фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей (часть 3, статья 41) и т.д.

В конце XX века российское законодательство уже имело широкую базу нормативных актов, регулирующих информационное право, были приняты больше 120 федеральных законов и около 105 законов регионального уровня. Например, Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1, Федеральный закон «О банках и банковской деятельности» от 02 декабря 1990 г. № 395-1[1], Закон Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 02 июля 1992 г. № 3185-1[2], Федеральный закон «О почтовой связи» от 17 июля 1999 г. № 176-ФЗ[3], Закон Российской Федерации «Осредствах массовой информации» от 27 декабря 1991 г. № 2124-1 и далее. Однако в начале XXI века законодательство, регулирующее

[1] Федеральный закон «О банках и банковской деятельности» от 02 декабря 1990 г. № 395-1 // Собрание законодательства РФ. 1996. № 6. Ст. 492.

[2] Закон Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 02 июля 1992 г. № 3185-1 // Ведомости СНД и ВС РФ. 1992. № 33. Ст. 1913.

[3] Федеральный закон «О почтовой связи» от 17 июля 1999 г. № 176-ФЗ // Собрание законодательства РФ. 1999. № 29. Ст. 3697.

общественные отношения, связанные со сбором и распространением информации, заметно расширилось и обновилось. Были приняты такие нормативно-правовые акты как Федеральный закон «О персональных данных» от 27 июля 2007 г. № 152-ФЗ, Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8-ФЗ, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, Федеральный закон «О коммерческой тайне» от29 июля 2004 г. № 98-ФЗ[1], Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10 июля 2002 г. № 86-ФЗ[2], Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31 мая 2002 г. № 63-ФЗ[3], Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ[4], Федеральный закон «О государственном банке данных о детях, оставшихся без попечения родителей» от 16 апреля 2001 г. № 44-ФЗ[5], Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20 августа 2004 г. № 119-ФЗ[6], Федеральный закон «Об электронной подписи» от 06 апреля 2011 № 63-ФЗ[7] и далее.

---

[1] Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ // Собрание законодательства РФ. 2004. № 32. Ст. 3283.

[2] Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10 июля 2002 г. № 86-ФЗ // Собрание законодательства РФ. 2002. № 28. Ст. 2790.

[3] Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31 мая 2002 г. № 63-ФЗ // Собрание законодательства РФ. 2002. № 23. Ст. 2102.

[4] Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ // Собрание законодательства РФ. 203. № 28. Ст. 2895.

[5] Федеральный закон «О государственном банке данных о детях, оставшихся без попечения родителей» от 16 апреля 2001 г. № 44-ФЗ // Собрание законодательства РФ. 2001. № 17. Ст. 1643.

[6] Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20 августа 2004 г. № 119-ФЗ // Собрание законодательства РФ. 2004. № 34. Ст. 3534.

[7] Федеральный закон «Об электронной подписи» от 06 апреля 2011 № 63-ФЗ // Собрание законодательства РФ.2011. №15. Ст. 2036.

Помимо вышеперечисленных законов, которые устанавливают требования по получению, передаче и хранению информации, в российском законодательстве существуют еще и кодифицированные нормативные акты, закрепляющие условия работы с информацией.

Статьей 102 Налогового кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ устанавливается налоговая тайна, которая состоит в недопущении распространения сведений о налогоплательщиках, плательщиках страховых взносов, полученных при осуществлении деятельности налоговых органов, органов внутренних дел, органов государственных внебюджетных фондов и таможенных органов. Статья 159 Семейного кодекса Российской Федерации от 29 декабря 1995 г. № 223-ФЗ обязывает судей, вынесших решение об усыновлении ребенка, или должностных лиц, осуществивших государственную регистрацию усыновления, а также лиц, осведомленных иным образом об усыновлении, хранить тайну по усыновлению ребенка.Также защита информации устанавливается частью 5.4, статьи 49 Градостроительного кодекса Российской Федерации от 29 декабря 2004 г. № 190-ФЗ, связанная с неразглашением органом исполнительной власти или экспертной организацией сведений о проектных решениях или иной конфиденциальной информации, которые стали известны в ходе проведения экспертизы. Ещё одним примером могут служить положения части 11 статьи 241 Бюджетного кодекса Российской Федерации от 31 июля 1998 г. № 145-ФЗ, которые устанавливают, что сведения о платежах и об их плательщиках являются информацией ограниченного доступа, что, соответственно, обязывает финансовые органы соблюдать требования по защите и использованию данной информации.

Защита информации и сведений, ставших известных при осуществлении государственной деятельности, устанавливается и процессуальными нормативно-правовыми актами. Согласно положениям статьи 161 Уголовно-процессуального кодекса Российской Федерации от 18

декабря 2001 г. № 174-ФЗ (далее– УПК РФ) сведения, ставшие известными в ходе предварительного следствия, не подлежат распространению, за исключением случаев, если следователем или дознавателем разрешено такое распространение в конкретном информационном объеме. Также данной нормой регламентирована ответственность по статье 310 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ (далее – УК РФ) «Разглашение данных предварительного расследования» лиц, которым стали известны данные предварительного следствия, за незаконное разглашение такие сведений без разрешения следователя или дознавателя.Также не допускается распространение сведений о частной жизни участников уголовного процесса, включая несовершеннолетних, без их согласия или согласия законных представителей. Еще одним примером защиты информации может послужить институт «тайны совещания судей». Все нормативно-правовые акт, закрепляющие нормы осуществления судопроизводства в Российской Федерации, устанавливают, что решения, выносимые судьями, должны приниматься в условиях абсолютной тайны в совещательных комнатах, что гарантируетреализацию конституционных требований о независимости судей при осуществлении правосудия. Нормативное закрепление данного института можно установить, исходя из содержания статьи 194 «Принятие решения суда» Гражданского процессуального кодекса Российской Федерации от 14 ноября 2002 г. № 138-ФЗ, статьи 20 «Порядок разрешения вопросов судом в коллегиальном составе. Особое мнение судьи» Арбитражного процессуального кодекса Российской Федерации от 24 июля 2002 г. № 95-ФЗ, статьи 175 «Принятие решения суда» Кодекса административного судопроизводства Российской Федерации от 08 марта 2015 г. № 21-ФЗ, статьи 298 «Тайна совещания судей» УПК РФ.

Особым видом защищаемой государством информации являются сведения о лицах, осуществляющих правоохранительную или иную

государственную деятельность, а также о лицах, сотрудничающих с правоохранительными органами.

Статья 2 Федерльного закона «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» от 20 апреля 1995 г. № 45-ФЗ[1] устанавливает круг лиц, подлежащих государственной защите. К ним относятся судьи судов общей юрисдикции, арбитражных судов, арбитражные заседатели, присяжные заседатели, прокуроры, следователи, дознаватели, лица, осуществляющие оперативно-розыскную деятельность, сотрудники федеральных органов внутренних дел, сотрудники учреждений и органов уголовно-исполнительной системы, военнослужащие,сотрудники органов федеральной службыбезопасности, сотрудники Следственного комитета Российской Федерации, сотрудники органов принудительного исполнения Российской Федерации, работники контрольных органов Президента Российской Федерации, сотрудники государственной охраны, сотрудники таможенных органов, работники налоговых органов, а также близкие родственники вышеперечисленных лиц. Согласно абзацу 2 статьи 9 данного нормативного акта сведения о данных лицах являются конфиденциальными и не подлежат распространению с момента поступления на службу или назначения на должность.

Защиту персональных данных сотрудников, осуществляющих правоохранительную деятельность, также предусмотрена нормативно-правовыми актами, регулирующими службу в правоохранительных органах. Информация о сотруднике, содержащаяся в личном деле или иных учетных документах, является служебной тайной и подлежит установлению конфиденциальности. В подтверждение данного высказыванияможно привести в пример следующие нормы: стать 39 «Персональные данные сотрудников органов внутренних дел, ведение их личных дел и документов

[1] Федерльный закон «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» от 20 апреля 1995 г. № 45-ФЗ // Собрание законодательства РФ. 1995. № 17. Ст. 1455.

учета сотрудников» Федерального закона «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30 ноября 2011 г. № 342-ФЗ[1], статья 39 «Персональные данные сотрудников, ведение кадрового учета сотрудников» Федерального закона «О службе в уголовно-исполнительной системе Российской Федерации и о внесении изменений в Закон Российской Федерации «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» от 19 июля 2018 г. № 197-ФЗ[2],статья 23 «Гарантии личной безопасности военнослужащих (сотрудников) войск национальной гвардии и членов их семей» Федерального закона «О войсках национальной гвардии Российской Федерации» от 03 июля 2016г. № 226-ФЗ[3], статья 39 «Персональные данные сотрудников федеральной противопожарной службы, ведение личных дел и документов учета сотрудников» Федерального закона «О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации» от 23 мая 2016 № 141-ФЗ[4], статья 7 «Защита сведений о федеральной службе безопасности» Федерального закона «О федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ[5].

---

[1] Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30 ноября 2011 г. № 342-ФЗ // Собрание законодательства РФ. 2011. № 49 (ч. 1). Ст. 7020.

[2] Федеральный закон «О службе в уголовно-исполнительной системе Российской Федерации и о внесении изменений в Закон Российской Федерации «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» от 19 июля 2018 г. № 197-ФЗ // Собрание законодательства РФ. 2018. № 30. Ст. 4532.

[3] Федеральный закон «О войсках национальной гвардии Российской Федерации» от 03 июля 2016 г. № 226-ФЗ // Собрание законодательства РФ. 2016. № 27 (ч. 1). Ст. 4159.

[4] Федеральный закон «О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации» от 23 мая 2016 № 141-ФЗ // Собрание законодательства РФ. 2016. № 22. Ст. 3089.

[5] Федеральный закон «О федеральной службе безопасности» от 03 апреля 1995 г.№ 40-ФЗ // Собрание законодательства РФ. 1995. № 15. Ст. 1269.

Помимо конфиденциальности сведений о сотрудниках правоохранительной системы законодательство Российской Федерации устанавливает защиту информации о лицах, содействующих правоохранительным органам. Согласно положениям пункта 34 части 1 статьи 13 «Права полиции» Федерального закона «О полиции» от 07 февраля 2011 г. № 3-ФЗ[1] и статьи 19 «Лица, содействующие органам федеральной службы безопасности» Федерального закона «О федеральной службе безопасности» сведения о лицах, содействующих правоохранительным органам на конфиденциальной основе, являются государственной тайной и охраняются законом, что, соответственно, запрещает распространение личных данных без особого согласия такого лица.

В рамках данного исследования также необходимо установить правовую основу применения информационных технологий, а также порядок использования информационных технологий правоохранительными органами.

Ранее весь комплекс информационно-технологических задач должен быть направлен на защиту интересов личности, законных интересов всех субъектов.В этой связи, развитие информационных технологий в нашей стране тесно связано с проводимой в стране административной реформой и появлением специализированных органов, государственной информационной политикой, информационной функцией государства, формированием единого информационного пространства и развитием государственных информационных систем, совершенствованием электронного правительства и электронного документооборота, расширением сферы предоставления государственных услуг в электронном виде.

Развитие информационных технологий особенно ярко проявилось с принятиемФедеральной целевой программы «Электронная Россия (2002–

[1] Федеральный закон «О полиции» от 07 февраля 2011 г. № 3-ФЗ // Собрание законодательства РФ. 2011. № 7. Ст. 900.

2010 годы)»[1]. Информация стала основой деятельности органов власти (управленческая информация). Государство, осознав преимущества информационных технологий, продолжилоразвитие и внедрение информационных технологий в государственную и общественную деятельность. Основными целями указанной программы являлись, во-первых, «повышение качества взаимоотношений государства и общества путем расширения возможности доступа граждан к информации о деятельности органов государственной власти, повышения оперативности предоставления государственных и муниципальных услуг, внедрения единых стандартов обслуживания населения», во вторых, «повышение эффективности межведомственного взаимодействия и внутренней организации деятельности органов государственной власти на основе организации межведомственного информационного обмена и обеспечения эффективного использования органами государственной власти информационных и телекоммуникационных технологий, повышения эффективности управления внедрением информационных и телекоммуникационных технологий в деятельность органов государственной власти», в-третьих, «повышение эффективности государственного управления, обеспечение оперативности и полноты контроля за деятельностью органов государственной власти». Федеральная целевая программа «Электронная Россия (2002-2010 годы)» вывела Российскую Федерацию на новый информационный уровень, с уверенностью можно утверждать об эффективности проводимой государством политики в сфере цифровизация. Так,по состоянию на декабрь 2010 года были введены в эксплуатацию в тестовом режиме такие информационные ресурсы, как федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)», единая система

[1] Постановление Правительства Российской Федерации от 28 января 2002 № 65 «О Федеральной целевой программе «Электронная Россия (2002–2010)» // Собрание законодательства РФ. 2002. № 5. Ст. 531.

межведомственного электронного взаимодействия, единая вертикально–интегрированная государственная автоматизированная система управления (ГАС «Управление») и так далее. Также в систему взаимодействия государственных органов посредством использования информационных технологий на базе защищенных каналов связи были включены около двадцати двух федеральных органов исполнительной власти, а общее количество сообщений, отправленных через информационную систему взаимодействия государственных органов, превышало значение в полтора миллиона сообщений[1].

Несмотря на высокую результативность программы,политика Российской Федерации до сих пор направлена на развитие и внедрение информационных технологий в государственную деятельность. Например, Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» от 09 мая 2017 № 203[2] (далее – Стратегия), действие которого направлено на развитие информационного общества Российской Федерации. Целью Стратегии выступает создание условийдля формирования в Российской Федерации общества знаний в целях развития информационного пространства. При этом приоритетными направлениями Стратегии выступают потребности граждан и общества в необходимости получения достоверной и качественной информации, оптимизация информационно-коммуникационной инфраструктуры Российской Федерации, развитие информационных технологий Российской Федерации, способных конкурировать на международной арене, формированиеновойтехнологическойосновыдляразвития экономики и

[1] Результаты проведения Федеральной целевой программы «Электронная Россия (2002-2010 годы)». Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/programs/6/#section-results (дата обращения 16.03.2020)

[2] Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» от 09 мая 2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

социальной сферы, а также внедрение цифровой экономики. Более значимый для правоохранительных органов является аспект оптимизации информационно-коммуникационной инфраструктуры Российской Федерации, так как в рамках данного направления обеспечивается свободный доступ, предоставленный гражданам, организациям, органам государственной власти и органам местного самоуправления в Российской Федерации, к достоверной информации. При этом в целях недопущения изменения, удаления, блокировки информации Стратегией предусмотрено развитие информационно-коммуникационной инфраструктуры только на уровнях программного обеспечения, информационных систем и сетей связи, предоставляемых российским сегментом информационно-телекоммуникационной сети «Интернет». В рамках данной Стратегии для развития устойчивой информационного поля в Российской Федерациии дальнейшего его функционирования, устанавливаются меры, направленные на обеспечение единого механизма государственного регулирования, мониторинга и управления информационной инфраструктурой Российской Федерации, поэтапное внедрение в деятельность государственных органов и органов местного самоуправления информационных технологий с использованием российских систем шифрования и криптографирования при электронном взаимодействии по средством использования сетей электросвязи Российской Федерации,а также проведение непрерывного мониторинга и анализа различного вида и рода угроз, возникающих при взаимодействии с помощью информационных технологий.

Развитие и использование информационных технологий в деятельности государственных органов, в том числе правоохранительных, имеет положительную тенденцию, влияющую на повышение эффективности работы сотрудников правоохранительных органов. Однако для невозможности допущения произвола и превышения должностных полномочий сотрудниками государством законодательно закреплены правила и порядок применения информационных технологий в

правоохранительной сфере. Безусловно, нельзя утверждать, что у всех правоохранительных органов единое направление использования информационных систем и технологий, различное применение обуславливается индивидуальностью решаемых задач тем или иным органом, а также их функций и полномочий.

Согласно положениям статьи 2 Федерального закона «О полиции» от 07 февраля 2011 г. № 3-ФЗ (далее – Федеральный закон «О полиции») основными направлениями деятельности полиции являются обеспечение защиты личности, общества и государства от противоправных посягательств; предупреждение, пресечение, выявление и раскрытие преступление, а также производство дознания по уголовным делам; предупреждение и пресечение административных правонарушений, а также производство по делам об административных правонарушениях, исполнение административных наказаний; осуществление розыска лиц; поддержание в общественных местах правопорядка; обеспечение безопасности дорожного движения; обеспечение защиты лиц, подлежащих государственной защите. Нормы статьи 11 данного федерального закона обязывают сотрудников полиции использовать в целях осуществления своей деятельности по указанным выше направлениямдостижения науки, техники исовременную информационную телекоммуникационную инфраструктуру (информационные системы и сети связи). При этом ФЗ «О полиции» предоставляет право принимать и регистрировать электронные документы, направлять электронные уведомления о результатах предоставления услуг, а также осуществлять взаимодействие с иными государственными (в том числе правоохранительными и муниципальными) органами в электронной форме. Полиция вправе использовать технические средства (видео-, аудио-, фототехнику)в целях фиксации и документирования обстоятельств совершения преступлений, административных правонарушений и происшествий, в том числе могут быть использованы автоматизированные информационные системы и интегрированные банки данных.

Другим правоохранительным органом, который вправе использовать информационные технологии в своей деятельности, является федеральная служба безопасности. При этом направления деятельности, как и цели использования информационных технологий, федеральной службы безопасности совершенно другие, относительно деятельности полиции.Согласно статье 20 Федерального закона «О федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ (далее – ФЗ «О федеральной службе безопасности») органы и подразделения федеральной службы безопасности вправе осуществлять разработку, создание и эксплуатирование информационных систем, систем связи и передачи данных, средств информационной защиты, включая криптографические защитные средства, без их лицензирования. Однако необходимо отметить, что данное право предоставлено только в случаях осуществления деятельности по направлениям, установленным в статье 8 ФЗ «О федеральной службе безопасности», в число которых входят, во-первых, осуществление контрразведывательной деятельности, во-вторых, проведение линии борьбы с терроризмом, в-третьих, проведение линии борьбы с преступностью, в-четвертых, разведывательная деятельность, в-пятых, осуществление пограничной деятельности, в-шестых, обеспечение информационной безопасности.Использование информационных технологий органами федеральной службой безопасности обуславливается и правами, пересиленными в статье 13 ФЗ «О федеральной службе безопасности», так как возможно осуществление шифровальных работ в целях контроля за соблюдением режима секретности при обращении с зашифрованной информацией (пункт «д»), осуществление мер в целях обеспечения собственной безопасности от преступного и незаконного проникновения к секретным сведениям с использованием технических средств (пункт «т»), осуществление регулирования в области разработки, производства, реализации и эксплуатации криптографических (шифровальных) средств и защищенных систем и комплексов телекоммуникации в Российской

Федерации (пункт «ш»), осуществление государственного контроля за криптографической и инженерно-технической безопасностью винформационно-телекоммуникационных системах, сетях связи специального назначения, иных сетях связи, за соблюдением режима секретности шифрованной информации, а также защита технических средств, размещенных на особо важных объектах (помещениях), от утечкиинформации по техническим каналам связи (пункт «щ»), участие в разработке, производстве, реализации, эксплуатации и обеспечении защиты технических средств, осуществляющих обработку, хранение и передачу информации ограниченного доступа (пункт «э»), обеспечение выявления средств (устройств) прихвата информации, составляющей государственную тайну (пункт «ю»).

Использование информационных технологий также можно наблюдать и в деятельности таможенных органов.Так, согласно статье 282 Федерального закона «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» от 03 августа 2018 г. № 289-ФЗ[1] между таможенными органами и заинтересованными лицами может осуществляться обмен электронными документами (сведениями) через информационного оператора, либо с использованием личного кабинета, либо с помощью других способов передачи документов и (или) сведений в электронной форме. При этом установлено, что документы и (или) сведения, предоставляемые в электронной форме, заверяются усиленной квалифицированной подписью заинтересованным лицом или уполномоченным должным лицом, после подписания электронные документы (сведения) приравниваются к документам, предоставленным на бумажном носителе с рукописными подписями указанных лиц.

[1] Федеральный закон «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» от 03 августа 2018 № 289-ФЗ // Собрание законодательства РФ. 2018. № 32. Ст. 5082.

Порядок и правила использования информационных технологий при осуществлении действий правоохранительных органов, направленных на выявление, пресечение, раскрытие, расследование и предупреждение преступлений и административных правонарушений, также закреплены в УПК РФ, Кодексе Российской Федерации об административных правонарушениях от 30 декабря 2011 г. № 195-ФЗ[1] (далее – КоАП РФ), Федеральном законе «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ[2] (далее – ФЗ «Об оперативно-розыскной деятельности»). Так, статья 164 УПК РФ предусматривает возможность применения технических средств при производстве следственных действий в целях обнаружения, фиксации и изъятия следов преступления и вещественных доказательств, при этом о применении технических средств следователем (дознавателем) предупреждаются лица, участвующие в проведении следственных действий. Статья 26.8 КоАП РФ предусматривает, что в целях фиксации административного правонарушения сотрудниками правоохранительных органов могут использоваться специальные технические средства, которые являются измерительными приборами, утвержденными в установленном порядке в качестве средств измерения, при этом которые имеют соответствующие сертификаты и прошли метрологическую проверку. Данные средства чаще всего применяются для фиксации административных правонарушений, предусмотренных главой 12 «Административные правонарушения в области дорожного движения» КоАП РФ. Также при осуществлении оперативно-розыскной деятельности могут быть использованы информационные системы, средства аудио-, фото-, кино- и видеофиксации, а также иные технические средства, которые не наносят ущерб жизни и здоровью людей и не причиняют вред окружающей среде. Статья 10 ФЗ «Об оперативно-розыскной деятельности» позволяет органам,

[1] Кодекс Российский Федерации об административных правонарушениях от 30 декабря 2001 г. №195-ФЗ // Собрание законодательства РФ. 2002. № 1. Ст. 1.

[2] Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

осуществляющим оперативно-розыскную деятельность, для решения поставленных задач осуществлять создание и использование различных информационных систем.

Таким образом, анализ законодательства Российской Федерации показал, что вопросы урегулирования порядка использования и применения информационных технологий в деятельности правоохранительных органов и, в целом, жизнедеятельности общества можно считать достаточно проработанными. Однако информационные технологии и способы передачи, хранения, обработки информации в настоящее время имеют тенденции к совершенствованию и быстротечному развитию. Поэтому изучение юридических проблем, возникающих при использовании информационных технологий в правоохранительной сфере, является актуальным направлением в правовой науке. Исследование правоприменительной практики и действующего законодательства в области информационных технологий позволят преодолеть проблемы и коллизии при осуществлении правоохранительной деятельности.

2 НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

2.1 Применение информационных технологий в административной деятельности правоохранительных органов

В развитии и применении информационных технологий значительную роль имеет административное право, исходя из того, что оно регламентирует организационные, технологические, межведомственные аспекты электронного документооборота для принятия своевременных решений в быстротечных технических процессах. Административное право, в какой-то мере, обеспечивает реализацию информационных функций государства, которые нуждаются в анализе и обсуждении как практическом, так и теоретическом, из-за своей новизны, оптимизации деятельности, минимизации расходов, заинтересованности субъектов, возможной конфликтности и противоречивости. Поэтому важнейшей функцией субъектов административного права является сбор, анализ и использование информации, внедрение и развитие современных информационных технологий в регулятивную и юрисдикционную сферы административно-правовой деятельности[1]

Несомненно, для успешной организации деятельности органов государственной власти и органов местного самоуправления необходимо обладать и распоряжаться актуальной, своевременной, точной и истинной информацией. Как было сказано ранее, государство посредством целевых программ намерено повсеместно внедрять информационные технологии для усиления цифровой информации, при этом необходимо отметить, что такое внедрение невозможно без административно-правового регулирования, потому что именно в этой сфере затрагиваются множественные публичные и

[1] Тихомиров Ю.А. Модернизация административного права: от «наказательности» к «регулирующему обеспечению» // Административное право и процесс. 2015. № 4. С. 5–11.

частные интересы субъектов права. Среди административно-правовых задач государства можно выделить: обеспечение общественного порядка и общественной безопасности; снижение затрат при проведении контрольных проверок и выполнении надзорных функций; совершенствование фискальной политики; развитие электронной торговли; доступ граждан к подготовке и обсуждению принимаемых государственных решений; охрана и защита охраняемой законом тайны в информационно-телекоммуникационных сетях и базах данных; поиск приемлемого компромисса между публичными и частными интересами.

Чем больше и стремительней будут внедряться в жизнь общества, тем больше возникнет необходимость в административном регулировании. Ведь проникая в технологический уклад государства, информационные технологии могут стать причиной нарушения инженерно-технической безопасности и привести к авариям и техногенным катастрофам. Таким образом, можно утверждать, что информационные технологии являются движущей силой развития российского и мирового сообщества. Соответственно, технологическое развитие требует развитие и нормативно-правовых актов, которые приводят к межведомственной правовой регламентации информационно-технологической деятельности, установлению правового статуса любого субъекта этой деятельности, а тем более управленческой и технологической. Таким образом, нормами административного права на современном этапе сформированы новые информационно-технологические правоотношения, определяющие электронно-цифровой характер правоприменительнойдеятельности.[1]

С развитием информационных технологий в административной деятельности возникли такие новые конструктивные понятия, как информационная база данных, обладатель информации, цифровая система управления, информационная безопасность, программное обеспечение,

[1] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 138.

электронный документ, оператор информационной сети и так далее. В общем-то, при возникновении административных отношений, связанных с использованием информационных технологий и цифровой информации, субъекты правоотношений (например, обладатель информации) имеют свои права и несут юридические обязанности, то есть для них устанавливается определенный правовой статус, необходимый для правоприменительной деятельности в условиях цифровизации.

Очевидно, что информатизация коснулась всех сфер деятельности, в том числе социальной, экономической, управленческой, правоохранительной, государственной, и, таким образом, можно утверждать, что административное право регулирует все виды отношений, возникающих в современном обществе, однако, нельзя отождествлять, что эти отношения имеют только публичный характер.Административное право, в первую очередь, направлено на достижение равновесия между публичными и личными интересами, а также обеспечение общественного порядка, путем непрерывного обмена информацией в целях соблюдения прав и законных интересов общества в условиях современной информационно-телекоммуникационной системе, например, получение информацию о деятельности государственных органов и органов местного самоуправления в электронном виде, получение государственной услуги через информационно-телекоммуникационную сеть «Интернет», подать заявление об административном правонарушении в форме электронного документа, так далее.

Нормативно-правовое регулирование административной деятельности, связанной с использованием информационных технологий, чаще всего выражается в различных положениях, инструкциях, регламентах,

руководствах[1]. Данные нормативные документы регулируют порядок накопления, хранения, использования, поиска и предоставления электронной информации о процессах, событиях и обращениях, в том числе связанных с административными правонарушениями. С уверенностью можно утверждать, что такая информация имеет несомненную важность при осуществлении правоохранительной деятельности. Зафиксированные в информационных системах сведения могут служить поводом для возбуждения дела об административном правонарушении, доказательством по административному делу в целях привлечения нарушителя к юридической ответственности.

Ярким примером использования информационных технологий для привлечения к административной ответственности являются средства фото- и видеофиксации административных правонарушений в области безопасности дорожного движения (далее – автоматизированные системы), которые используются государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации. Применение автоматизированных систем в области обеспечения безопасности дорожного движения впервые регламентировано Федеральным законом «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 24 июля 2007 г. № 210-ФЗ, из положений которого установлено, с 2007 года КоАП РФ дополнен статьей 2.6.1, регламентирующей, что собственники транспортных средств привлекаются к административной ответственности за правонарушения, предусмотренные главой 12 КоАП РФ, в случае если имеется фиксация административного правонарушения автоматизированными системами.

Цель использования данных информационных систем связана с сокращением гибели людей, участвующих в дорожном движении, в полтора раза данное заявление было сделано в 2011 году заместителем министра

[1] См., например, Постановление Правительства Российской Федерации «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия») от 08 сентября 2010 № 697 // Собрание законодательства РФ. 2010. № 38. Ст. 4823.

внутренних дел Российской Федерации по безопасности на транспорте, В.Н. Кирьяновым[1]. Согласно статистическим данным за 2015 календарный год в Российской Федерации произошло 184 000 дорожно-транспортных происшествий, при этом, в них пострадало 231 197 человек, а погибло – 23 114[2]. За 2019 календарный год было установлено 164 358 дорожно-транспортных происшествий, в результате чего пострадало 210 877 человек и погибло – 16 981[3]. Из статистики видно, что количество дорожно-транспортных происшествий за четыре года снизилось на 10,7 %, при этом смертность от дорожно-транспортных происшествий снизилась на 26,5 %. Исходя из этого, можно сделать вывод, что использование автоматизированных систем действительно способствует безопасности дорожного движения, дисциплинирует и организует всех участников дорожного движения.

Также необходимо обозначить, что использованиеавтоматизированных систем широко распространено в Российской Федерации, в общей сложности установлено около 16 000 комплексов фото- и видеофиксации нарушений правил дорожного движения, из них примерно 12 000 – стационарные, 4 000 – мобильные[4]. В частности, в Челябинской области количество автоматизированных систем, фиксирующих административные правонарушения в области дорожного движения, равно 112[5].

---

[1] История Госавтоинспекции. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://гибдд.рф/about/history (дата обращения 23.03.2020).

[2] Показатели состояния безопасности дорожного движения. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: http://stat.gibdd.ru/ (дата обращения 23.03.2020).

[3] Там же.

[4] Места размещения технических средств автоматической фото - и видеофиксации в Российской Федерации. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://гибдд.рф/milestones?all=true (дата обращения 23.03.2020).

[5] Места размещения технических средств автоматической фото - и видеофиксации в Челябинской области. Официальный сайт государственной инспекцией безопасности

Преимущественное число комплексов, установленных в Челябинской области, относятся к виду «DigitalPatrol», который представляет собой стационарный аппаратно-программный комплекс фиксации нарушений правил дорожного, с возможностью фиксации скорости автомобиля от 1 км/ч до 300 км/ч, при этом, погрешность такого комплекса не велика и составляет всего 2 км/ч[1].

Вся информация, полученная из автоматизированных систем, об административных правонарушениях также поступает в аппаратно-программный комплекс «Безопасный город» (далее – АПК «Безопасный город»), который является еще одним средством использования информационных технологий правоохранительными органами с целью обеспечения правопорядка и общественной безопасности.

Концепция построения и развития АКП «Безопасный город» утверждена Распоряжением Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р, согласно которой аппаратно-программный комплекс предназначен для устойчивого социально-экономического развития Российской Федерации путем осуществления единого системного подхода к обеспечению правопорядка и общественной безопасности в условиях разного рода рисков, в том числе техногенных и природных[2]. АПК «Безопасный город» обеспечивает сбор электронной доказательственной информации приобеспечении безопасности методом круглосуточной фиксации в автоматическом режиме событий административных правонарушений посредством видеонаблюдения с последующем направлением зафиксированной информации в системные автоматизированные системы. При этом видеофиксация административных правонарушений

дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://гибдд.рф/r/74/milestones (дата обращения 23.03.2020).

[1] Комплексы фиксации нарушений правил дорожного движенияDigitalPatrol [Электронный ресурс]. URL: http://digitalpatrol.ru/(дата обращения 23.03.2020).

[2] Распоряжение Правительства Российской Федерации «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» от 03 декабря 2014 г. № 2446-р // Собрание законодательства РФ. 2014. № 50. Ст. 7220.

обеспечивается географической локацией произошедшего инцидента с визуализацией на карте города с целью дальнейшей аналитической обработки участка местности на уровень криминализации. Актуальность и распространённость использования АПК «Безопасный город» можно проиллюстрировать на примере г. Челябинска[1]. Всего на территории города установлено 94 аппаратно-программных комплексов, снабженных средствами фото- и видеофиксации, при этом большинство из них установлены с целью фиксации совершения административных правонарушений в области дорожного движения. Однако 16 из указанных комплексов установлены в местах, где предположительно может быть большое скопление людей, например, Комсомольская площадь, пешеходный промежуток на улице Кирова, ПКиО «Сад Победы», ЦПКиО им. Ю.А. Гагарина, площадь Революции, а также на территориях торгово-развлекательных центов. Также стоит отметить, что информация, зафиксированная через АПК «Безопасный город» на территории г. Челябинска и Челябинской области автоматические поступает в информационные системы Главного управления МЧС России по Челябинской области; Управления ФСБ России по Челябинской области; Главного управления МВД России по Челябинской области; Управления ГИБДД ГУ МВД России по Челябинской области; Управления Федеральной Службы Войск Национальной Гвардии России по Челябинской области;Государственного учреждения «Поисково-спасательная служба

[1] Карта расположения средств фиксации преступлений и административных правонарушений в Челябинской области [Электронный ресурс]. URL:https://74.ru/text/auto/ (Дата обращения 25.03.2020).

Челябинской области», а также в иные государственные органы, ведомства и службы[1].

Необходимость в создании такого рода систем возникла исходя из возросших требований к системам, обеспечивающих безопасность. Однако, отсутствие на региональном и муниципальном уровнях комплексных многоуровневых информационных систем, обеспечивающих правопорядок и общественную безопасность, привело бы к нарушению жизнедеятельности общества и развитию криминальной среды. Стоит заметить, что такие технические средства, как АПК «Безопасный город», работают на основе современных походов, которые выражаются в виде мониторинга, прогнозирования, предупреждение преступлений, правонарушений, предупреждение происшествий и чрезвычайных ситуаций, а также своевременное реагирование на такие явления. Создание единого информационного пространства позволит эффективно и незамедлительно взаимодействовать всем силам и службам, обеспечивающим безопасность среды обитания. Однако развитие только информационных технологий не приведет к их эффективному использованию, также необходимо способствовать повышению уровня профессиональной подготовки сотрудников правоохранительных в области использования информационных систем. Совокупное совершенствование технического и профессионального аспектов использования информационных технологий позволит продуктивно и результативно осуществлять правоохранительную деятельность.

Использование информационных технологий, обеспечивающих сохранение сведений об административных правонарушениях, помимо

---

[1] Техническое задание на создание и внедрение опытного участка АПК «Безопасный город» на территории Челябинского городского округа и пилотных муниципальных образований Челябинской области. Официальный сайт Министерства информационных технологий и связи Челябинской области [Электронный ресурс]. URL:http://mininform74.ru/htmlpages/Show/activities/InformacionnoeobshhestvoAPKBezopasnyjgorod (Дата обращения 25.03.2020).

правоохранительной деятельности, замечено также и в судебной деятельности. Зафиксированная с помощью фото- и видеосредств информация может быть представлена в как доказательство при рассмотрении жалобы на постановление по делу об административном правонарушении. Так, согласно пункту 8 части 1 статьи 30.6 КоАП РФ на стадии рассмотрения жалобы на постановление об административном правонарушении проверятся законность и обоснованность вынесенного решения по делу об административном правонарушении на основании изучения всех материалов, имеющихся или дополнительных. К данным материал как раз могут относиться сведения о событии административного правонарушения, зафиксированные с помощью автоматизированных систем. Примером из практики может служить решение Металлургического районного суда г. Челябинска от 12 ноября 2018 г. № 12-368/2018[1] по жалобе гражданки К.А. Миролюбовой на постановление по делу об административном правонарушении, вынесенное старшим инспектором по ИАЗ ООПДАП ЦАФАПОДД ГИБДД ГУ МВД РФ по Челябинской области Н.С. Юрпалова. Согласно постановлению об административном правонарушении, вынесенному сотрудником ГИБДД ГУ МВД РФ по Челябинской области, К.А. Миролюбова совершила административное правонарушение, предусмотренное частью 2 статьи 12.9 КоАП РФ, передвигаясь на собственном автомобиле, превысила скоростной режим движения на 26 км/ч, что было зафиксировано АПК «Безопасный город», расположенным по адресу: г. Челябинск, ул. Свердловский проспект, д. 20. В судебной жалобе на постановление по делу об административном правонарушении гражданка К.А. Миролюбова ссылалась на то, что на фотоматериалах, предоставленных с АКП «Безопасный город», отсутствует четкая видимость государственного регистрационного номера автомобиля, и

[1] Решение Металлургического районного суда г. Челябинска от 12 ноября 2018 г. № 12-368/2018 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 25.03.2020).

требовала отмену постановления. На стадии изучения всех материалов дела об административном правонарушении судьей был проанализирован фотоматериал, предоставленный сАКП «Безопасный город», на предмет его качества и достоверности данных. После изучение снимка фотофиксации судья пришел к выводу, что государственный регистрационный знак автомобиля, принадлежащего К.А. Миролюбовой, был виден отчетливо и принял решения постановление старшего инспектора Н.С. Юрпалова оставить без изменений, а жалобу К.А. Миролюбовой – без удовлетворения. Проанализировав данный случай из судебной практики, можно прийти к выводу, что сведения с автоматизированных систем представляют интерес не только для правоохранительных органов, а также для органов судебной системы и граждан Российской Федерации, причем данные, зафиксированные на фото- или видеосредства, помогают визуализировать момент совершения административного правонарушения.

Внедрение и использование информационной технологии не могло пройти мимо такого направления административной деятельности как административно-юрисдикционная деятельность. Административно-юрисдикционная деятельность (административная юрисдикция) понимается в учебной и научной литературе, как совокупность властных правомочий уполномоченных государственных органов и их должностных лиц разрешать во внесудебном порядке споры в административно-правовой сфере и привлекать лиц к юридической ответственности. При этом данный вид деятельности может осуществляться через производство по административно-правовым жалобам.

Основанием для возбуждения производства по административно-правовой жалобе является сама жалоба, которая подается заявителем в органы государственной власти, органы местного самоуправлении, их должностным лицам (далее - адресат) с целью восстановить или защитить нарушенные права, свободы или законные интересы заявителя либо права, свободы или законные интересы других лиц.

Действующее законодательство устанавливает две формы обращения граждан, в том числе и жалоб – это письменная и устная формы. При этом письменное обращение может иметь форму электронного документа. Следует отметить, что впервые право граждан на письменные обращения в форме электронного документа было установлено законодателем в 2006 году Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации» от 02 мая 2006 г. № 59-ФЗ (далее – ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»).

По общему правилу жалобы, как вид обращения, поступившие адресату в форме электронного документа, подлежит рассмотрению в порядке, установленном ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». При этом статья 7 указанного нормативного правового акта устанавливает требования к структуре такой жалобы.

В то же время, помимо ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» другими федеральными конституционными законами, федеральными законами может быть установлен иной порядок рассмотрения жалобы и установлены иные требования к структуре и содержанию жалобы. Поскольку автор акцентирует внимание на производстве по административно-правовой жалобе, то приведем в качестве примера федеральные законы, которые закрепляют положения об осуществлении специальногопроизводства по административно-правовым жалобам. Так, порядок рассмотрения административно-правовых жалоб граждан в таможенные органы регламентируется Федеральным законом «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» от 3 августа 2018 г. № 289-ФЗ (далее – ФЗ «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»). Согласно части 5 статьи 300 ФЗ «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»

гражданин вправе направить жалобу в электронной форме в федеральные органы исполнительной власти, осуществляющие контроль и надзор в области таможенного дела. Порядок рассмотрения административно-правовых жалоб граждан в налоговые органы регламентируется Налоговым кодексом Российской Федерации (далее – НК РФ). Так, абзац второй, части 1, статьи 139.2 НК РФ регламентирует, что обжалование актов налоговых органов, а также действия или бездействия их должностях лиц может осуществляться путем подачи жалобы в электронной форме по телекоммуникационным каналам связи или через личный кабинет налогоплательщика.

Бесспорно, что электронная форма документа способствует более оперативной и эффективной работе с жалобами и другими обращениями граждан и организаций адресатом при обработке, передаче, получении, сборе необходимой информации.

Но, является ли письменная жалоба в форме электронного документа востребованной у заявителей? Для ответа на данный вопрос автором проведено анкетирование, в котором приняли участие 130 респондентов (Приложение 1).

По данным социологического опроса 26,9 % респондентов обращались с жалобой в государственные органы или органы местного самоуправления. 65,7 % респондентов обращались в государственные органы или органы местного самоуправления в письменной форме,34,3 % – в форме электронного документа. При этом 82,3% респондентов знают о том, что жалобу можно направить соответствующему адресату в электронной форме, а также 56,2 % респондентов отметили, что обратились бы с жалобой в электронной форме, если бы умели использовать электронные ресурсы (Приложение 2).

Результат анкетирования позволяет сделать вывод, что письменная форма жалоб в форме электронного документа не пользуется популярностью среди граждан, в том числе по причинениизкого уровня

информационной культуры населения. По мнению автора, игнорирование данной проблемы приводит, прежде всего, к недостаточно эффективной и мобильной реализации непосредственно самого права граждан на обращение, создает определенные трудности и в работе адресата, уполномоченного рассматривать данное обращение.

Для решения обозначенной проблемы и популяризации использования для реализации прав граждан, в том числе права на защиту письменной жалобы в форме электронного документа необходимо:

- доведения до граждан информации о возможных электронных ресурсах (как например Личный кабинет налогоплательщика, электронная приемная, электронная почта и пр.), которые возможно использовать для обращения, в том числе и с жалобами (СМИ, листовки, баннеры, СМС-сообщения и пр.);

- доступные для любого заявителя (в независимости от возврата, статуса, национальности и пр.) рекомендации по заполнению жалобы в форме электронного документа, в том числе, с демонстрацией необходимых примеров (образцов);

- организация и проведение обучающих семинаров для граждан, желающих повысить уровень своей информационной культуры, путем привлечения в данную работу волонтеров.

Подводя итоги исследования, проведенного в рамках данной части выпускной квалификационной работы, необходимо отметить, что использование информационных технологий в настоящее время стремительно развивается в административной деятельности правоохранительных органов. Существующая правовая статистика и снижение количества случаев совершения административных правонарушений, по сравнению с предыдущими годами, показывает, что применение различных информационных систем и комплексов в административной деятельности позволяет осуществлять мониторинг иконтроль со стороны силовых структур, а также немедленное реагирование

на явления, нарушающие общественную безопасность и правопорядок. Также информационные технологии в данном направлении деятельности результативны для других государственных органов, органов судебной системы, а также для граждан, так как позволяют сохранять доказательственную базу для разрешения административных споров и жалоб. При этом анкетирование среди граждан показал, что для успешного внедрения информационных технологий в российское общество необходимо повышать информационную культуру граждан. Также необходимо обратить внимание на профессиональные навыки сотрудников правоохранительных органов в работе с информационными системами и техническими средствами, которые тоже нуждаются в развитии и улучшении.

2.2 Использование информационных технологий в расследовании по уголовным делам в Российской Федерации и за рубежом.

Обуславливая актуальность развития и внедрения в общественную жизнь информационных технологий, необходимо отметить, что их использование также необходимо и для расследования преступлений. Так как на сегодняшний день отмечается тенденция совершения преступлений с помощью информационных технологий и использования преступниками различных цифровых платформ, что, соответственно, влияет на внедрение в деятельность правоохранительных органов технических средств и достижений науки в области информационных технологий с целью повышения эффективности расследования преступлений.

Согласно пункту 6 части 2 статьи 74 УПК РФ одним из видов доказательств могут быть иные документы, которые содержат сведения, зафиксированные как в письменном виде, так и в виде фото-, видеоматериалов, киносъемки, аудиозаписей, а также иные носители информации (часть 2 статьи 84 УПК РФ). Однако в нормах уголовно-процессуального права нет четкого понимания, что является информацией, а также не установлено, как необходимо определять допустимость

электронных доказательств, полученных с помощью информационных технологий, как вид доказательства по уголовному делу. Многие юристы считают, что электронные доказательства по своей юридической природе являются «уязвимыми» или «косвенными», так как подлинность таких доказательств чаще всего сложно установить. В пример можно привести преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, которые на данный момент чаще всего совершаются с использованием зашифрованных мобильных приложений, таких как «VIPole», «Telegram», «WhatsApp», «TelegramX» и тому подобное. Как правило, преступники, используя данные мобильные приложения, приискивают поставщика наркотических средств и психотропных веществ с целью их дальнейшего распространения. Соответственно, общение между преступником и поставщиком происходит в формате диалога, который может быть сохранен на мобильном устройстве до момента производства осмотра мобильного телефона следователем. В момент проведения следственного действия, направленного на установления всех необходимых обстоятельств уголовного дела, путем проведения осмотра мобильного телефона, в нем может быть обнаружен диалог с поставщиком, в котором установлены все обстоятельства совершения преступления, в том числе местонахождение наркотических средств или психотропных веществ, время создания, так называемой, «закладки» с наркотическим средством или психотропным веществом, координаты местонахождения «закладки», а в некоторых случаях и фотографии. Однако следователь при проведении данного следственного действия сталкивается с рядом процессуальных проблем, во-первых, если объем информации слишком большой, то на составление протокола будет затрачено значительное количество времени, во-вторых, для наглядности содержания протокола осмотра составляется фототаблица, которая также будет объемной, исходя из наличия цифровой информации, содержащейся на мобильном телефоне, и, в-третьих, установление подлинности информации. Конечно, факт участия преступника в данном диалоге может подтвердить

только он сам, однако, встает вопрос, как подтвердить подлинность данного доказательства, если имеет место конфликтная ситуация и преступник не признает использование данного мобильного устройства? Для преодоления последней названной проблемы следователям приходится использовать различные тактические приемы допроса обвиняемого, которые, в конечном итоге, помогают найти истину по уголовному делу. А также для экономии времени и сил следователей при проведении аналогичных осмотров, по мнению автора, необходимо создание цифровых приложений, позволяющих загружать из мобильных телефонов всю необходимую для уголовного дела информацию на персональный компьютер следователя путем создания электронного документа, который бы впоследствии приобщался к уголовному делу в виде доказательства и представлялся на носителе информации (USB-флеш-накопитель или компактный диск CD-RW).

Исходя из приведенного анализа, можно утверждать, что информация в виде электронных доказательств в настоящее время на практике применяется с осторожностью, по мнению автора, это, прежде всего, связано с отсутствием правового регулирования электронных доказательств, а именно нет четкого законодательного закрепления каким образом собирать, сохранять и предоставлять данные доказательства со всеми конкретными и надлежащими юридическими гарантиями, чтобы они могли быть допущены к суду, как обычный тип доказательств.

Однако УПК РФ в ряде случаев закрепляет порядок получения информации на электронных носителях. Согласно части 4.1 статьи 164 УПК РФ не допускается необоснованное изъятие электронных носителей информации при производстве следственных действий по уголовным делам о преступлениях, предусмотренных частями 1-4 статьи 159, статьями 159.1, 159.3, 159.5, 159.6, 160, 165 УК РФ, если эти преступления совершены в сфере предпринимательской деятельности, а также частями 5-7 статьи 159, статьями 171, 171.1, 171.3 - 172.2, 173.1 - 174.1, 176 - 178, 180, 181, 183, 185 - 185.4 и 190 - 199.4 УК РФ. При этом часть 1 статьи 164.1 УПК РФ

регламентирует, что изъятие электронных носителей информации возможно только в случаях вынесения постановления о назначении судебной экспертизы в отношении электронных носителей информации, наличие судебного решения на изъятие электронных носителей информации, содержание на электронных носителях той информации, на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение. При этом данное следственное действие должно производиться в присутствии специалиста, то есть лица, обладающего специальными знаниями, привлекаемого к участию в процессуальных действиях в порядке, установленном УПК РФ, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Протокол данного процессуального действия также содержит свои особенности. Так, согласно части 3 статьи 164.1 УПК РФ следователь в протоколе обязан указать технические средства, которые применялись для копирования информации, порядок применения, наименования и качества электронных носителей, к котором применялись данные средства, а также полученные результаты в ходе производства данного следственного действия, а также к протоколу должны прилагаться электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия. Участие специалиста в данном процессуальном действии подтверждает истинность, единство и верность полученной электронной информации, ведь в данном случае специалист выступает как незаинтересованное в ходе уголовного дела лицо, которое гарантирует объективность полученной информации.

Помимо вышеперечисленных примеров, УПК РФ закрепляет иные виды и способы использования информационных технологий. Согласно общим правилам, закреплённым в статье 164 УПК РФ, при производстве следственных действий могут быть использованы технические средства и способы обнаружения, фиксации и изъятия следов преступления, а также вещественных доказательств. Так, в пример можно привести несколько норм уголовного процесса, дозволяющие использование информационных технологий в досудебном производстве по уголовным делам. Согласно части 2, статьи 166 УПК РФ протокол следственного действия может быть изготовлен с помощью технических средств, а также в ходе следственного действия могут применяться фото-, киносъемка, видео-, аудиозапись, фотографирование, о применении которых уведомляются все участники следственного действия, о чем в протоколе делается отметка. При этом вся полученная с помощью технических средств информация хранится при уголовном деле. Также в ходе допроса по инициативе следователя или ходатайству допрашиваемого лица может производиться фото-, киносъемка, видео-, аудиозапись, фотографирование, о чем делается отметка в протоколе, при этом полученные материалы также хранятся при уголовном деле. Согласно статье 186 УПК РФ при расследовании уголовных дел о преступлениях средней тяжести, тяжких и особо тяжких допускается производство на основании судебного решения контроля и записи телефонных переговоров подозреваемого, обвиняемого и иных лиц, в случае если имеются достаточные основания полагать, что телефонные переговоры этих лиц могут содержать значимую информацию по уголовному делу. Следователь направляет постановление о производстве контроля и записи переговоров в соответствующий орган для дальнейшего исполнения, как правило, в оперативные подразделения. Материалы данного следственного действия предоставляются в качестве фонограммы с сопровождением печатного документа, дублирующего фонограмму (справка-меморандум, сводка телефонных переговоров), которые впоследствии осматриваются

следователем и приобщаются к уголовному делу как вещественные доказательства.

Использование информационных технологий, помимо досудебного производства по уголовному делу, можно наблюдать и на стадии возбуждения уголовного дела. Так, согласно пункту 1 части 1 статьи 140 УПК РФ одним из поводов для возбуждения уголовного дела является заявление о преступлении, а также в части 2 статьи 141 УПК РФ установлено, что заявление о преступлении может быть подано в правоохранительные органы в устной или письменной форме, в том числе электронной. Электронная форма обращений законодательно закреплена впервые в Федеральном законе от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»), при этом в статье 7 указанного нормативно-правового актаустанавливаются требования к структуре такого заявления. Обязательными требованиям для электронного обращения являются указание фамилии, имени и отчества заявителя, адрес электронной почты, по которому должны быть направлены ответ и уведомление о перенаправлении обращения, также в качестве права данная норма устанавливает возможность приложения заявителем всех необходимых документов и материалов, соответственно, в электронной форме.

Нормативно-правовым актом, четко регулирующим и закрепляющим порядок приёма и регистрации электронных заявлений граждан, является Приказ Министерства внутренних дел Российской Федерации «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных

правонарушениях, о происшествиях» от 29 августа 2014 г. № 736[1] (далее – Инструкция о порядке, приеме, регистрации и разрешения заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях). Согласно пункту 6 Инструкции о порядке, приеме, регистрации и разрешения заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях электронные заявления о преступлениях, об административных правонарушениях, о происшествиях принимаются посредством использования программного обеспечения на официальных сайтах МВД России, предусматривающего обязательное заполнения реквизитов, необходимых для работы с заявлениями о преступлениях и об административных правонарушениях. В данном случае обязательными реквизитами являются предусмотренные ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», а также само сообщение сведений, указывающих на признаки совершенного или готовящегося к совершению преступления, либо сведений о событиях, угрожающих личной или общественной безопасности. Для дальнейшей работы заявление, поданное в электронной форме, распечатывается и используется как письменное заявление согласно пункту 11 Инструкции о порядке, приеме, регистрации и разрешения заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях. Далее электронное заявление, преобразованное в письменное, регистрируется в Книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (далее – КУСП), после чегопроводится проверка сообщения о преступлении.Согласно пункту 50 Инструкции о порядке, приеме, регистрации и разрешения заявлений и сообщений о преступлениях, об административных правонарушениях, о

[1] Приказ Министерства внутренних дел Российской Федерации «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» от 29 августа 2014 г. № 736 // Российская газета. 2014. 14 ноября.

происшествиях по результатам рассмотрения заявления о преступлении может быть принято одно из следующих решений: о возбуждении уголовного дела, об отказе в возбуждении уголовного дела, о передаче по подследственности в соответствии со статьей 151 УПК РФ, а по уголовным делам частного обвинения о направлении в суд в соответствии с частью 2 статьи 20 УПК РФ.В течение 24 часов с момента принятия заявления о принятом решении сообщается заявителю в форме электронного документа посредством направления по электронной почте, при этом разъясняется право на обжалование принятого решения или действия, а также порядок обжалования. Анализируя данный нормативный акт также было отмечено, что при подаче письменного заявления о преступлении заявитель предупреждается об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 УК РФ, о чем делается отметка, заверяемая подписью заявителя, однако относительно электронного заявления о преступлении законодательне закрепляет такого предупреждения.

Помимо ведомственного приказа МВД России, существуют и другие ведомственные акты о порядке приема, регистрации и проверки сообщений о преступлениях. Например, Приказ Федеральной службы безопасности Российской Федерации «Об утверждении Инструкции по организации в органах федеральной службы безопасности приема, регистрации и проверки сообщений о преступлениях и иной информации о преступлениях и событиях, угрожающих личной и общественной безопасности» от 16 мая 2006 г. № 205[1] и Приказ Следственного комитета Российской Федерации «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» от 11 октября 2012 г. №

[1] Приказ Федеральной службы безопасности Российской Федерации «Об утверждении Инструкции по организации в органах федеральной службы безопасности приема, регистрации и проверки сообщений о преступлениях и иной информации о преступлениях и событиях, угрожающих личной и общественной безопасности» от 16 мая 2006 г. № 205 // Российская газета. 2006. 20 октября.

72[1]. Однако в данных нормативных актах не установлен порядок приема, регистрации и проверки сообщений о преступлениях, поступивших в электронной форме.

По мнению автора необходимо отметить, что ведомственные приказы по своей сущности являются регулирующими нормативными актами, а не устанавливающими. Устанавливающими актами являются федеральные конституционные и федеральные законы Российской Федерации, в том числе и кодифицированные. Таким образом, в данном научном исследовании обнаружен юридический пробел, который выражен в не закреплении в нормах уголовного процесса института электронного сообщения о преступлении. Важно отметить, что из приведенного выше анализа ведомственных актов, только МВД России разработан порядок приема, регистрации и проверки электронных сообщений о преступлениях, тем не менее, существуют и другие органы исполнительной власти, которые обязаны принимать, регистрировать и рассматривать сообщения о преступлениях. В связи с этим, автор считает необходимым закрепить в УПК РФ норму, отражающую институт электронного заявления о преступлении, которая будет являться устанавливающей для всех органов исполнительной власти, уполномоченных принимать, регистрировать и рассматривать сообщения о преступлениях.

В целях отражения актуальности закрепления в нормах УПК РФ института электронного сообщения о преступлении автором было проведено анкетирование среди гражданского населения, в котором приняли участие 92 респондентаразличных возрастных категорий (Приложение 3). По данным опроса только 44,6 % респондентов знают о возможности подачи заявления о преступлении в правоохранительные органы в электронной форме, 55,4 % – не знают о такой возможности. При этом 79,3 % опрошенных считают, что

[1] Приказ Следственного комитета Российской Федерации «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» от 11 октября 2012 г. № 72 // Российская газета. 2013. 25 февраля.

данный способподачи заявления о преступлении в электронной форме является удобны. Также 93,5 % респондентов заметили, что такой способ подачи заявления о преступлении является для них доступным и у них есть возможность выхода в информационно-телекоммуникационную сеть «Интернет» (Приложение 4).

Таким образом, можно сделать вывод о том, что электронная форма заявлений удобна и эффективна, экономит время, как гражданам, так и сотрудникам правоохранительных органов. Проведение анкетирования показало, что для граждан актуально электронное сообщение о преступлении, однако имеются ряд проблем, связанных с низким уровнем использования электронного сообщения о преступлении, во-первых, 37 % граждан указали, что одним из отрицательных свойств электронного заявления о преступлении является попадание личных данных в информационно-телекоммуникационную сеть «Интернет», что указывает на недоверие граждан к деятельности государства по защите персональных данных в сети «Интернет», во-вторых, 56,5 % заметили, что при подаче электронного заявления о преступлении отсутствует возможность подробно объяснить обстоятельства произошедшего, это объясняется тем, что для человека намного проще взаимодействовать с другим человеком, а не с цифровым средством, также это может быть связано с низкой информационной культурой населений, так как 14,1 % указали, что у них отсутствуют навыки работы с электронными устройствами с выходом в сеть «Интернет». По мнению автора, игнорирование данной проблемы приводит, прежде всего, к недостаточно эффективной и мобильной реализации непосредственно самого права граждан на заявление о преступлении, создает определенные трудности в работе адресата, понижает эффективность и оперативность деятельности сотрудников правоохранительных органов в части рассмотрения заявлений о преступлениях. Для указанных проблем автор предлагает следующие пути решения: разработка доступных рекомендаций по заполнению электронных форм для заявителей; проведение

обучающих семинаров по использованию информационных технологий среди населения; информирование граждан о возможности подачи заявления о преступлении с помощью информационных ресурсов.

В рамках данного исследования, по мнению автора, необходимо обозначить зарубежный опыт применения информационных технологий при расследовании преступлений. Тенденция внедрения информационных технологий в деятельность правоохранительных органов присуща всем странам мира. Поэтому в данном исследовании, помимо российского опыта применения информационных технологий в уголовном процессе, считаем необходимым отразить опыт ряда зарубежных стран. При анализе уголовно-процессуального законодательства зарубежных стран можно сделать вывод о том, что только ряд стран, таких как Федеративная Республика Германия, Республика Казахстан, Эстонская Республика, закрепили порядок применения информационных технологий в уголовном процессе, а, например, в Саудовской Аравии и Турции порядок регламентирован подзаконными нормативными актами.

Так, относительно недавно, в мае 2019 года, в Уголовно-процессуальный закон Латвийской Республики было внесено изменение, закрепившее институт электронных доказательств в виде сведений о фактах в форме информации, сохраненной или переданной устройствами или системами автоматизированной обработки данных[1]. Еще одним примером закрепления в законодательстве использование информационных технологий является Уголовно-процессуальный кодекс Федеративной Республики Германии[2] (далее – УПК ФРГ).

---

[1] Уголовно-процессуальный закон Латвийской Республики на русском языке [Электронный ресурс]. URL: http://www.pravo.lv/likumi/29_upz.html(Дата обращения: 12.03.2020).

[2] Официальный сайт Министерства юстиции и защиты предпринимателей Федеративной Республики Германии [Электронный ресурс]. URL: http://www.gesetze-im-internet.de/stpo/index.html (Дата обращения: 12.03.2020).

В УПК ФРГ четко закреплено, что возможно использование информационных технологий в отношении подозреваемого, в том числе, могут быть произведены фото-, видео-, киносъемка, а также могут быть использованы иные технические средства, предназначенные для наблюдения, например, средства ночного видения, сигнализации, датчики GPRS для отслеживания местоположения. При этом использование таких средств санкционирует суд, а в исключительных случаях не терпящих отлагательства – прокуратура, с последующим уведомлением суда. Также § 32 b — 32 f, § 496 УПК ФРГ закрепляют, что предварительное расследование возможно осуществлять в форме электронного уголовного дела, при этом приравнивают данную форму с бумажным вариантом уголовного дела, устанавливают порядок расследования уголовного дела в электронной форме, условия обработки и использования личных данных в электронном файле по уголовному делу, а также в § 32 b регламентировано, что все документы предоставленные в электронной форме должны быть подписаны квалифицированной электронной подписью всех ответственных лиц.

Статья 213 уголовно-процессуального кодекса Республики Польши[1] (далее – УПК Польши) закрепляет возможность установления личности преступника посредством использования номера PESEL (номер Универсальной электронной регистрации населения), а в случае, если у лица, совершившего преступление, отсутствует номер PESEL установить информацию, имеющую значение для уголовного дела, по номеру телефона или адрес электронной почты. С помощью данных средств устанавливаются анкетные данные преступника, документ, подтверждающий его личность, возраст обвиняемого, его семейное положение, образование, род занятий и

[1] Уголовно-процессуальный кодекс Республики Польши от 6 июня 1987 г. № OJ.2020.30 // Законодательный вестник Польши (выпуск от 09.01.2020) [Электронный ресурс]. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-16798685l (Дата обращения: 12.03.2020).

источники дохода, данные о его судимости и налоговый идентификационный номер (NIP), если таковой имеется.

Относительно приема заявлений о преступлениях в электронной форме в зарубежных странах также имеется свой опыт. Например, в Китайской Народной Республике (далее - КНР) в 2016 году разработана органами общественной безопасности КНР интернет-система по приему сообщений о преступлениях и правонарушениях, получившая наименование «cyberpolice». Данная электронная система принимает к регистрации информацию о распространении порнографических материалов, вовлечении в занятие проституцией, распространении компьютерных вирусов, мошеннических действиях в сети Интернет, организации азартных игр, продаже оружия, боеприпасов к нему, а также торговле документами, фальшивыми деньгами, человеческими органами, распространении запрещенной информации о религиозных культах. В тоже время разработчики сайта поощряют передачу любой информации о деятельности организации Исламское движения Восточного Туркестана и иной информации о вооруженно-террористических организациях, целью которой является создание фундаменталистского исламского государства[1].

Также при анализе зарубежного уголовно-процессуального законодательства установлена возможность электронного документооборота. В пример можно привести Соединенные Штаты Америки (далее – США). В судах федеративного и местного уровня установлена возможность подачи документов в суд всеми участниками уголовного процесса в форме электронных документов с использованием систем подготовки электронного документооборота уголовного дела для дальнейшего его рассмотрения в суде (CaseManagementandElectronicCaseFilessystem). Система электронного документооборота является комплексной системой, позволяющей судам

[1] Захарова В.К. Применение современных медиакоммуникационных технологий в деятельности органов общественной безопасности и народной прокуратуры КНР // Академическая мысль. 2018. № 2. С. 100–102.

регистрировать и рассматривать уголовные дела в электронном формате. Также данные системы во всех штатах США позволяют, предоставлять все необходимые для уголовного дела документы в электронном формате, а в некоторых случаях, когда судебный процесс осуществляется только в электронной форме, и обязывают участников представлять электронные документы. Например, если адвокат не имеет возможности подать документ в электронной форме и предоставляет его в суд на бумажном носителе, он обязан объяснить по какой причине не соблюден порядок подачи документов через электронные системы[1].

В таких странах как Польша и Румыния применяется извещение и вызовы с помощью цифровых технологий. Согласно § 2 статьи 131 УПК Польши установлено, что если в уголовном деле имеет место большое количество потерпевших и каждое индивидуальное уведомление об их правах может стать серьезным препятствием для ведения уголовного дела, то такие лица уведомляются с помощью средств массовой информации: пресса, радио или телевидение, а также через официальные сайты прокуратуры и суда в сети «Интернет».Также согласно части 5 статьи 257 Уголовно-процессуального кодекса Румынии вызов в орган предварительного следствия или в суд, помимо письменной повестки, может осуществляться по электронной почте или с помощью любой другой системы электронных сообщений (например, через социальные сети)[2].

В некоторых странах мира предусмотрено удаленное осуществление устного перевода. Так, в статье 43 Уголовно-процессуального кодекса Литовской Республики[3] установлено, что переводчик, как лицо, обладающее языковыми навыками, необходимыми для перевода, может участвовать в

---

[1] Пастухов П.С. Электронный документооборот в уголовном процессе США // Правопорядок: история, теория, практика. 2018. № 4. С. 81–87.

[2] Уголовно-процессуальный кодекс Румынии [Электронный ресурс]. URL: https://wolterskluwer.ro/codul-de-procedura-penala/ (Дата обращения: 13.03.2020).

[3] Уголовно-процессуальный кодекс Литовской Республики [Электронный ресурс]. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482 (Дата обращения: 13.03.2020).

уголовном процессе посредством использования аудио или видео средств, заисключением случаев, когда непосредственное участие переводчика необходимо для того, чтобы участник надлежащим образом реализовал свои права или понимал ход уголовного процесса, то есть, в случае участия сурдопереводчика, то естьлица, понимающего немые или глухие символы. Согласностатьи 69 Уголовно-процессуального кодекса Эстонской Республики[1] лицо, ведущее производство, может провести дистанционный допрос свидетеля, если непосредственный допрос свидетеля затруднен или повлечет за собой чрезмерные затраты, а также с учетом необходимости защиты свидетеля или потерпевшего. При этом под дистанционным допросом в данном акте понимается в двух значениях, во-первых, как допрос при помощи технического решения, в результате чего участники процесса непосредственно видят и слышат в прямой трансляции показания свидетеля, не находящегося в следственном органе, прокуратуре или суде, и могут задавать ему вопросы через лицо, ведущее производство, во-вторых, как допрос по телефону, в результате чего участники процесса непосредственно слышат показания свидетеля, не находящегося в следственном органе или суде, и могут задавать ему вопросы через лицо, ведущее производство.

Хотелось бы также отметить, что в зарубежных странах активно используется видео- или аудиопротоколирование. Согласно § статьи 147 УПК Польши ход следственных действий может быть записан с помощью устройств для записи изображений или звука, о котором лица, участвующие в действиях, должны быть уведомлены перед началом следственного действия и запуском устройства. А также согласно части 3 статьи 226А Уголовно-процессуального кодекса Греческой Республики[2] показания

[1] Уголовно-процессуальный кодекс Эстонской Республики [Электронный ресурс]. URL: https://v1.juristaitab.ee/sites/www.juristaitab.ee/files/elfinder/ru-seadused (Дата обращения: 13.03.2020).

[2] Уголовно-процессуальный кодекс Греческой Республики [Электронный ресурс]. URL: https://docplayer.ru/86989074-Ugolovno-processualnyy-kodeks-grecheskoy-respubliki.html (Дата обращения: 13.03.2020).

несовершеннолетнего составляются в письменной форме и регистрируютсятакженаэлектронномаудиовизуальномсредстве,когдаэто возможно.Электроннаядемонстрацияпоказанийнесовершеннолетнего заменяет его физическое присутствие на последующих стадиях процесса.

Подводя итог вышесказанному, необходимо отметить, что использование информационных технологий в процессе расследования и раскрытия преступлений в зарубежных странах имеет большее распространение, чем в Российской Федерации. Осуществляются такие способы использования информационных технологий как электронное уголовное дело, аудио- и видеопротоколирование следственных действий, передача уголовного дела в суд в электронном формате, прием и регистрации электронных заявлений о преступлениях. Однако нельзя утверждать, что Российская Федерация отстает по возможностям применения информационных технологий в уголовном процессе от передовых стран, многие способы применения технических средств существует и на сегодняшний день, а также допустимы перспективы развития применения цифровых технологий при расследовании преступлений в России.

2.3 Функционирование информационных технологий в оперативно-розыскной деятельности

Согласно содержанию статьи 2 Конституции Российской Федерации одной из главных обязанностей государства является защита прав и свобод человека и гражданина. Оперативно-розыскная деятельность, являясь формой борьбы с преступностью, позволяет реализовывать и исполнять данную обязанность в значительной мере. Статья 1 ФЗ «Об оперативно-розыскной деятельности» содержит понятие, исходя из которого, можно сделать вывод, что к отличительным признакам оперативно-розыскной деятельности относятся, во-первых, оперативно-розыскная деятельность является государственной деятельностью, во-вторых, сочетает в себе гласные и негласные методы, в-третьих, осуществляет социально-полезные и

значимые функции, в-четвертых, реализуется путем проведения оперативно-розыскных мероприятий. Иными словами, оперативно-розыскная деятельность – это ответ государства на вызов преступности в её изощренных проявлениях, при этом данный вид деятельности государства носит вынужденных характер, направленный на обеспечение безопасности личности, общества и государства. Оперативно-розыскная деятельность правоохранительных органов также отличается от иных видов деятельности основными направлениями, которые заключаются в предупреждении преступлений, выявлении, пресечении и раскрытии преступлений, розыске лиц, скрывающихся от органов предварительного следствия и дознания, суда, а также от исполнения наказания, розыске без вести пропавших лиц, производстве по делам оперативного учета, оперативном сопровождении производства по уголовным делам, обеспечении безопасности участников уголовного процесса, и близких лиц и родственников и так далее. При этом законодатель четко определил, какие органы вправе осуществлять оперативно-розыскную деятельность, к их числу относятся органы внутренних дел Российской Федерации, органы федеральной службы безопасности Российской Федерации, таможенные органы Российской Федерации, службы внешней разведки Российской Федерации, а в исключительных случаях и органы внешней разведки Министерства обороны Российской Федерации.

Для осуществления направлений оперативно-розыскной деятельности, в настоящей действительности, правоохранительные органы не могут не использовать информационные технологии, так как большинство преступных действий совершаются в условиях информационной среды, в том числе распространение наркотических средств и психотропных веществ, мошенничество в различных проявлениях, незаконное предоставление поддельных документов и тому подобное. Право использования оперативно-розыскными органами информационных технологий закреплено в положениях статьи 10 ФЗ «Об оперативно-розыскной деятельности»,

согласно которой создание и использование информационных систем возможно только в рамках осуществления задач оперативно-розыскной деятельности.

Также необходимо отметить, что следствием осуществления оперативно-розыскной деятельности является оперативная информация или результат оперативно-розыскной деятельности. В юридическом научном сообществе понятия «оперативная информация» и «результат оперативно-розыскной деятельности» принято считать синонимами, однако в исключительных случаях необходимо их разграничивать в зависимости от контекста. Так, А.Ю. Шумилов отметил, что оперативная информация – это информация, полученная в результате оперативно-розыскной деятельности[1]. Легального определения, чем же всё-таки является оперативная информация, нет. Поэтому в рамках данного исследования автор предлагает оперативную информацию понимать как возникшую в результате произошедших, готовящихся, совершаемых или совершенных преступных проявлений, документально закреплённую форму выражения внешних явлений и материальных объектов, которая была получена в результате оперативно-розыскной деятельности. Научное сообщество выделяет два вида оперативной информации: ориентирующая (применяется для следственного планирования по уголовным делам и разрешения тактических действий) и доказательственная (используется как доказательство при расследовании преступлений). Как уже было отмечено ранее, при осуществлении оперативно-розыскной деятельности органы вправе использовать информационные технологии и иные технические средства, в результате чего образуется оперативная информация, содержащаяся на электронных носителях, то есть электронная оперативно-розыскная информация, которая также может использоваться для решения сыскных задач и уголовного процесса.

---

[1] Новый оперативно-розыскной закон России: учебно-практическое пособие. 3-е изд., испр. и доп. / авт. сост. А.Ю. Шумилов. М., 1997. С. 34.

Оперативно-значимая информация, необходимая для успешного и эффективного раскрытия и расследования преступлений, может быть обнаружена сотрудниками правоохранительных органов при различных ситуациях, в том числе, при исследовании информационного пространства. Поэтому автор считает необходимым отразить точку зрения учёного-процессуалиста С.В. Зуева[1], который считает, что электронная оперативно-розыскная информация подразделяется на следующие виды:

1) первичная, которая может быть получена сотрудниками оперативных подразделений при изучении информационно-телекоммуникационной сети «Интернет», путем посещения различных сайтов, интернет-порталов, форумов, а также при исследовании страниц социальных сетей. При этом такая информация должна быть документально закреплена и тщательно проверена с помощью оперативно-розыскных методов. Например, при исследовании интернет-сервисов на соискание вакансий может быть обнаружена вакансия «закладчик», подразумевается лицо осуществляющее распространение наркотических средств и психотропных веществ, а далее путем проведения оперативно-розыскных мероприятий осуществляется раскрытие преступления. Также к данному виду электронной информации можно отнести сведения, поступившие в правоохранительные органы с использованием цифровых устройств от анонимных источников и агентурного аппарата;

2) информация как результат проведения оперативно-розыскных мероприятий, которая может быть получения в результате проведения оперативно-розыскных мероприятий с использованием технических средств (опрос, наведение справок, наблюдение, прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации). Особым условием для такого виды информации

[1] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 296.

является то, что она обязательно закреплена на материальном носителе информации.

На первый взгляд может показаться, что информация первого и второго вида идентичны друг другу, однако между ними есть отличительные черты, во-первых, этапы осуществления оперативно-розыскной деятельности, во-вторых,масштабность и сложность получения электронной оперативной информации. В любом случае электронная оперативная информация, как средство доказывания по уголовному делу, подлежит проверке оценке на соответствие требований, установленных законодательством Российской Федерации (статья 11 ФЗ «Об оперативно-розыскной деятельности»). В рамках уголовно-процессуальной деятельности электронная оперативная информация оценивается с точки зрения допустимости, относимости, достоверности и достаточности доказательства (статья 89 УПК РФ), при этом проверяется не только информация, но иеё материальный носитель в аспекте способа получения и закрепления.

Получение информации с применением технических средств при осуществлении оперативно-розыскной деятельности имеет свои особенности. Статей 6 ФЗ «Об оперативно-розыскной деятельности» определено, что проведение оперативно-розыскных мероприятий, связанных с получением той или иной электронной информацией, проводятся впорядке, установленном межведомственным нормативно-правовыми актами или соглашениями правоохранительными органами, с использованием исключительно техническими силами и средствами органов внутренних дел и органов федеральной службы безопасности. При этом если необходимость использования технических средств при проведении оперативно-розыскных мероприятий определено, то к участию привлекаются должностные лица, обладающие специальными знаниями и навыкамииспользования технических средств для получения оперативно-значимой информации. Категории и виды специальных технических средств, которые могут использоваться для получения электронной информации, определены в

закрытом Перечне видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, утвержденном постановлением Правительства Российской Федерации от 01 июля 1996 г. № 770[1]. В данный перечень входят всего 10 видов специальных технических средств, соответственно, по видам оперативно-розыскных мероприятий, некоторыми из которых являются средства, используемые в целях негласного получения и регистрации акустической информации, исследования предметов и документов, идентификации личности и так далее.

Необходимо отметить, что главенствующую роль в организации применения информационных технологий при осуществлении оперативно-розыскной деятельности возлагается на органы внутренних дел и органы федеральной службы безопасности. Так, согласно указу Президента Российской Федерации «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» от 01 сентября 1995 г. № 891развитие на объектах связиоперативно-технических средств осуществляется силами и средствами указанных выше правоохранительных органов при долевом финансовом обеспечении с другими органами[2]. Также при проведении оперативно-розыскных мероприятий, направленных на получение негласной информации, с использованием специальных технических средств правоохранительные органы, уполномоченные осуществлять оперативно-

[1]Постановление Правительства Российской Федерации «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных для негласного получения информации, и перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» от 01 июля 1996 г. № 770 // Собрание законодательства РФ. 1996. № 28. Ст. 3382.

[2] Указ Президента Российской Федерации «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» от 01 сентября 1995 г. № 891 // Собрание законодательства РФ. 1999. № 24. Ст. 2954.

розыскнуюдеятельностью, обязаны организовывать и тактически выстраивать оперативно-розыскные мероприятия на основании ведомственных нормативных актов, согласованных с Федеральной службой безопасности Российской Федерации (статья 4 ФЗ «Об оперативно-розыскной деятельности»).

Получение электронной оперативной информации чаще всего сопряжено с проведением оперативно-розыскных мероприятий, ограничивающих конституционные права граждан, поэтому условия проведения таких мероприятий необходимо отметить в рамках данного исследования.К таким видам оперативных мероприятий относятся, например,получение компьютерной информации, прослушивание телефонных переговоров, снятие информации с технических каналов связи. Согласно статье 8 ФЗ «Об оперативно-розыскной деятельности» важным условием проведения таких мероприятий является судебное решение на разрешение ограничения конституционных прав граждан исключительно при наличии информации о признаках преступления (на различных стадиях); о лицах, намеренных совершить, совершающих или совершивших преступление, по которому производство предварительного следствия обязательно;о событиях или действия, создающих угрозу безопасности Российской Федерации. Однако из этого правила есть исключение,в случаях нетерпящих отлагательства при возможном осуществлении противоправных действий, могущих привести к совершению тяжкого или особо тяжкого преступления либо угрожающих безопасности Российской Федерации,оперативно-розыскные мероприятия, ограничивающие конституционные права граждан, могут проводиться без судебного решения, с обязательным уведомлением суда в течение 24 часов. Проведение такого оперативно-розыскного мероприятия как «прослушивание телефонных переговоров» также законодательно ограничено и проводится только в отношении подозреваемых или обвиняемых, совершивших преступления средней тяжести, тяжких или особо тяжких преступлений.

Статья 6 ФЗ «Об оперативно-розыскной деятельности» закрепляет перечень оперативно-розыскных мероприятий, который является закрытым и может быть изменен или дополнен только на основании федерального законодательства. В рамках данного исследования считаем необходимым выделить несколько оперативно-розыскных мероприятий, которые даже исходя из наименования предполагают использование специальных технических средств для получения электронной оперативно-значимой информации. К их числу относятся, во-первых, прослушивание телефонных переговоров, во-вторых, снятие информации с технических каналов связи, в-третьих, получение компьютерной информации.

Прослушивание телефонных переговоров представляет собой оперативно-розыскное мероприятие, которое проводится и используется для фиксации с помощью технических средств разговоров физических лиц, осуществляемых по телефонным линиям связи. Проводится органами внутренних дел и органами федеральной службы безопасности как самостоятельно, так и с привлечением организаций, предоставляющих услуги связи. Может проводиться гласно или негласно. Гласное проведение оперативно-розыскного мероприятия проводится на основании постановления руководителя оперативного подразделения и по заявлению или согласию отдельных лиц, в случаях, если возникла угроза их жизни, здоровья или собственности.Негласный контроль может осуществлять путем подключения к стационарной аппаратуре предприятий (учреждений), предоставляющих услуги связи, а также путем сканирования радиосигнала. Результаты предоставляются в виде фонограммы, чаще всего на неперезаписываемых компактных дисках типа CD-RW, проверяются и приобщаются к уголовному делу в виде доказательства. При этом необходимо отметить, что записи телефонных переговоров сопровождаются справкой-меморандумом или сводкой контроля телефонных переговоров на бумажных носителях, которые дублируют звуковую информацию.

Снятие информации с технических каналов связи – оперативно-розыскное мероприятие, которое состоит в негласном контроле и фиксации электронной информации, передаваемой по техническим каналам связи, для решения оперативных задач. Само по себе мероприятие представляет собой сканирование технических каналов либо радиоперехват с целью копирования и сохранения информации на материальных носителях, в том числе и на электронных. Для проведения данного оперативно-розыскного мероприятия могут привлекаться сотрудники организаций (учреждений), предоставляющих услуги связи, сотрудники специализированных подразделений органов внутренних дел и органов федеральной службы безопасности, которые используют собственные специальные технические и аппаратные средства. Результаты оперативно-розыскного мероприятия в виде информации, сохраненной на материальном носителе, совместно с рапортом сотрудника, осуществляющего оперативно-розыскное мероприятие, приобщается к уголовному делу в виде доказательства.

Получение информации с технических каналов связи является одним из видов оперативно-розыскных мероприятий и осуществляется оперативными подразделениями с целью получения оперативно-значимой информации, передаваемой с помощью компьютерных систем. Информация может быть в виде следов противоправной деятельности, электронных сообщений, ссылок на сетевые адреса, сеансы прямой связи, а также в виде условных сигналов. Такого рода информация может быть обнаружена в двух формах: сохраненная на электронно-машинном носителе или переданная по каналу связи. Само по себе мероприятие представляет дистанционное или непосредственное исследование персонального компьютера, которое непосредственно сопровождается копированием, обнаруженных электронных файлов в целях дальнейшего изучения, а также заключается в обследовании содержимого сетевых информационных ресурсов. Дистанционное исследование, в рамках данного оперативно-розыскного мероприятия может быть связано с преодолением защитных средств и

сокрытия следов доступа. Результат в виде информации сохраняется на материальном носителе, в том числе электронном или магнитном, совместно с рапортом имеют как доказательственное, так и ориентирующее значение.

По мнению автора, несправедливым будет утверждение, что для проведения иных видов оперативно-розыскных мероприятий специальные технические средства являются бесполезными. Для подтверждения указанного мнения считаем необходимым привести несколько примеров из судебной практики.

Так, оперативными сотрудниками отдела по борьбе с организованной преступностью управления уголовного розыска ГУ МВД России по Челябинской области для подтверждения факта совершения преступления, предусмотренного пунктами «а», «в», «г» части 2 статьи 161 УК РФ, то есть грабеж (открытое хищение чужого имущества), совершенный группой лиц по предварительному сговору с применением насилия, не опасного для жизни или здоровья, либо с угрозой такого насилия, гражданами Лупенковым Д.А., ЗахаровымМ.А., Рыполевым М.Б. и Семыкиным А.В., которые являются жителями г. Троицка Челябинской области, было принято решение проведения оперативно-розыскного мероприятия «наблюдения» путем негласного получения информации с помощью специальных технических средств. После получения судебного решения, разрешающего ограничить конституционные права гражданин при осуществлении оперативно-розыскных мероприятий, установили в жилых помещениях гражданина Лупенкова Д.А. специальные технические средства, которые осуществляли негласную аудио- и видеозапись. Полученный результат содержал в себе видеозаписи, на которых гражданин Лупенков Д.А. рассказывает третьим лицам о том, что он, совместно с ЗахаровымМ.А., Рыполевым М.Б. и Семыкиным А.В., совершил открытое хищение чужого имущества и приглашал третьих присоединиться к нимдля совершения аналогичных преступлений. Результаты проведенного оперативно-розыскного

мероприятия были направлены в следственные органы и приобщены к уголовному делу в качестве доказательств по уголовному делу[1].

Другим примером может послужить решение оперативных сотрудниковуправления по контролю за оборотом наркотиков ГУ МВД по Челябинской области оп проведении оперативно-розыскного мероприятия «оперативный эксперимент» в целях изобличения в преступной деятельности, связанной со сбытом наркотических средств, неустановленных лиц, при содействии ранее задержанного гражданина Н., санкционированное заместителем начальника ГУ МВД по Челябинской области.Гражданин Н. был задержан сотрудниками полиции в момент извлеченияиз тайниковой закладки, расположенной в лесном массиве в Курчатовском районе г. Челябинска, наркотическое средство а-Пирролидиновалерофенон (а-PVP), массой 2000 граммов. В момент, когда он находился в помещении управления по контролю за оборотом наркотиков ГУ МВД по Челябинской области от лица, зарегистрированного под никнеймом «А.», через интернет-мессенджер поступили указания организовать пять тайниковых закладок с наркотическими средствами. Гражданин Н. дал согласие на использование ноутбука, принадлежащего ему на праве собственности, в рамках оперативно-розыскного мероприятия для осуществления интернет-переписки с лицом, сообщавшим места тайниковых закладок с наркотическими веществами (далее – «оператор»). В целях осуществления оперативно-розыскного мероприятия «оперативный эксперимент» сотрудниками были изготовлены пять муляжей наркотических средств определённого вида и массы, которые были размещены в местах скрытого хранения на территории Курчатовского района г. Челябинска. С помощью ноутбука, принадлежащего гражданину Н., сотрудники посредством интернет-перепискиот имени гражданина Н. сообщили «оператору» точное место положения

[1] Приговор Троицкого городского суда Челябинской области от 28 июля 2015 г. № 1-191/2015 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

наркотических средств, куда были помещены муляжи наркотических средств. Далее путем проведения оперативно-розыскного мероприятия «наблюдение» были установлены и задержаны лица, отыскавшие муляжи, изготовленные оперативными сотрудниками[1].

Использование информационных технологий также можно отметить при проведении оперативно-розыскного мероприятия «проверочная закупка». Так, свидетель К.М.В. (сведения о личности сохранены в тайне), являясь лицом, употребляющим наркотические средства, приобретал у Кузьмина А.М. наркотическое средство героин для личного употребления. 15 октября 2018 г. К.В.М. обратился вуправление по контролю за оборотом наркотиков ГУ МВД по Челябинской области и сообщил об отношениях с Кузьминым А.М., которые складывались у них при купли-продажи некротических средств. Сотрудники полиции предложили К.В.М. принять участие в оперативно-розыскном мероприятии «проверочная закупка», на что К.В.М. заявил добровольное согласие участвовать в роли покупателя наркотических средств у Кузьмина А.М. Оперативно-розыскное мероприятие «проверочная закупка» проводилось со специальными техническими средствами негласной аудиозаписи. К.В.М. в присутствии оперативных сотрудников позвонил по собственному мобильному устройству Кузьмину А.М. и договорился о личной встрече для приобретения наркотических средств на сумму 48 000 рублей. Сотрудниками полиции заблаговременно до проведения оперативно-розыскного мероприятия денежные купюры общей суммой 48 000 рублей, которые К.В.М. должен был передать Кузьмину А.М. за приобретение наркотического средства, были осмотрены и сняты светокопии. Результат оперативно-розыскного мероприятия «проверочная закупка» был предоставлен в виде компактного диска CD-R, на котором имелись аудиозаписи разговора между К.В.М. и Кузьминым А.М. в момент

[1] Приговор Курчатовского районного суда г. Челябинска от 10 июля 2019 г. № 1-10/2019 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

приобретения наркотического средства в рамках данного мероприятия, и приобщен к материалам уголовного дела в качестве доказательства, подтверждающего виновность совершения Кузьминым А.М. преступления, предусмотренного пунктом «г» части 4 статьи 228.1 УК РФ[1].

Следует заметить, что использование оперативной информации (в том числе электронной) для доказывания по уголовным делам не всегда приветствуется в практике, что подтверждается в нормативных актах высших судебных инстанций Российской Федерации, которые содержат в себе своего рода противоречия.

Так, согласно абзацу 3 части 14 постановлению Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» информация, которая стала результатом оперативно-розыскных мероприятий, «связанных с ограничением конституционного права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также с проникновением в жилище против воли проживающих в нем лиц (кроме случаев, установленных федеральным законом)», может быть иметь доказательственное значение по уголовным делам только в случаях, когда оперативно-розыскные мероприятия проведены по разрешению суда и проверены органами предварительного следствия на соответствие уголовно-процессуальному законодательству.[2]

Иная точка зрения отражена в определении Конституционного Суда Российской Федерации от 14 февраля 1999 г. № 18-О, согласно которой информация, которая стала результатом оперативно-розыскных

---

[1] Приговор Советского районного суда г. Челябинска от 25 июня 2019 г. № 1-161/2019 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

[2] Постановлению Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // Бюллетень Верховного Суда Российской Федерации. 1996. № 2. С. 1.

мероприятий, может восприниматься как сведения об источниках фактов, могущие стать доказательством по уголовному делу только при условии их законного полученияв соответствии с ФЗ «Об оперативно-розыскной деятельности» и надлежащего процессуального закрепления в соответствии с уголовно-процессуальным законодательством[1].

По мнению С.В. Зуева данное противоречие связано со следующими причинами, во-первых, отрицательная оперативно-следственная практика, которая возникла во времена сталинских репрессий, когда оперативная информация не отличалась высоким уровнем достоверности, во-вторых, низкая степень профессионализма правоприменителядля разграничения электронной оперативно-розыскной информации по значению, в-третьих, отсутствие четких законодательно закреплённых требований относительно оперативной информации[2].

Подводя итог исследования, проведенного в рамках данного параграфа, необходимо отметить, что информационные технологии в оперативно-розыскной деятельности правоохранительных органов играют ключевую роль. Для конкретных видов оперативно-розыскных мероприятий, таких как прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации, использование информационных технологий и специальных технических средств необходимо, так как без их применения невозможно осуществления целей и задач оперативно-розыскной деятельности. Однако для других оставшихся видов оперативно-розыскных мероприятий информационные технологии и их использование носят вспомогательный характер, с их помощью осуществление оперативно-розыскной деятельности можно считать более

---

[1] Определение Конституционного Суда Российской Федерации «По жалобе граждан М.Б.Никольской и М.И.Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона «Об оперативно-розыскной деятельности» от 14 февраля 1999 г. № 18-О // Вестник Конституционного Суда РФ. 1999. № 3.

[2] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 306.

эффективным, продуктивным и результативным. Также электронная информация на материальном носителе, которая получена вследствие использования информационных технологий, может быть использована как хорошая доказательственная база при расследовании уголовного дела. Помимо указанного, результат оперативно-розыскных мероприятий в виде материально закрепленной электронной информации может служить хорошей гарантией для сотрудников оперативных подразделений, с точки зрения того, что весь порядок проведения оперативно-розыскных мероприятий материально закреплён и может быть использован для подтверждения законности и правильности проведения оперативных мероприятий.

ЗАКЛЮЧЕНИЕ

Информационные технологии, как показало исследование в рамках данной выпускной квалификационной работы, имеют широкое применение во всех сферах и областях деятельности общества, в том числе в деятельности правоохранительных органов. В рамках исследования на тему: «Информационные технологии в деятельности правоохранительных органов» были проанализированы и определены такие понятия как «информация», «информационные технологии», исследовано настоящее законодательство, регулирующее использование информационных технологий, исследован имеющийся практический опыт применения информационных технологий, изучены основания и условия применения информационных технологий в различных направлениях правоохранительной деятельности, а также был проанализирован зарубежный опыт применения информационных технологий при раскрытии и расследовании преступлений.

Анализ законодательства Российской Федерации показал, что вопросы урегулирования порядка использования и применения информационных технологий в деятельности правоохранительных органов и, в целом, жизнедеятельности общества можно считать достаточно проработанными. Однако информационные технологии и способы передачи, хранения, обработки информации в настоящее время имеют тенденции к совершенствованию и быстротечному развитию. Поэтому изучение юридических проблем, возникающих при использовании информационных технологий в правоохранительной сфере, является актуальным направлением в правовой науке. Исследование правоприменительной практики и действующего законодательства в области информационных технологий позволят преодолеть проблемы и коллизии при осуществлении правоохранительной деятельности.

Также необходимо отметить, что в развитии и применении информационных технологий значительную роль имеет административное

право, исходя из того, что оно регламентирует организационные, технологические, межведомственные аспекты электронного документооборота для принятия своевременных решений в быстротечных технических процессах. Административное право, в какой-то мере, обеспечивает реализацию информационных функций государства, которые нуждаются в анализе и обсуждении как практическом, так и теоретическом, из-за своей новизны, оптимизации деятельности, минимизации расходов, заинтересованности субъектов, возможной конфликтности и противоречивости. Существующая правовая статистика и снижение количества случаев совершения административных правонарушений, по сравнению с предыдущими годами, показывает, что применение различных информационных систем и комплексов в административной деятельности позволяет осуществлять мониторинг иконтроль со стороны силовых структур, а также немедленное реагирование на явления, нарушающие общественную безопасность и правопорядок. Также информационные технологии в данном направлении деятельности результативны для других государственных органов, органов судебной системы, а также для граждан, так как позволяют сохранять доказательственную базу для разрешения административных споров и жалоб. При этом анкетирование среди граждан показал, что для успешного внедрения информационных технологий в российское общество необходимо повышать информационную культуру граждан путем проведения государством обучающих семинаров по использованию информационных технологий среди населения. Также необходимо обратить внимание на профессиональные навыки сотрудников правоохранительных органов в работе с информационными системами и техническими средствами, которые тоже нуждаются в развитии и улучшении.

Помимо изучения использования информационных технологий в административной деятельности правоохранительных органов был проведен анализ применения информационных технологий в досудебном

производстве. Результат проведенного научного исследования в области применения информационных технологий в расследовании по уголовным делам позволяет сделать следующие выводы:

- во-первых, проанализировав настоящее законодательство, авторы пришли к мнению, что применение информационных технологий в расследовании по уголовным делам с целью получения электронных доказательств в настоящий момент является недостаточной проработанной областью в уголовном процессе.Использование цифровых информации при расследовании преступлений на сегодняшний день имеет противоречивое значение и не пользуются большой актуальностью среди сотрудников правоохранительных органов. Однако опыт зарубежных стран использования информационных технологий при расследовании и раскрытии уголовных дел показал, что использование цифровых средств удобно и эффективно как для сотрудников, так и для всех участников уголовного процесса. Поэтому можно сделать вывод о том, что цифровые средства при расследовании преступлений в Российской Федерации имеют все шансы найти свое практическое применение и наиболее точное законодательное закрепление;

- во-вторых, проведенное в рамках данного научного исследования анкетирование показало, что граждане Российской Федерации не в полной мере осведомлены о возможности подачи электронного сообщения о преступлении с помощью информационно-телекоммуникационной сети «Интернет», большинство опрошенных граждан указали, что не знают о таком способе заявления. Для решения возникшей проблемы государственным органам необходимо осуществлять более качественное информирование граждан о возможности подачи заявления о преступлении с помощью информационных ресурсов, например, через официальные интернет-сайты органов государственной власти, средства массовой информации, электронную почту, СМС-оповещения и тому подобное;

- в-третьих, анкетирование показало, что граждане не доверяют государственной защите персональных данных. Респонденты отметили, что

для них электронная форма заявлений о преступлениях не является актуальной в связи с тем, что необходимо заполнять реквизиты, связанные с личными данными. В связи с этим мы предлагаем развивать доверие граждан в области государственной защиты персональных данных, путем распространения информации об имеющихся гарантиях защищенности персональных данных граждан;

- в-четвертых, анализ ведомственных нормативных актов правоохранительных органов, уполномоченных принимать, регистрировать и рассматривать заявления о преступлениях показал, что устанавливающая норма, в которой закреплен порядок приема, регистрации и рассмотрения заявлений о преступлениях в электронной форме, отсутствует в действующем законодательстве. Отсутствие устанавливающей нормы, но наличие регулирующей, по нашему мнению, является существенным пробелом в уголовном процессе.

На основании проведенного исследования отмечаем необходимость совершенствования уголовно-процессуального законодательства в области применения информационных технологий в расследовании по уголовным делам, считаем важным рекомендовать проект Федерального закона (Приложение 5). Проектом Федерального закона предлагаем внести изменение в часть вторую УПК РФ «Досудебное производство», а именно главу 19 «Поводы и основание для возбуждения уголовного дела» раздела VII «Возбуждение уголовного дела» дополнить статьей 141.1 «Электронное заявление о преступлении».

Говоря об уголовном направлении деятельности правоохранительных органов нельзя было игнорировать и оперативно-розыскную деятельность, так как они, несомненно, связаны между собой. И исследование в этой области показало,что информационные технологии в оперативно-розыскной деятельности играют ключевую роль. Для конкретных видов оперативно-розыскных мероприятий, таких как прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной

информации, использование информационных технологий и специальных технических средств необходимо, так как без их применения невозможно осуществления целей и задач оперативно-розыскной деятельности. Однако для других оставшихся видов оперативно-розыскных мероприятий информационные технологии и их использование носят вспомогательный характер, с их помощью осуществление оперативно-розыскной деятельности можно считать более эффективным, продуктивным и результативным. Также электронная информация на материальном носителе, которая получена вследствие использования информационных технологий, может быть использована как хорошая доказательственная база при расследовании уголовного дела. Помимо указанного, результаты оперативно-розыскных мероприятий, в виде материально закрепленной электронной информации, могут служить хорошей гарантией для сотрудников оперативных подразделений, с точки зрения того, что весь порядок проведения оперативно-розыскных мероприятий материально закреплён и может быть использован для подтверждения законности и правильности проведения оперативных мероприятий.

Подводя итог вышесказанному, информационные технологии в правоохранительной деятельности можно считать как совокупность методов и средств, которые на основе технических процессов способны хранить, обрабатывать, передавать, изменять, получать, собирать информацию, необходимую для осуществления правоохранительной деятельности. Использование информационных технологий имеют позитивный характер, так как посредством их применения у сотрудников правоохранительных органов имеется возможность более оперативно реагировать на антиобщественные проявления. При этом информационные технологии повышают эффективность правоохранительной деятельности путем сбора, хранения и передачи информации, необходимой для решения задач, связанных с охраной законных интересов и прав личности, общества и государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ IНОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1 Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

2 Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

3 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства РФ. 2001. № 52. Ст. 4921.

4 Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. 2002. № 1. Ст. 1.

5 Федеральный закон «О банках и банковской деятельности» от 02 декабря 1990 г. № 395-1 // Собрание законодательства РФ. 1996. № 6. Ст. 492.

6 Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ (утратил силу) // Собрании законодательства РФ. 1995. № 8. Ст. 609.

7 Федеральный закон «О федеральной службе безопасности» от 03 апреля 1995 г.№ 40-ФЗ // Собрание законодательства РФ. 1995. № 15. Ст. 1269.

8 Федерльный закон «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» от 20 апреля 1995 г. № 45-ФЗ // Собрание законодательства РФ. 1995. № 17. Ст. 1455.

9 Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

10 Федеральный закон «О почтовой связи» от 17 июля 1999 г. № 176-ФЗ // Собрание законодательства РФ. 1999. № 29. Ст. 3697.

11 Федеральный закон «О государственном банке данных о детях, оставшихся без попечения родителей» от 16 апреля 2001 г. № 44-ФЗ // Собрание законодательства РФ. 2001. № 17. Ст. 1643.

12 Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31 мая 2002 г. № 63-ФЗ // Собрание законодательства РФ. 2002. № 23. Ст. 2102.

13 Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10 июля 2002 г. № 86-ФЗ // Собрание законодательства РФ. 2002. № 28. Ст. 2790.

14 Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ // Собрание законодательства РФ. 203. № 28. Ст. 2895.

15 Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ // Собрание законодательства РФ. 2004. № 32. Ст. 3283.

16 Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20 августа 2004 г. № 119-ФЗ // Собрание законодательства РФ. 2004. № 34. Ст. 3534.

17 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

18 Федеральный закон «О персональных данных» от 27 июля 2007 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31. Ст. 3451.

19 Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного

самоуправления» от 9 февраля 2009 г. № 8-ФЗ // Собрание законодательства РФ. 2009. 7. № 776.

20 Федеральный закон «О полиции» от 07 февраля 2011 г. № 3-ФЗ // Собрание законодательства РФ. 2011. № 7. Ст. 900

21 Федеральный закон «Об электронной подписи» от 06 апреля 2011 № 63-ФЗ // Собрание законодательства РФ.2011. №15. Ст. 2036.

22 Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30 ноября 2011 г. № 342-ФЗ // Собрание законодательства РФ. 2011. № 49 (ч. 1). Ст. 7020.

23 Федеральный закон «О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации» от 23 мая 2016 № 141-ФЗ // Собрание законодательства РФ. 2016. № 22. Ст. 3089.

24 Федеральный закон «О войсках национальной гвардии Российской Федерации» от 03 июля 2016 г. № 226-ФЗ // Собрание законодательства РФ. 2016. № 27 (ч. 1). Ст. 4159.

25 Федеральный закон «О службе в уголовно-исполнительной системе Российской Федерации и о внесении изменений в Закон Российской Федерации «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» от 19 июля 2018 г. № 197-ФЗ // Собрание законодательства РФ. 2018. № 30. Ст. 4532.

26 Федеральный закон «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» от 03 августа 2018 № 289-ФЗ // Собрание законодательства РФ. 2018. № 32. Ст. 5082.

27 Закон Российской Федерации «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 // Российская газета. 1992. 08 февраля.

28 Закон Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 02 июля 1992 г. № 3185-1 // Ведомости СНД и ВС РФ. 1992. № 33. Ст. 1913.

29 Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1 // Собрание законодательства РФ. 1997. № 41. Ст. 8220–8235.

30 Указ Президента Российской Федерации «О Концепции правовой информатизации России» от 28 июня 1993 г. № 966 // Собрание актов Президента и Правительства Российской Федерации. 1993. № 27. Ст. 2521.

31 Указ Президента Российской Федерации «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» от 01 сентября 1995 г. № 891 // Собрание законодательства РФ. 1999. № 24. Ст. 2954.

32 Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» от 09 мая 2017 № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

33 Постановление Правительства Российской Федерации «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных для негласного получения информации, и перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» от 01 июля 1996 г. № 770 // Собрание законодательства РФ. 1996. № 28. Ст. 3382.

34 Постановление Правительства Российской Федерации от 28 января 2002 № 65 «О Федеральной целевой программе«Электронная Россия (2002–2010)» // Собрание законодательства РФ. 2002. № 5. Ст. 531.

35 Распоряжение Правительства Российской Федерации «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» от 03 декабря 2014 г. № 2446-р // Собрание законодательства РФ. 2014. № 50. Ст. 7220.

36 Приказ Федеральной службы безопасности Российской Федерации «Об утверждении Инструкции по организации в органах федеральной службы безопасности приема, регистрации и проверки сообщений о преступлениях и иной информации о преступлениях и событиях, угрожающих личной и общественной безопасности» от 16 мая 2006 г. № 205 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 42.

37 Приказ Следственного комитета Российской Федерации «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» от 11 октября 2012 г. № 72 // Российская газета. 2013. 25 февраля.

38 Приказ Министерства внутренних дел Российской Федерации «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» от 29 августа 2014 г. № 736 // Российская газета. 2014. 14 ноября.

39 Техническое задание на создание и внедрение опытного участка АПК «Безопасный город» на территории Челябинского городского округа и пилотных муниципальных образований Челябинской области. Официальный сайт Министерства информационных технологий и связи Челябинской области [Электронный ресурс].

URL:http://mininform74.ru/htmlpages/Show/activities/Informacionnoeobshestvo/APKBezopasnyjgorod (Дата обращения 25.03.2020).

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1 Айламазян, А.К. Информатика и теория развития/ А.К. Айламазян. М.: Наука, 1989. 172с.

2 Берталанфи, Л. Общая теория систем: Критический обзор / Л. Берталанфи // Исследования по общей теории систем: Сборник переводов / под ред. Э.Г. Юдина. М.: Прогресс, 1969. С. 23–82.

3 Борисенко, А.А. О сущности информации/ А.А. Борисенко // Фундаментальные исследования. 2005. № 7. С. 32–33.

4 Винер, Н. Кибернетика или управление и связь в животном и машине; или Кибернетика и общество. 2-е издание / Н. Винер. М., Главная редакция изданий для зарубежных стран, 1983. 391 с.

5 Гадасин, А.В. Концепция триад понятие «информация» как субстанции/ А.В. Гадасин// Ежегодник ВНИИПВТИ: сб. науч. трудов. Минск, 2007. С. 186–190.

6 Захарова, В.К. Применение современных медиакоммуникационных технологий в деятельности органов общественной безопасности и народной прокуратуры КНР / В.К. Захарова // Академическая мысль. 2018. № 2. С. 100–102.

7 Идальго, С. Как информация управляет миром / С. Идальго. М., 2016. 256 с.

8 Копин, П.В. Введение в марксистскую гносеологию / П.В. Копин. Киев: Наукова Думка, 1966. 288 с.

9 Курушин, В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин. М.: Новый Юрист, 1998. 256 с.

10 Лысак, И.В. Информация как общенаучное и философское понятие: основные подходы к определению / И.В. Лысак // Философские

проблемы информационных технологий и киберпространства. 2015. № 2. С. 9–26.

11 Мизин, И.А., Синицын, И.Н., Доступов, Б.Г. Развитие определений «информатика» и «информационные технологии» / под ред. И.А. Мизина. М.: ИПИ АН СССР, 1991. 22 с.

12 Новый оперативно-розыскной закон России: учебно-практическое пособие. 3-е изд. / авт. сост. А.Ю. Шумилов. М., 1997. 48 с.

13 Ожегов, С.И. Толковый словарь русского языка / под ред. Н.Ю. Шведова 4-е изд. / С.И. Ожегов. М.: Азбуковник, 2000. 944 с.

14 Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. 400 с.

15 Пастухов, П.С. Электронный документооборот в уголовном процессе США / П.С. Пастухов // Правопорядок: история, теория, практика. 2018. № 4. С. 81–87.

16 Развитие информационных технологий в уголовном судопроизводстве: моногр. / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2018. 248 с.

17 Саушкин, Б.П. Наукоёмкие технологии – основа технологического суверенитета страны / Б.П. Саушкин. Липецк: ЛГТУ, 1997. 247 с.

18 Седов, Е.А. Эволюция и информация / Е.А. Седов. М.: Наука, 1976. 232 с.

19 Стоинер, Т. К новой теории информации. Информационная революция: наука, экономика, технология: рефератив. сборник / под ред. А.И. Ракитова / Т. Стоинер. М., 1993. 235 с.

20 Тихомиров, Ю.А. Модернизация административного права: от «наказательности» к «регулирующему обеспечению» / Ю.А. Тихомиров // Административное право и процесс. 2015. № 4. С. 5–11.

21 Умняшкин, С.В. Основы теории цифровой обработки сигналов / С.В. Умняшкин. М., 2016. 528 с.

РАЗДЕЛ III ПОСТАНОВЛЕНИЕ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКИЙ ПРАКТИКИ

1 Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // Бюллетень Верховного Суда Российской Федерации. 1996. № 2. С. 1.

2 Определение Конституционного Суда Российской Федерации «По жалобе граждан М.Б.Никольской и М.И.Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона «Об оперативно-розыскной деятельности» от 14 февраля 1999 г. № 18-О // Вестник Конституционного Суда Российской Федерации. 1999. № 3.

3 Приговор Троицкого городского суда Челябинской области от 28 июля 2015 г. № 1-191/2015 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

4 Приговор Курчатовского районного суда г. Челябинска от 10 июля 2019 г. № 1-10/2019 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

5 Приговор Советского районного суда г. Челябинска от 25 июня 2019 г. № 1-161/2019 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 01.04.2020).

6 Решение Металлургического районного суда г. Челябинска от 12 ноября 2018 г. № 12-368/2018 Документ официально опубликован не был [Электронный ресурс]. URL:https://sudact.ru/regular/doc/ (Дата обращения 25.03.2020).

РАЗДЕЛ IV ЭЛЕКТРОННЫЕ ИСТОЧНИКИ

1. Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей. Официальный сайт Федеральной службы государственной статистики Российской Федерации [Электронный ресурс]. Режим доступа. URL: https://gks.ru/free_doc/new_site/business/it/fed_nabl-croc/index.html (дата обращения 01.03.2020)
2. История Госавтоинспекции. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://гибдд.рф/about/history (дата обращения 23.03.2020).
3. Карта расположения средств фиксации преступлений и административных правонарушений в Челябинской области [Электронный ресурс]. URL:https://74.ru/text/auto/ (Дата обращения 25.03.2020).
4. Комплексы фиксации нарушений правил дорожного движенияDigitalPatrol [Электронный ресурс]. URL: http://digitalpatrol.ru/(дата обращения 23.03.2020).
5. Места размещения технических средств автоматической фото - и видеофиксации в Российской Федерации. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://гибдд.рф/milestones?all=true (дата обращения 23.03.2020).
6. Места размещения технических средств автоматической фото - и видеофиксации в Челябинской области. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации

[Электронный ресурс]. URL: https://гибдд.рф/r/74/milestones (дата обращения 23.03.2020).

7. Официальный сайт Министерства юстиции и защиты предпринимателей Федеративной Республики Германии [Электронный ресурс]. – URL: http://www.gesetze-im-internet.de/stpo/index.html (Дата обращения: 12.03.2020).
8. Показатели состояния безопасности дорожного движения. Официальный сайт государственной инспекцией безопасности дорожного движенияМинистерства внутренних дел Российской Федерации [Электронный ресурс]. URL: http://stat.gibdd.ru/ (дата обращения 23.03.2020).
9. Результаты проведения Федеральной целевой программы «Электронная Россия (2002-2010 годы)». Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/programs/6/#section-results (дата обращения 16.03.2020)
10. Уголовно-процессуальный закон Латвийской Республики на русском языке [Электронный ресурс]. URL: http://www.pravo.lv/likumi/29_upz.html(Дата обращения: 12.03.2020).
11. Уголовно-процессуальный кодекс Греческой Республики [Электронный ресурс]. URL: https://docplayer.ru/86989074-Ugolovno-processualnyy-kodeks-grecheskoy-respubliki.html (Дата обращения: 13.03.2020).
12. Уголовно-процессуальный кодекс Литовской Республики [Электронный ресурс]. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482 (Дата обращения: 13.03.2020).
13. Уголовно-процессуальный кодекс Республики Польши от 6 июня 1987 г. № OJ.2020.30 // Законодательный вестник Польши (выпуск от

09.01.2020) [Электронный ресурс]. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-167986851 (Дата обращения: 12.03.2020).

14. Уголовно-процессуальный кодекс Румынии [Электронный ресурс]. URL: https://wolterskluwer.ro/codul-de-procedura-penala/ (Дата обращения: 13.03.2020).
15. Уголовно-процессуальный кодекс Эстонской Республики [Электронный ресурс]. URL:https://v1.juristaitab.ee/sites/www.juristaitab.ee/files/elfinder/ru-seadused (Дата обращения: 13.03.2020).

ПРИЛОЖЕНИЕ 1

Анкета для гражданского населения.

Уважаемые граждане!

Юридический институт Южно-Уральского государственного университета проводит исследование на тему: «Информационные технологии в деятельности правоохранительных органов». Просим Вас принять участие в анкетировании и ответить на предложенные вопросы.

1. Укажите Ваш возраст:

а) до 25 лет;

б) от 26 до 45 лет;

в) от 46 лет и более.

2. Укажите Ваш статус:

а) обучающийся/студент;

б) работающий;

в) пенсионер.

3. Обращались ли Вы в органы государственной власти и органы местного самоуправления с жалобой?

а) да;

б) нет.

4. Укажите, в какой форме была Ваша жалоба?

а) в письменной форме;

б) в электронной форме;

5. Знаете ли Вы, что в органы государственной власти, органы местного самоуправления можно подавать жалобы в электронной форме?

а) да;

б) нет;

6. Если Вы не обращались в органы государственной власти и органы местного самоуправления, укажите, в какой форме Вы бы предпочли обратиться?

а) в электронной форме;

б) в письменной форме;

Спасибо за участие!

ПРИЛОЖЕНИЕ 2

В ходе научного исследования проблемы, обозначенной в выпускной квалификационной работе, был проведено анкетирование среди гражданского населения натему: «Информационные технологии в деятельности правоохранительных органов» в целях установления актуальности обращения в органы государственной власти и органы местного самоуправления в электронной форме. Всего было опрошено 130 человек.

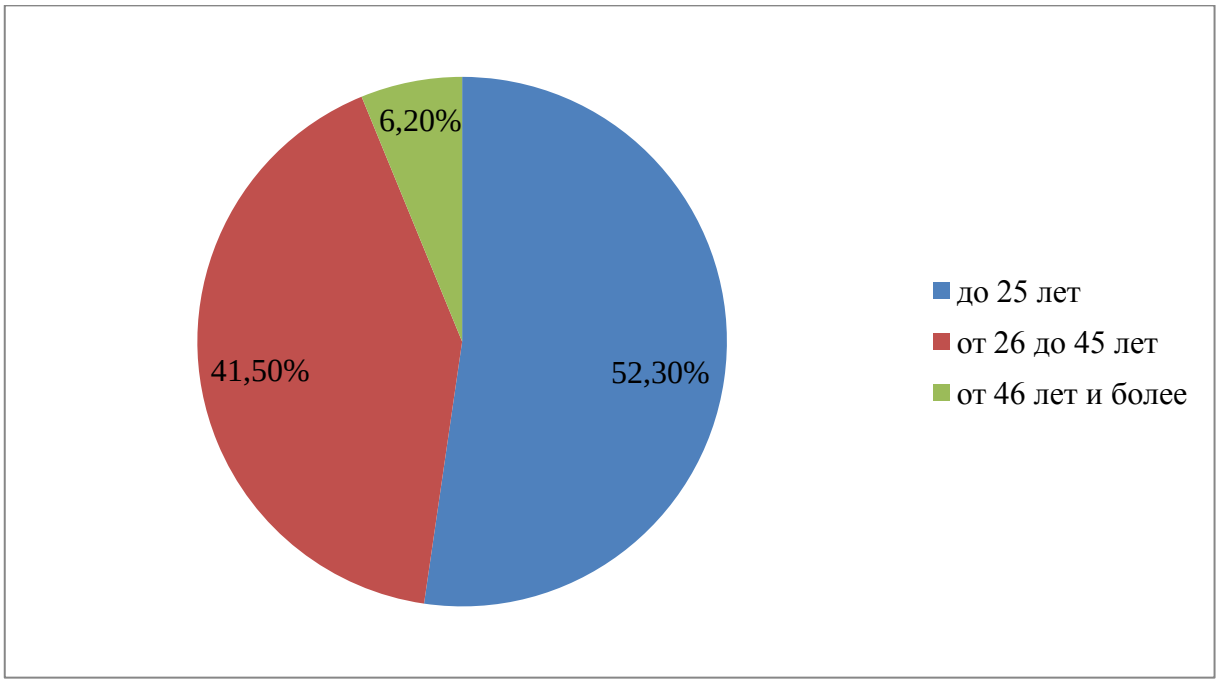

Рисунок 1 – Диаграмма, отражающая возраст опрошенных респондентов.

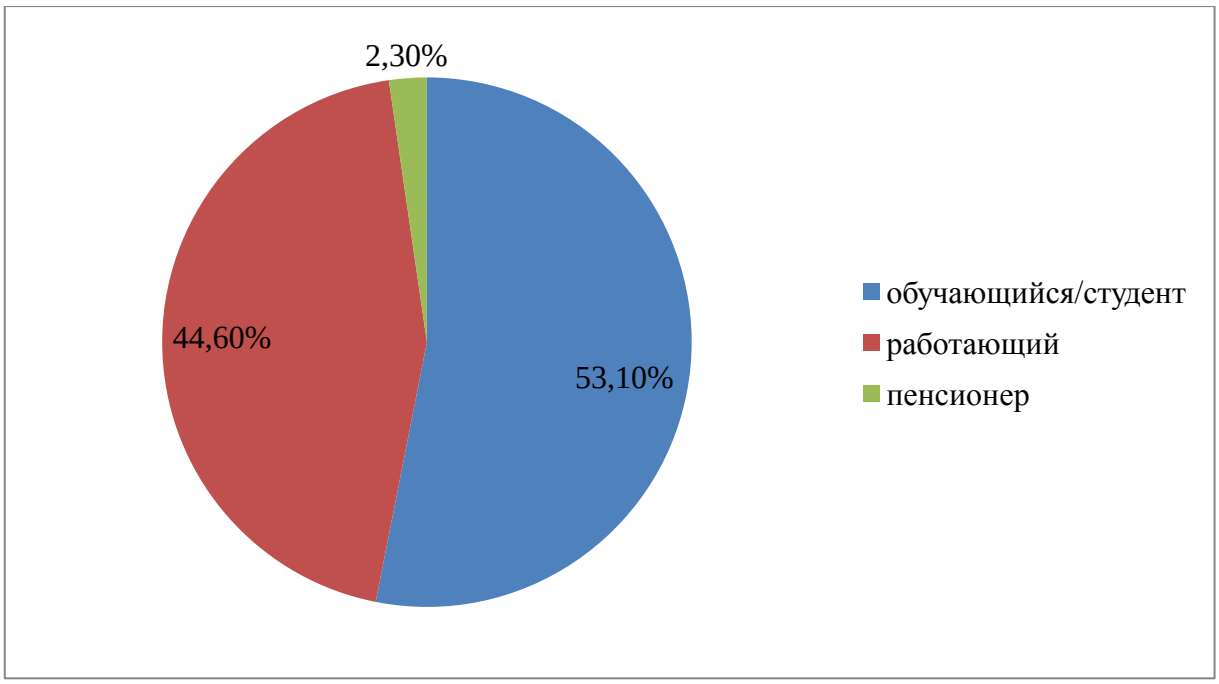

Рисунок 2 – Диаграмма, отражающая социальный статус опрошенных респондентов.

Продолжение приложения 2

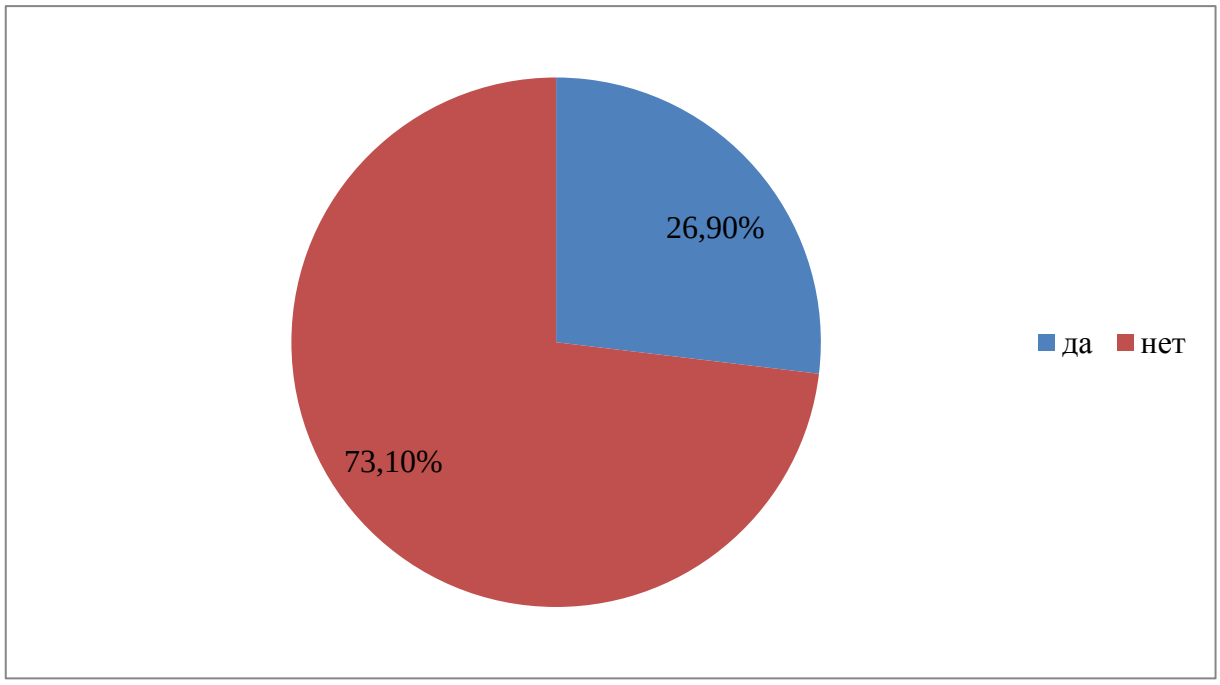

Рисунок 3 – Диаграмма, отражающая факт обращения опрошенных респондентов в органы государственной власти и органы местного самоуправления.

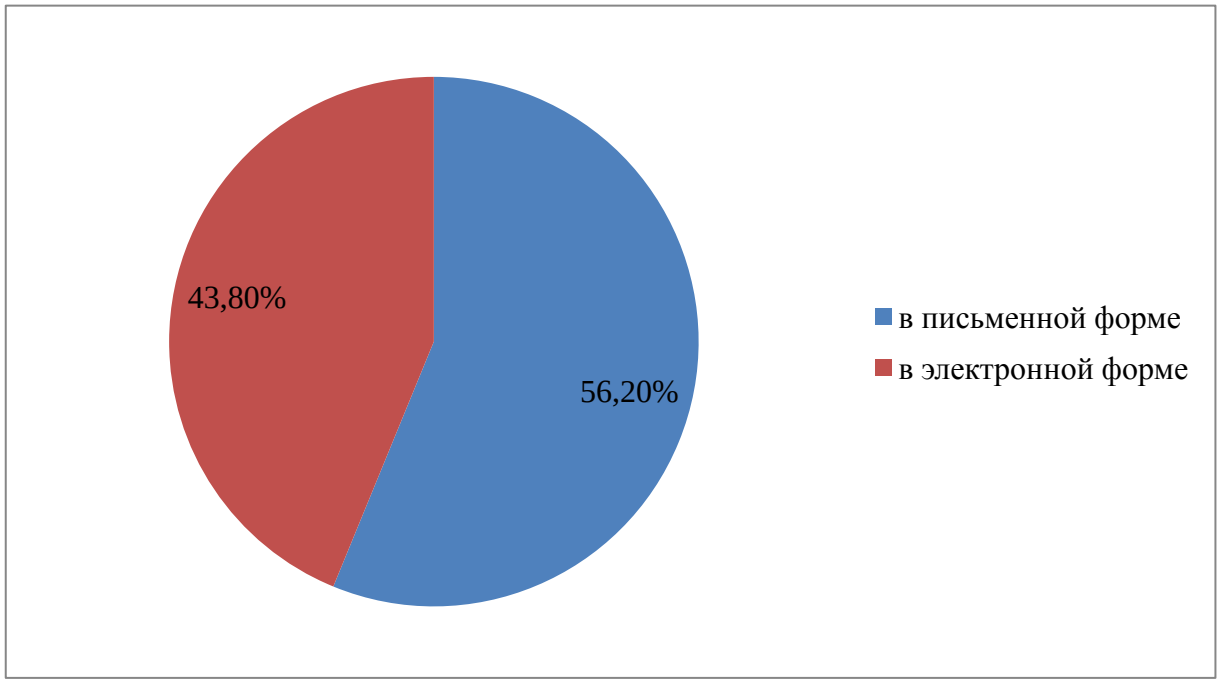

Рисунок 4 – Диаграмма, отражающая формат обращений в органы государственной власти и органы местного самоуправления среди опрощенных граждан.

Продолжение приложения 2

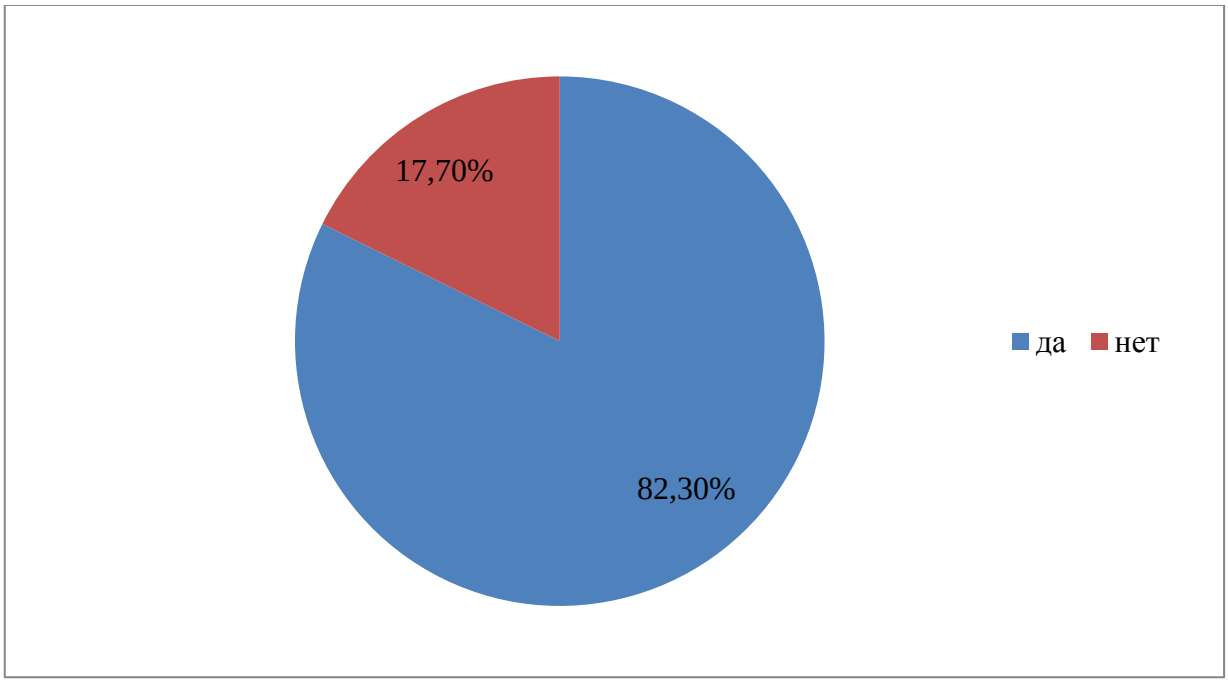

Рисунок 5 – Диаграмма, отражающая осведомленность граждан о возможности подачи обращения в электронной форме в органы государственной власти и органы местного самоуправления.

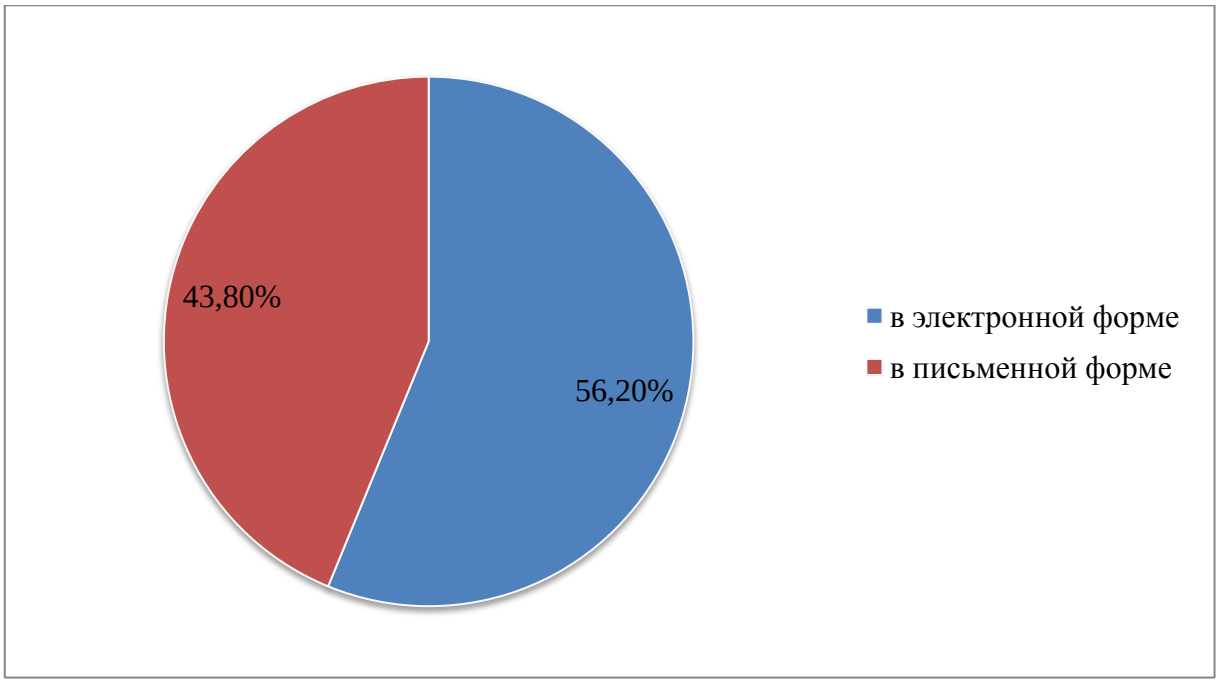

Рисунок 6 – Диаграмма, отражающая мнение граждан относительно того, какую бы форму использовали при обращении в органы государственной власти и органы местного самоуправления.

ПРИЛОЖЕНИЕ 3

Анкета для гражданского населения.

Уважаемые граждане!

Юридический институт Южно-Уральского государственного университета проводит исследование на тему: «Использование информационных технологий при расследовании уголовных дел». Просим Вас принять участие в анкетировании и ответить на предложенные вопросы.

1. Укажите Ваш возраст:

а) до 25 лет;

б) от 26 до 45 лет;

в) от 46 лет и более.

2. Укажите Ваш статус:

а) обучающийся/студент;

б) работающий;

в) пенсионер.

3. Знаете ли Вы о возможности подачи заявления о преступлении в правоохранительные органы в электронной форме?

а) да;

б) нет.

4. Считаете ли Вы удобным способом подачи заявления о преступлении в электронной форме?

а) да;

б) нет.

5. Укажите, является ли для Вас доступным способ подачи заявления в электронной форме?

а) да, у меня есть возможность выхода в информационно-телекоммуникационную систему «Интернет»;

б) нет, у меня отсутствуют средства выхода в информационно-телекоммуникационную сеть «Интернет»;

в) нет, я не умею пользоваться информационными технологиями с возможностью выхода в информационно-телекоммуникационную сеть «Интернет».

6. Укажите, какими, по Вашему мнению, положительными свойствами обладает электронное заявление о преступлении?

а) эффективность;

б) оперативность;

в) экономия времени;

г) возможность заявить о преступлении в любое время и в любом месте;

7. Укажите, какими, по Вашему мнению, отрицательными свойствами обладает электронное заявление о преступлении:

а) нет возможности выхода в сеть «Интернет»;

б) отсутствуют навыки работы с электронными устройствами с выходом в сеть «Интернет»;

в) личные данные попадают в сеть «Интернет»;

г) отсутствует возможность подробно объяснить обстоятельства происшествия;

д) не обнаружено отрицательных свойств.

Спасибо за участие!

ПРИЛОЖЕНИЕ 4

В ходе научного исследования проблемы, обозначенной в выпускной квалификационной работе, был проведено анкетирование среди гражданского населения на тему: «Информационные технологии в деятельности правоохранительных органов» в целях установления актуальности заявления о преступлении в правоохранительные органы в электронной форме. Всего было опрошено 92 человека.

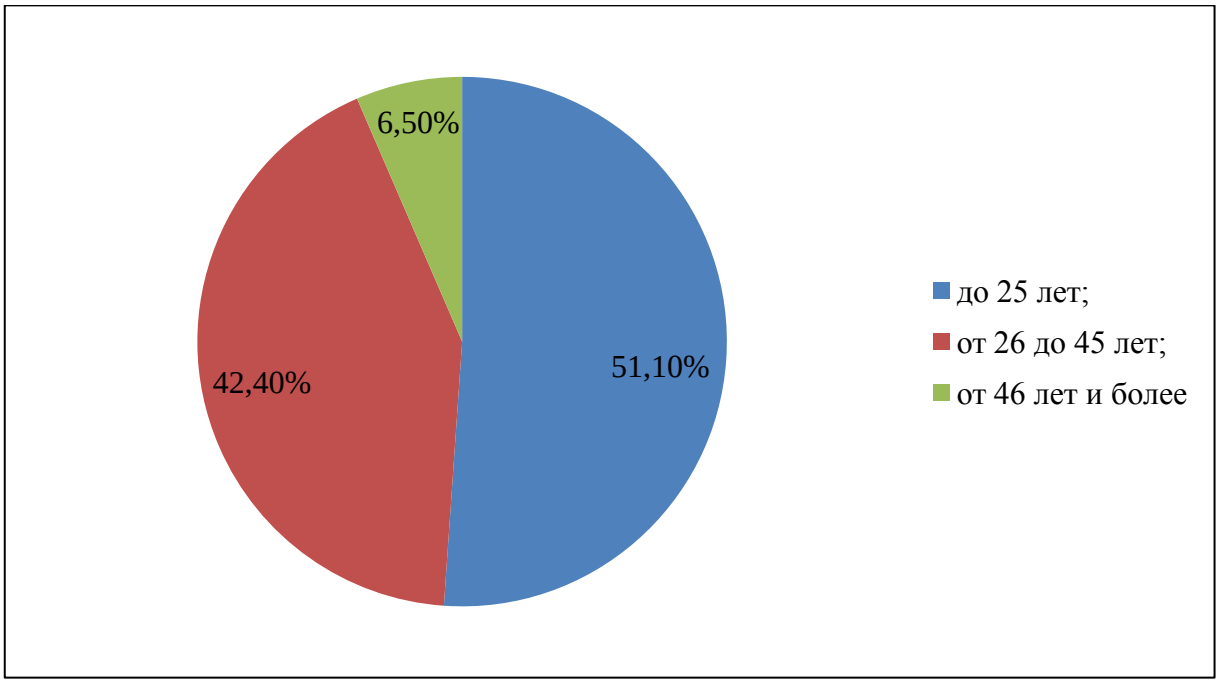

Рисунок 1 – Диаграмма, отражающая возраст опрошенных респондентов.

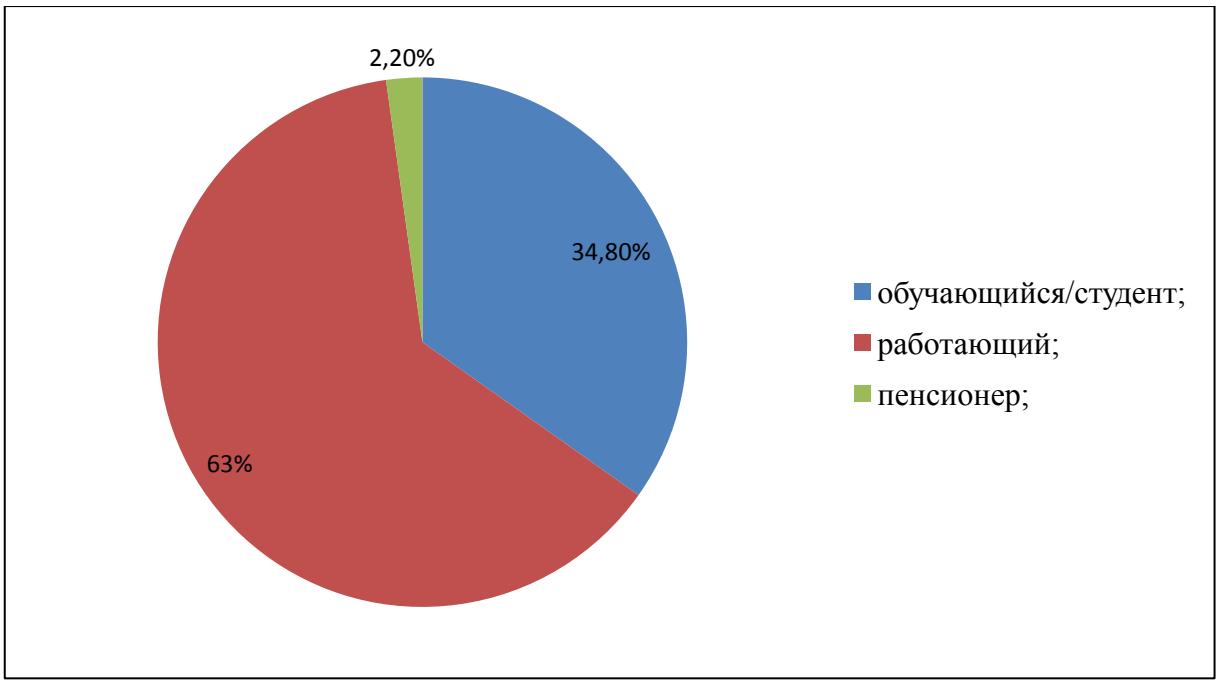

Рисунок 2 – Диаграмма, отражающая социальный статус опрошенных респондентов.

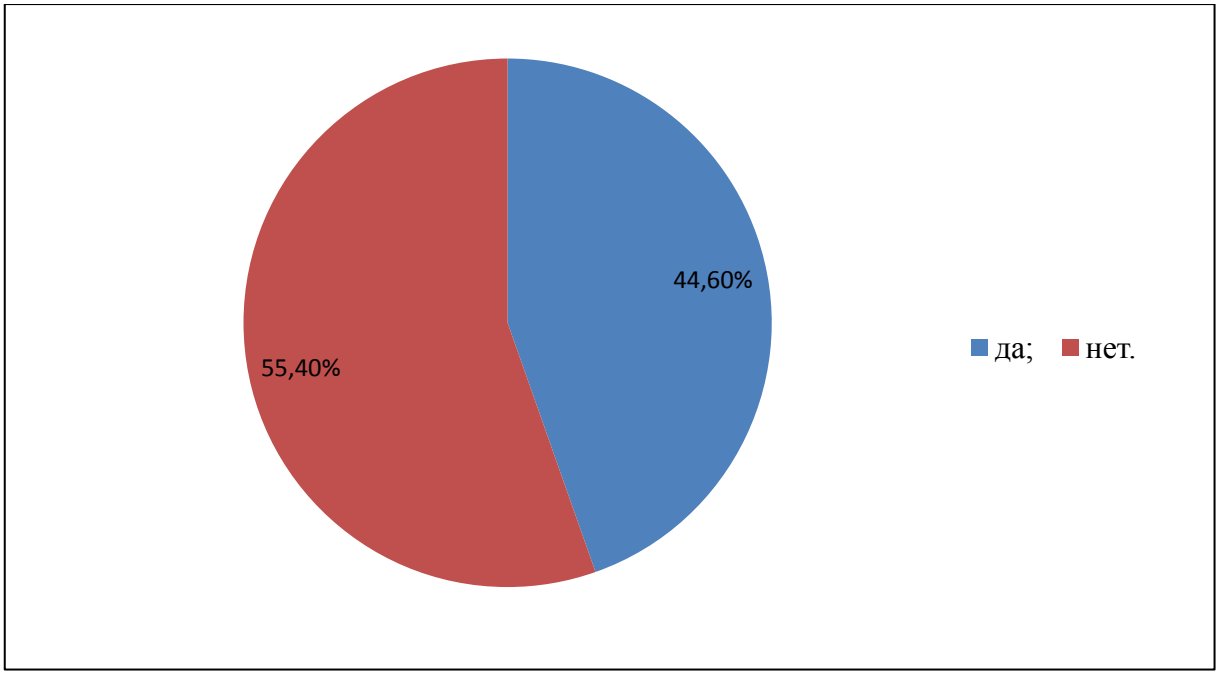

Рисунок 3 – Диаграмм, отражающая осведомленность респондентов о возможности подачи заявления о преступлении в электронной форме.

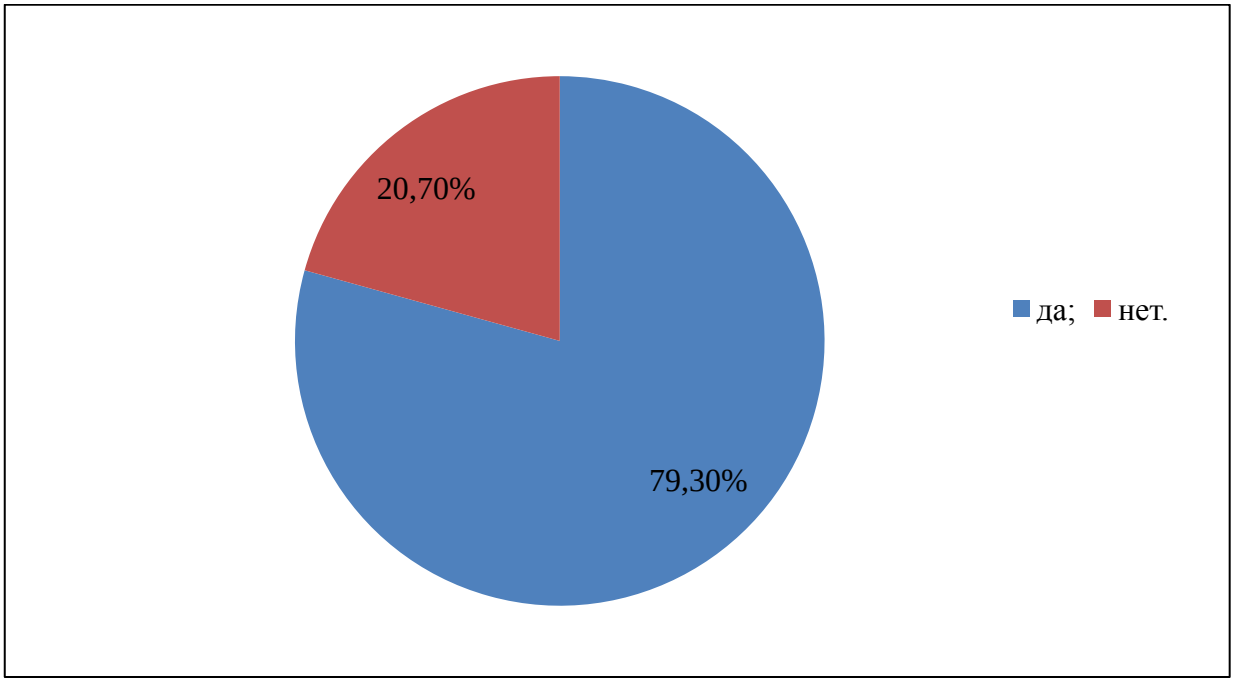

Рисунок 4 – Диаграмма, отражающая отношение респондентов к удобству заявления о преступлении в электронной форме.

Рисунок 5 – Диаграмма, отражающая отношение респондентов к доступности заявления о преступлении в электронной форме.

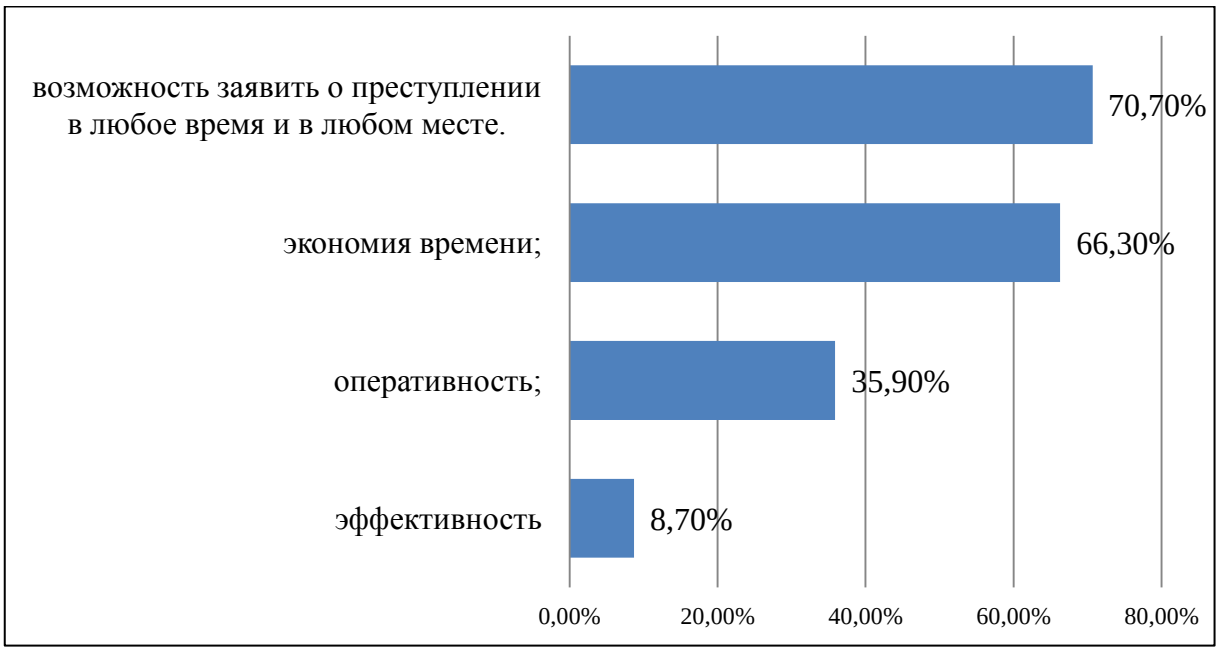

Рисунок 6 – Диаграмма, отражающая мнение респондентов о положительных свойствах электронного заявления о преступлении.

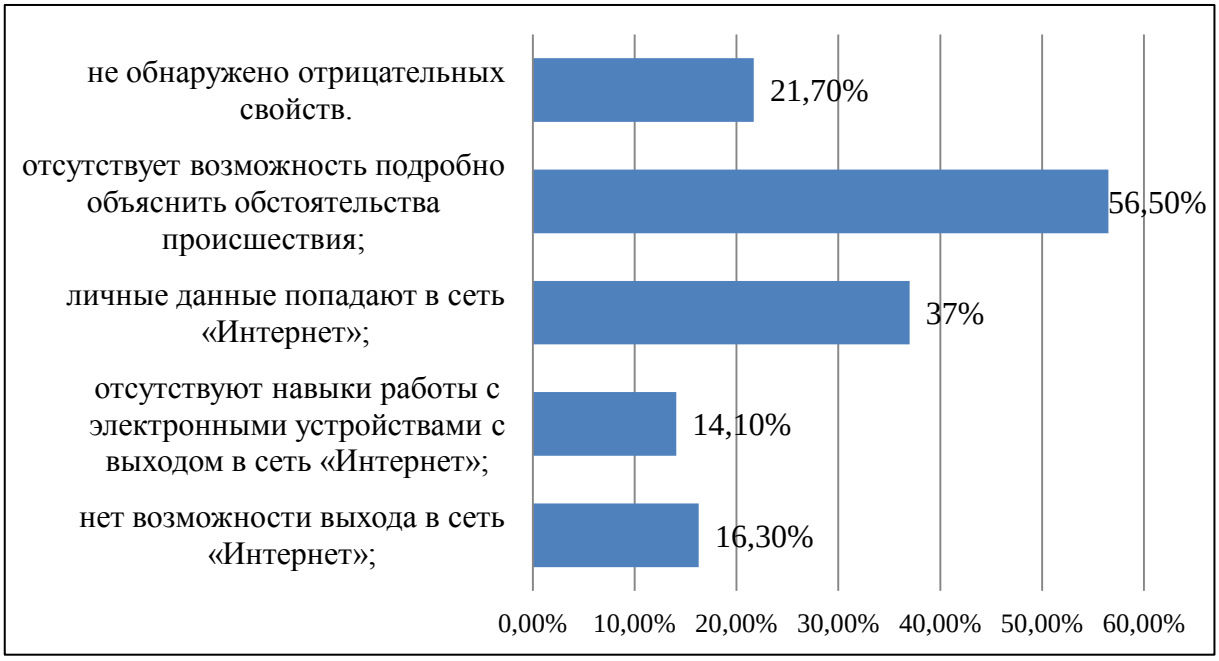

Рисунок 7 – Диаграмма, отражающая мнение респондентов об отрицательных свойствах электронного заявления о преступлении.

ПРИЛОЖЕНИЕ5

Проект №_____
Внесен Правительством
Российской Федерации

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О ВНЕСЕНИИ ИЗМЕНЕНИЙ
ВУГОЛОВНО-ПРОЦЕССУАЛЬНЫЙКОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 1.

Внести в Уголовно-процессуальный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 2001, № 52, ст.4921; 2002, № 22, ст.2027; № 30, ст.3020, 3029; № 44, ст.4298; 2003, № 27, ст.2700, 2706; № 50, ст.4847; 2004, № 27, ст.2711; 2005, № 1, ст.13; 2006, № 28, ст.2975, 2976; № 31, ст.3452; 2007, № 1, ст.46; № 24, ст.2830, 2833; № 49, ст.6033; № 50, ст.6248; 2009, № 11, ст.1267; № 44, ст.5170; 2010, № 1, ст.4; № 15, ст.1756; № 21, ст.2525; № 27, ст.3431; № 31, ст.4164, 4193; № 49, ст.6412; 2011, № 1, ст.16; № 23, ст.3259; № 30, ст.4598, 4605; № 45, ст.6334; № 50, ст.7361, 7362; 2012, № 10, ст.1162, 1166; № 30, ст.4172; № 31, ст.4330, 4331; № 47, ст.6401; № 49, ст.6752; № 53, ст.7637; 2013, № 26, ст.3207; № 27, ст.3442, 3478; № 30, ст.4078; № 44, ст.5641; № 51, ст.6685; № 52, ст.6945; 2014, № 19, ст.2303, 2310, 2333; № 23, ст.2927; № 26, ст.3385; № 30, ст.4219, 4259, 4278; № 48, ст.6651; 2015, № 1, ст.83, 85; № 6, ст.885; № 21, ст.2981; № 29, ст.4391; 2016, № 1, ст.61; № 14, ст.1908; № 18, ст.2515; № 26, ст.3868; № 27, ст.4256, 4257, 4258, 4262; № 28, ст.4559; № 48, ст.6732; № 52, ст.7485; 2017, № 15, ст.2135; № 24, ст.3489; № 31, ст.4743, 4752, 4799; № 52, ст.7935; 2018, № 1, ст.53, 85; № 18, ст.2569, 2584; № 27, ст.3940; № 31, ст.4818; № 53, ст.8446, 8456; 2019, № 14, ст.1459; № 30, ст.4108, 4111)

изменения, дополнив статьей 141.1 следующего содержания:

« Статья 141.1. Электронное заявление о преступлении

1. Электронное заявление о преступлении подается путем направления электронной формы посредством программного обеспечения на официальных сайтах правоохранительныхи иных государственных органов Российской Федерации, предусматривающего обязательное заполнение реквизитов, необходимых для работы с заявлением о преступлениях.

2. Обязательные реквизиты:

а) фамилия, имя и отчество заявителя;

б) адрес электронной почты, по которому должны быть направлены решения, принятые впоследствии проверки заявления, и уведомление о перенаправлении заявления по подследственности в соответствии со статьей 151 настоящего Кодекса;

в) сообщение сведений, указывающих на признаки совершенного или готовящегося к совершению преступления, либо сведений о событиях, угрожающих личной или общественной безопасности;

3. Заявитель вправе приложить к электронному заявлению все необходимые документы и материалы в электронной форме.

4. Заявитель предупреждается об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 Уголовного кодекса Российской Федерации, о чем в электронной форме документа делается отметка».

Статья 2.

Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент
Российской Федерации