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»

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.01. 2016. 514. ВКР

Руководитель работы,
д-р. юрид. наук, доцент
заведующий кафедрой
_____Сергей Васильевич Зуев
_____2021 г.

Автор работы,
студент группы Ю-514
____Александр Андреевич Маторин
_____2021 г.

Нормоконтролер,
___Наталья Владимировна Агаркова
_____2021 г.

Челябинск
2021

АННОТАЦИЯ

Маторин А.А.. Выпускная квалификационная работа «Использование цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации»: ФГАОУ ВО «ЮУрГУ (НИУ)», Ю-514, 84 с., библиогр. список – 77 наим., прил. 1.

Объектом работы являются общественные отношения, складывающиеся по поводу использования цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации.

Цель работы –изучение использования цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации.

В работе рассмотрены информационные технологии: история развития и современный этап, изучено нормативно-правовое регулирование использования информационных технологий, рассмотрено внедрение цифровых технологий в деятельность правоохранительных органов, проанализирована зарубежная практика использования информационных технологий в правовом обеспечении национальной безопасности страны, а также сформулированы предложения по разрешению данных проблем.

Результаты работы имеют практическую значимость, содержат выводы, практические рекомендации и предложения автора по совершенствованию норм.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы. Эра информационных технологий постепенно затрагивает все сферы жизни российского общества.

Создание электронных писем, справочно- информационных интернет-порталов, государственных автоматизированных систем, смарт-контрактов и многих других информационных продуктов меняет нашу привычную жизнь. Например, на данный момент идея отмены бумажных российских паспортов практически реализована, в 2022 году выдадут последние бумажные документы (в пределах г. Москвы), а на смену им придет электронный документ; с 2021 года предполагается полный переход на электронные трудовые книжки.

В ряде зарубежных стран осуществляется переход от бумажных уголовных дел к электронным (в их числе Германия, США, Канада, Эстония, Грузия, Саудовская Аравия, Сингапур, Южная Корея)[1]. Следует отметить, что в РФ на июль 2015 года Генеральная прокуратура РФ не смогла определить местонахождение 270 тыс. уголовных дел.[2] Также в иностранных государствах (например, Германия, Италия, Финляндия, Швеция, Эстония)[3] используется видео-конференц-связь, дистанционный допрос, депонирование показаний.

Подобные нововведения вызывают дискуссии о позитивности данных изменений. Положительны или отрицательны подобные новшества? Вероятно, покажет практика и время. Но бесспорно только то, что

---

[1] Зуев С.В. Электронное уголовное дело: за и против. Правопорядок: история, теория, практика. 2018. №4 (19). С.6–10

[2] Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: Дис..... канд. юрид. наук. Н. Новгород. 2016. С. 188.URL: https://search.rsl.ru/ru/record/01006659588 (Дата обращения: 29.03.2021)

[3] Антонович Е.К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства российской федерации и законодательства некоторых иностранных государств). Актуальные проблемы российского права. 2019. № 6 (103). С. 125–136.

«цифровизация» нашей жизни неизбежна, и она коснётся всех сфер общественной жизни, в том числе и уголовного процесса, а именно предварительного расследования, а именно следственных действий, в ходе которых формируется совокупность доказательств по конкретному уголовному делу. Следственные действия имеют огромное значение для расследования любых видов преступлений и каждый вид следственного действия выполняет свою функцию и имеет свое значение, свои задачи, но вместе они служат единой цели – объективному и всестороннему расследованию преступления.

На протяжении длительного времени постоянно совершенствуется законодательное регулирование информационного обеспечения уголовного судопроизводства. Однако законодатель этим занимается несистемно и непоследовательно. Информационные технологии открывают новые возможности для появления качественно новых преступлений, поэтому стандартный набор средств доказывания, следственных действий на сегодняшний день необходимо модифицировать. Так как необходимо помнить, что главным назначением уголовного судопроизводства являются: защита прав и законных интересов лиц и организаций, потерпевших от преступлений и защита личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод (ст. 6 УПК РФ).

Именно прогрессивное использование информационных технологий в уголовном судопроизводстве окажет положительное влияние на уровень предварительного расследования, повысит качество гарантий, предоставленных участникам уголовного процесса, так как при их применении выполнение некоторых процессуальных действий, которые ранее проводились в очень длительные сроки, перестает быть затруднительным, появляются возможности для создания новых следственных действий.

На данный момент эффективность правоохранительной деятельности в значительной степени зависит от качества поддержки информационной

сферы в Российском государстве, в связи с этим информационные технологии находят многостороннее применение в деятельности сотрудников правоохранительных органов.

Информационные технологии, которые используются в правоохранительной деятельности, выглядят как систему процессов по сбору, хранению, обработке и передаче информации, необходимой для пресечения, предотвращения и раскрытия преступлений, осуществляемых с помощью компьютерной техники.

В результате развития технологического прогресса и информационных систем и технологий, которые используются повсеместно, в каждой из сфер жизнедеятельности человека, правоохранительные органы начали широко использовать информационные системы для своих целей и задач, а также для защиты прав и свобод человека и гражданина.

Актуальность выбранной темы выпускной квалификационной работы обусловлена необходимость рассмотреть быстроменяющиеся информационные и цифровые технологии, применяемыми сотрудниками правоохранительных органов для обеспечения национальной безопасности.

Степень научной разработанности темы исследования. Вопросы, связанные с информационно-цифровым обеспечением Органов Внутренних Дел, широко рассматриваются в специальной литературе. Большой вклад в разработку множества аспектов данной проблематики внесли такие ученые, как Н.П. Водько, Ю.С. Блинов, В.М. Атмажитов, В.Г. Бобров, С.С. Галахов, Д.В. Гребельский, В.Ю. Голубовский, В.Г Кувалдин, Н.А. Климов, В.Г Кувалдин, А.Г. Лекарь, В.Д. Ларичев, В.А. Лукашов, В.Ф. Луговик, А.С Овчинский, С.С. Овчинский, В.Н. Омелин, Е.Н. Яковец Г.К. Синилов, и другие.

Объект исследования – общественные отношения, складывающиеся по поводу использования цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации.

Предмет исследования – нормативно-правовые акты, регламентирующие использование цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации.

Цель выпускной квалификационной работы – изучить использование цифровых технологий органами внутренних дел в обеспечении национальной безопасности Российской Федерации.

Для достижения поставленной цели необходимо решить следующие задачи:

– изучить историю развития и современный этап развития информационных технологий;

– описать нормативно-правовое регулирование использования информационных технологий;

– исследовать внедрение цифровых технологий в деятельность правоохранительных органов;

– изучить зарубежную практику взаимодействия информационных технологий и правоохранительных органов, с целью обеспечения национальной безопасности страны.

Методологическую основу данного научного исследования составляет диалектико-материалистическое познание. В качестве научного инструментария использовались такие методы научного познания, как формально-логический, исторический, системный, сравнительно-правовой, моделирование, анкетирование, интервьюирование, наблюдение и др.

Нормативно-правовую базу исследования составляют следующие акты: Конституция РФ; акты международного законодательства, регулирующие использование информационных технологий; уголовно-процессуальное, оперативно-розыскное, уголовное и административное законодательство, а также другие нормативные правовые акты Российской Федерации.

Теоретическую основу исследования составили научные издания по исследуемой проблематике, учебная литература (учебные пособия,

комментарии к законодательству, учебники и монографии), статьи в периодических изданиях по исследуемой проблематике. При написании работы использовались научные труды следующих авторов: Венедиктова А.А., Волков А.Н., Карманов Е.А., Розанова Е.В., Соловьев А.А., Таранова Д.В., Харламов П.В., Черноусова Н.В., Шеяфетдинова Н.А., а также других учёных рассматривающих данную тему.

Структура выпускной квалификационной работы состоит из введения, двух глав, заключения и библиографического списка.

1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИИ

1.1. Информационные технологии: история развития и современный этап

В настоящее время развитие информационных технологий является основным направлением формирования современного общества.

Информационная технология – это процесс, использующий совокупность методов, производственных процессов и программно-технических средств, объединенных технологическим процессом по сбору, хранению, обработке, выводу и распространению информации для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности[1].

Информационная технология – процесс, использующий совокупность средств и методов сбора, получения, накопления, хранения, обработки, анализа и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта)[2]. Итак, в Федеральном законе «Об информации, информационных технологиях и о защите информации» информационные технологии определяется как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

---

[1] Иванова С.И., Микаилов С.М. Стратегия национальной безопасности Российской Федерации и основные направления деятельности полиции // Юридическая наука и правоохранительная практика. 2017. №2 (40). URL: https://cyberleninka.ru/article/n/strategiya-natsionalnoy-bezopasnosti-rossiyskoy-federatsii-i-osnovnye-napravleniya-deyatelnosti-politsii (дата обращения: 04.04.2021).

[2] Венедиктова А.А., Волков А.Н., Таранова Д.В. Влияние информатизации общества на экономическую безопасность государства // Сборник статей-презентаций научно-исследовательских работ студентов, магистров, аспирантов, молодых ученых - участников Международной Межвузовской Студенческой конференции по проблеме «Национальная безопасность как основа конкурентоспособности и экономического роста страны». 2019. С. 51–59.

Информационные ресурсы – совокупность данных представляющих ценность для организации и выступающих в качестве материальных ресурсов. К ним относятся файлы данных, документы, тексты, графики, знания, аудио- и видеоинформация.

Анализ определений сущности информационных технологий позволяет сделать вывод, что в современных условиях они становятся эффективным инструментом совершенствования управления организацией, особенно в таких областях управленческой деятельности, как стратегическое управление, управление, делопроизводство, управление персоналом и организационная культура.

Основная цель применения информационных технологий – производство информации для ее анализа человеком и принятия на его основе решения по выполнению обеспечивать эффективное использование информационных ресурсов:[1]

– при разработке стратегических планов развития организаций;

– в процессе изучения влияния инвестиционно-инновационной деятельности;

– для обеспечения конкурентоспособности подразделений организации на основе учета мнения клиентов, состояния конкурентов;

– для осуществления поддержки принятия управленческих решений[2].

Развитие информационных технологий во всем мире объясняется возросшей интенсивностью информационных потоков вследствие развития процессов глобализации мировой экономики и становления информационного пространства.

---

[1] Несмиянова Ирина Олеговна Информационные технологии: этапы развития, понятие и классификация // Известия ТулГУ. Экономические и юридические науки. 2020. №1. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-etapy-razvitiya-ponyatie-i-klassifikatsiya (дата обращения: 13.04.2021).

[2] Шеяфетдинова Н.А., Соловьев А.А., Розанова Е.В., Черноусова Н.В., Харламов П.В., Карманов Е.А. Взаимоотношения государства и общества в фокусе новых технологий и информатизации // Современное право. 2021. № 1. С. 510.

Существует несколько точек зрения на развитие информационных технологий с использованием компьютеров, которые определяются различными признаками деления. Общим для всех изложенных ниже подходов является то, что с появлением персональных компьютеров начался новый этап развития информационных технологий. Основной целью становится удовлетворение персональных информационных потребностей человека, как для профессиональной, так и для бытовой сферы[1].

В процессе своего развития информационные технологии прошли через ряд этапов, начало которых связывается с появлением электронных вычислительных машин.

1. Первый этап охватывает период с конца 60-х до начала70-х годов, когда с появлением электронных вычислительных машин первого поколения встала задача ускорения процесса кодирования программ по заранее формализованным алгоритмам.

2. Второй этап развития информационных технологий охватывает период с начала 70-х до начала 80-х годов, который характеризуются появлением моделей единой системы электронных вычислительных машин третьего поколения, отличающихся друг от друга только быстродействием и объемом оперативной памяти.

3. Третий этап развития информационных технологий охватывает период с начала 80-х годов до начала 90-х годов.

В этот период появилась тенденция замены программистов на конечных пользователей, т. е. специалистов в конкретной предметной области, но не имеющих профессиональной подготовки в области вычислительной техники и программирования, благодаря появлению на рынке компьютерных средств настольных микроэлектронных

[1] Антонович Е.К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства российской федерации и законодательства некоторых иностранных государств). Актуальные проблемы российского права. 2019. № 6 (103). С. 125–136

вычислительных машин, ориентированных на персональный режим работы и получивших название персональных компьютеров.

Таким образом, 4-й этап (с середины 80 – х – начало 90 – х) – «компьютерная» («новая») технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов для различных целей. Информационные технологии широко применяются в различных областях науки и техники.

Отсюда, информационная технология – это процесс, использующий совокупность методов, производственных процессов и программно-технических средств, объединенных технологическим процессом по сбору, хранению, обработке, выводу и распространению информации для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности.

1.2. Нормативно-правовое регулирование использования информационных технологий

Информационно-коммуникационные технологии являются одними из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества[1].

Так, первым государственным органом в СССР, в названии которого появилось слово «информатика» (термина «информатизация» тогда еще не было), а в выполняемых функциях – слово «координация», был Государственный комитет СССР по вычислительной технике и информатике (ГКВТИ СССР), созданный по постановлению ЦК КПСС и Совета Министров СССР от 20.03.1986 № 361 «Об улучшении координации работ в

[1]Окинавская Хартия Глобального информационного общества http://www.iis.ru/library/okinawa/charter.ru.html (дата бращения:30.03.2021)

области вычислительной техники и о повышении эффективности ее использования»[1].

Практически все координационные функции Государственного комитета СССР по вычислительной технике и информатике, определенные в Положении о ГКВТИ (утв. постановлением Совета Министров СССР от 21.04.1987 № 456), звучат вполне современно и актуально, несмотря на то, что они были сформулированы более 30 лет назад. Вот лишь пара примеров:[2]

– координация и научно-методическое руководство разработкой целевых программ по повышению эффективности использования вычислительной техники и автоматизированных систем в народном хозяйстве и контроль за их выполнением, подготовка и утверждение научно-методической документации для формирования этих программ, методическое руководство и координация деятельности межотраслевых научно-технических комплексов в области вычислительной техники и информатики;

Одним из главных концептуально-стратегических результатов деятельности Государственного комитета СССР по вычислительной технике и информатике СССР стала разработка и публикация «Концепции информатизации советского общества».

Сегодня, с высоты исторического знания, следует признать, что Государственный комитет СССР по вычислительной технике и информатике СССР был первым и, видимо, последним полноправным и полноценным координатором государственной информатизации в нашей стране. У Государственного комитета СССР по вычислительной технике и информатике было все: финансовые и материальные ресурсы, властные и

[1] Постановление ЦК КПСС и Совета Министров СССР от 20.03.1986 № 361 «Об улучшении координации работ в области вычислительной техники и о повышении эффективности ее использования» // Режим доступа: http://www.consultant.ru (дата обращения:30.03.2021)

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901

контрольные полномочия, четко определенные задачи и зоны ответственности, критерии оценки эффективности деятельности.

Государственный комитет СССР по вычислительной технике и информатике СССР был упразднен 1 апреля 1991 года. «Концепция информатизации советского общества» так и не была реализована.

Указом Президента Российской Федерации от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации»[1]:

– определены основные направления государственной политики в сфере информатизации;

– образован Комитет при Президенте РФ по политике информатизации (Роскоминформ);

– определены основные задачи Роскоминформа.

Среди наиболее значимых результатов деятельности Роскоминформа:

– разработка проекта федеральной целевой программы «Информатизация России» (1994);

– разработка проекта «Концепции формирования и развития законодательства в сфере информации, информатизации и информационной безопасности в Российской Федерации» (1995).

Позднее на основе этого проекта был разработан проект «Программы формирования и развития информационного законодательства в Российской Федерации»;

– разработка и принятие Федерального закона от 25.01.1995 № 24-ФЗ «Об информации, информатизации и защите информации»[2]. Закон стал первым нормативно-правовым актом РФ высшего уровня, посвященным вопросам информатизации;

[1] Указ Президента РФ от 20.01.1994 № 170 (ред. от 09.07.1997) «Об основах государственной политики в сфере информатизации» // Российская газета. 1994. № 19

[2] Федеральный закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003) «Об информации, информатизации и защите информации» // Собрание законодательства РФ. 1995. № 8. Ст. 609. – утратил силу

– разработка «Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов» (1995);

– разработка проекта программы «Создание и использование федеральных и межотраслевых баз и банков данных».

Большинство пунктов Указа № 170 утратило силу в 1997 году в связи с тем, что основные положения государственной политики в сфере информатизации были перенесены в принятый 25.01.1995 Федеральный закон № 24–ФЗ «Об информации, информатизации и защите информации» (предшественник Федерального закона от 27.07.2006 № 149–ФЗ). За 30 с лишним лет российской госинформатизации было разработано около десятка концептуальных документов, содержавших стратегические аспекты. В силу ограниченных сроков, на которые разрабатывались эти концепции, ни одна из них не актуальна в качестве действующего документа, хотя некоторые базовые идеи из них нашли свое место в действующих сегодня НПА.

Основу для разработки стратегического планирования в сфере информационных технологий в конце 2000-х годов заложила «Стратегия развития информационного общества в Российской Федерации», утвержденная Указом Президента РФ от 07.02.2008 № Пр–212[1].

Основными направлениями реализации «Стратегии…» были объявлены:

– формирование современной информационной и телекоммуникационной инфраструктуры, предоставление на ее основе качественных услуг в сфере информационных и телекоммуникационных технологий и обеспечение высокого уровня доступности для населения информации и технологий;

[1] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 N Пр–212) // Российская газета. 2008. № 34. – утратил силу

– повышение качества образования, медицинского обслуживания, социальной защиты населения на основе развития и использования информационных и телекоммуникационных технологий;

– совершенствование системы государственных гарантий конституционных прав и свобод человека и гражданина в информационной сфере;

– развитие экономики Российской Федерации на основе использования информационных и телекоммуникационных технологий;

– повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг;

– развитие науки, технологий, техники и подготовка квалифицированных кадров в сфере информационных и телекоммуникационных технологий;

– сохранение культуры многонационального народа Российской Федерации, укрепление нравственных и патриотических принципов в общественном сознании, развитие системы культурного и гуманитарного просвещения;

– противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России.

Первым документом стратегического характера в сфере информационных технологий, разработанным в начале 2010-х годов стала государственная программа «Информационное общество (2011–2020)»[1]. Она считается наследницей федеральной целевой программы «Электронная Россия», хотя наследие здесь скорее календарное, а не концептуальное.

[1] Постановление Правительства РФ от 21.10.2016 N 1083 «О внесении изменений в Государственную программу Российской Федерации «Информационное общество (2011 – 2020 годы)» // Собрание законодательства РФ. 2016. № 44. Ст. 6139

Первоначально сроки реализации государственной программы «Информационное общество (2011–2020)» были установлены в диапазоне 2010–2020 годов, однако в связи с тем, что в 2019 году в состав государственной программы «Информационное общество (2011–2020)» были включены федеральные проекты нацпрограммы «Цифровая экономика», имевшие срок реализации 2019–2024, до 2024 года была продлена (с изменением параметров финансирования и контрольных показателей) и вся государственная программа «Информационное общество (2011–2020)»

Ожидается, что в ближайшее время сроки реализации государственной программы «Информационное общество (2011–2020)» снова будут скорректированы – теперь до 2030 года, так как до этого года планируется продлить все нацпроекты.

Все редакции государственной программы «Информационное общество (2011–2020)», принятые после 2014 года, разрабатывались уже с учетом принятого Федерального закона № 172-ФЗ. В 2017 году была принята «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»[1].

«Стратегия развития информационного общества», утвержденная Указом Президента РФ от 09.05.2017 № 203, – главнейший стратегический документ для сферы государственных информационных технологий.

Новая редакция вышеуказанной Стратегии понадобилась в связи с тем, что у предыдущей редакции, утвержденной в 2008 году, закончился «срок годности»: она охватывала период только до 2015 года. К тому же её обновление происходило уже после принятия Федерального закона № 172 – ФЗ, и при подготовке новой редакции Стратегии учитывались требования этого закона. Согласно классификации стратегических документов, принятой в 172–ФЗ, Она относится к отраслевым документам стратегического

[1] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901

планирования — именно в этом статусе ее можно найти на портале государственной автоматизированной информационной системы «Управление»[1].

Наряду с обсуждаемой Стратегией, к отраслевым стратегическим документам в сфере информационных технологий отнесены также «Стратегия развития искусственного интеллекта в РФ» (срок действия – 2019–2030 годы)[2] и «Стратегия развития отрасли информационных технологий в РФ»[3] на 2014–2020 годы и на перспективу до 2025 года.

«Стратегия развития искусственного интеллекта в РФ» пока еще носит декларативный характер и позиционируется очень широко, охватывая не только государственные информационные технологии, но фактически все отрасли экономики[4].

Стратегия развития отрасли информационных технологий, наоборот, имеет довольно узкое позиционирование – прежде всего касается компаний, создающих ИТ-продукцию, – и в этом смысле практически не нацелена конкретно на государственные информационных технологий[5].

Положениями «Стратегии развития информационного общества в Российской Федерации» руководствуются все органы государственной власти РФ и органы местного самоуправления.

---

[1] Несмиянова Ирина Олеговна Информационные технологии: этапы развития, понятие и классификация // Известия ТулГУ. Экономические и юридические науки. 2020. №1. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-etapy-razvitiya-ponyatie-i-klassifikatsiya (дата обращения: 13.04.2021).

[2] «Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // Собрание законодательства РФ. 2019. № 41. Ст. 5700

[3] Распоряжение Правительства РФ от 01.11.2013 № 2036-р (ред. от 18.10.2018) «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года» // Собрание законодательства РФ. 2013. № 46. Ст. 5954.

[4] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901

[5] Рахманин Е.М. Проблемные вопросы терминологии УК РФ, используемой при регулировании вопросов в сфере информационной безопасности // Современные научные исследования и инновации. 2019. № 2. С. 15.

Регулярно обновляемая государственная программа «Информационное общество» также учитывает ключевые установки «Стратегии развития информационного общества».

Она посвящена главным образом информационно-коммуникативным технологиям, как важнейшему элементу национальной инфраструктуры.

В ней определены приоритеты России в сфере информационно-коммуникативных технологий:

– формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

– развитие информационной и коммуникационной инфраструктуры;

– создание и применение российских информационно-коммуникативных технологий, обеспечение их конкурентоспособности на международном уровне;

– формирование новой технологической основы для развития экономики и социальной сферы;

– обеспечение национальных интересов в области цифровой экономики.

Цель формирования информационного пространства знаний (в «Стратегии развития информационного общества» используется и такой термин) состоит в «обеспечении прав граждан на объективную, достоверную, безопасную информацию и создании условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора».

– совершенствование механизмов законодательного регулирования деятельности средств массовой информации, а также таких средств обеспечения доступа к информации, как интернет-телевидение, новостные агрегаторы, социальные сети, сайты, мессенджеры;

– меры по эффективному использованию современных информационных платформ для распространения достоверной и качественной информации российского производства;

– обеспечение условий для научно-технического творчества;

– совершенствование дополнительного образования для привлечения детей к занятиям научными изысканиями и творчеством, развития их способности решать нестандартные задачи;

– создание условий для популяризации русской культуры и науки за рубежом;

– насыщение рынка доступными, качественными и легальными медиапродуктами и сервисами российского производства;

– поддержку традиционных средств распространения информации (радио-, телевещания, печатных средств массовой информации, библиотек);

– информационно-технологическую инфраструктуру.

Государственное регулирование в сфере применения информационных технологий предусматривает:[1]

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

[1] Досье на проект федерального закона № 47591–7 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (внесен 06.12.2016 Правительством РФ). Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456958/ (дата обращения: 04.04.2021).

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей[1].

Вывод: информационная технология – это процесс, использующий совокупность методов, производственных процессов и программно-технических средств, объединенных технологическим процессом по сбору, хранению, обработке, выводу и распространению информации для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности.

С конца 90-х годов и по настоящее время широко внедряется всемирная паутина Интернет, а также появляются технологии информационных хранилищ, электронного документооборота и поддержки принятия решений.

«Стратегия развития информационного общества», утвержденная Указом Президента РФ от 09.05.2017 № 203, – главнейший стратегический документ для сферы государственных информационных технологий.

В вышеуказанной Стратегии определены приоритеты России в сфере информационно-коммуникативных технологий:

1. Формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

2. Развитие информационной и коммуникационной инфраструктуры;

3. Создание и применение российских информационно-коммуникативных технологий, обеспечение их конкурентоспособности на международном уровне;

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 09.03.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 20.03.2021) // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448

4. Формирование новой технологической основы для развития экономики и социальной сферы;

5. Обеспечение национальных интересов в области цифровой экономики.

2. ДЕЙСТВУЮЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

2.1 Внедрение цифровых технологий в деятельность правоохранительных органов

В условиях современных преобразований применение новейших информационных технологий в рамках правоохранительной системы, в том числе в органах внутренних дел, следует считать одним из ключевых направлений максимизации результативности деятельности[1].

Внедрение информационных технологий и телекоммуникаций выступает в качестве неотъемлемого компонента оптимизации деятельности при повышении качества оперативности при прогнозировании оперативной обстановки, своевременном реагировании на правонарушения, разработке модели распределения сил и средств при решении оперативных задач, планировании деятельности производственно-экономических служб и оптимизации управленческой структуры и оценке результативности функционирования подразделений[2].

Перед Россией стоит стратегическая задача – внедрение в деятельность государственных органов инновационных технологий, повышающих объективность и обеспечивающих прозрачность при принятии юридических решений, а также обеспечивающих межведомственное электронное взаимодействие государственных органов и их взаимодействие с гражданами и организациями в рамках оказания государственных услуг, в том числе в правоохранительной сфере. Необходимым инструментом решения подобной задачи является совокупность математических моделей, методов и

[1] Ансель М. Методологические проблемы сравнительного права (фрагменты) / М. Ансель // Вестник Университета имени О.Е. Кутафина. 2015. № 5. С. 187–188.

[2] Пыхтин И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) // Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48.

алгоритмов, ориентированных на выработку оптимального решения в данной обстановке исходя из стоящих правоохранительных задач[1].

Современные технологии не просто следуют алгоритмам, созданным человеком, но самостоятельно корректируют и подстраивают эти алгоритмы с учетом предыдущего опыта, как собственного, так и чужого. Компьютер в состоянии в короткие сроки обработать неимоверный объем данных, что позволяет ему использовать в своей деятельности большое количество факторов и примеров из предыдущего опыта, сравнимое с многолетним опытом специалиста-человека. Кроме того, компьютеры не подвержены субъективным факторам, таким как усталость, плохое самочувствие или дурное настроение, которые могут оказывать значительное влияние на эффективность работы человека, не говоря уже о том, что компьютер может работать круглосуточно, поскольку ему не требуются перерывы на сон и отдых[2].

Раскрывая содержание понятия «правоохранительная деятельность», прежде всего заметим, что оно по-прежнему может считаться дискуссионным, несмотря на большое количество учебников и специальной литературы, посвященной данной проблематике.

Сегодня сложилось два подхода к пониманию правоохранительной деятельности – широкий и узкий, конкретная наполненность которых отличается в зависимости от выбранного основания для классификации.

Так, по такому основанию, как субъекты правоохранительной деятельности, сторонники широкого подхода говорят о том, что она осуществляется всеми органами законодательной, исполнительной и

[1] Никитин Е.В. О новых возможностях применения современных цифровых технологий в правоохранительной деятельности // Правопорядок: история, теория, практика. 2018. №4 (19). URL: https://cyberleninka.ru/article/n/o-novyh-vozmozhnostyah-primeneniya-sovremennyh-tsifrovyh-tehnologiy-v-pravoohranitelnoy-deyatelnosti (дата обращения: 13.04.2021).

[2] Никифорова, Т. С. Оставят ли роботы юристов без работы? / Т. С. Никифорова, К. М. Смирнова // Закон. 2017. № 11. С. 120

судебной власти, обеспечивающими соблюдение прав и свобод человека и гражданина, поддержание законности и правопорядка[1].

Для узкого подхода характерно представление правоохранительной деятельности как деятельности только несудебных государственных органов по охране прав, осуществляемую путем применения властных полномочий по отношению к лицам, не состоящим с ними в отношениях подчинения типа «работодатель – работник»[2].

Некоторые авторы выделяют государственные органы, для которых правоохранительная деятельность является основным видом деятельности, для других – второстепенной и осуществляется наряду с другими.

Являясь одной из правовых форм реализации охранительной функции государства, правоохранительная деятельность зависит от социально-экономической, политической ситуации, складывающейся в обществе, актуальных тенденций развития общественных отношений, уровня правосознания и правовой культуры и т. п. Сегодня мы являемся свидетелями процесса построения информационного общества, которое приходит на смену обществу постиндустриальному. Суть этого процесса достаточно лаконично охарактеризовал Клаус Шваб, президент Всемирного экономического форума, который описал создаваемый новый мир как мир, в котором «виртуальные и физические системы производства гибко взаимодействуют между собой на глобальном уровне»[3].

Действительно, искусственный интеллект, Интернет вещей, роботизация, виртуализация распространяются масштабно и внедряются во все сферы человеческой жизнедеятельности, преобразуя его природную, экономическую и гуманитарную среду обитания.

---

[1] Грейскоп А.А., Кузяшев А.Н. Актуальные вопросы цифровизации и информатизации // Экономика и бизнес: теория и практика. 2021. № 1–1 (71). С. 81–83.
[2] Там же
[3] Грейскоп А.А., Кузяшев А.Н. Актуальные вопросы цифровизации и информатизации // Экономика и бизнес: теория и практика. 2021. № 1 (71). С. 81–83.

Предполагается, что в недалеко будущем к объектам реального мира будут подсоединены более 20 млрд датчиков, что позволит создать цифровые двойники для миллиардов сущностей. В результате конкретные физические лица или технические объекты будут заменены их точными цифровыми отображениями, которые могут быть использованы для моделирования и прогнозирования поведения людей как в обыденных, так и в чрезвычайных ситуациях[1].

Цифровые платформы, использующие современную информационную инфраструктуру, способствуют распространению новых моделей взаимодействия производителей и потребителей, формированию «экономики по требованию». Подходы к организации бизнеса, применяемые такими компаниями, как Alibaba, Amazon, Uber, Яндекс, позволяют обеспечить совместный доступ к технике, технологическому оборудованию и ресурсам различных физических и юридических лиц, минуя многочисленные бюрократические формальности[2].

Все большое распространение получили краудфандинговые площадки, аккумулирующие денежные средства для различных стартапов и социальных проектов. Аналогичные процессы происходят сегодня и в Российской Федерации, в которой развитие информационного общества и формирование цифровой экономики провозглашены стратегическими целями на ближайшие десятилетия.

Их достижение предполагает обеспечение комплекса национальных интересов, среди которых повышение эффективности государственного управления и развитие свободного, устойчивого и безопасного

[1] Никитин Е.В. О новых возможностях применения современных цифровых технологий в правоохранительной деятельности // Правопорядок: история, теория, практика. 2018. №4 (19). URL: https://cyberleninka.ru/article/n/o-novyh-vozmozhnostyah-primeneniya-sovremennyh-tsifrovyh-tehnologiy-v-pravoohranitelnoy-deyatelnosti (дата обращения: 13.04.2021).

[2] Пыхтин И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) // Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48.

взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления.

Приказами МВД России от 29 декабря 2014 г. № 1144 и от 30 июня 2017 г. № 430 определен перечень из тридцати пяти государственных услуг, предоставляемых органами внутренних дел, создана система мониторинга их качества и утверждена форма статистической отчетности.

Критериями, в соответствии с которыми заявитель (физическое или юридическое лицо) формулирует свои выводы, выступают: время предоставления услуги; время ожидания в очереди; компетентность сотрудника; комфортность помещения, доступность информации о порядке предоставления государственных услуг.

На основе дальнейшего анализа определяется уровень удовлетворенности заявителя качеством предоставляемых услуг, значение которого в дальнейшем используется при оценке деятельности руководителей территориальных органов внутренних дел.

В органах прокуратуры в 2017 г. была утверждена Концепция цифровой трансформации органов и организаций прокуратуры Российской Федерации, которая ориентирована:

– на формирование и развитие цифровой среды органов прокуратуры с учетом потребностей граждан, бизнеса и государства в своевременном получении качественной информации на основе использования инфраструктуры электронного правительства и внедрения сервисной модели;

– на обеспечение согласованного развития цифровой экосистемы органов прокуратуры и других субъектов контрольно-надзорной деятельности системы государственного управления России.

Среди реализуемых в Генеральной прокуратуре Российской Федерации цифровых проектов нельзя не отметить федеральную государственную информационную систему «Единый реестр проверок», которая была разработана в 2015 г. для учета проверок, проводимых при осуществлении

государственного контроля (надзора), муниципального контроля, а также их результатов.

Основное предназначение федеральной государственной информационной системы «Единый реестр проверок» – повышение прозрачности деятельности органов, уполномоченных на осуществление государственного контроля (надзора) и муниципального контроля в отношении юридических лиц, индивидуальных предпринимателей; обеспечение свободного доступа к информации о плановых и внеплановых проверках, о результатах проверки, принятых мерах по итогам ее проведения, о выдаче предписания об устранении выявленных нарушений, его исполнении или неисполнении; обеспечение гласности в деятельности органов прокуратуры и органов, уполномоченных на осуществление государственного контроля (надзора), муниципального контроля, действующего законодательства на указанном участке работы; поддержка безусловного исполнения органами, уполномоченными на осуществление государственного контроля (надзора), муниципального контроля, действующего законодательства.

В условиях информационного общества существенно возрастает роль информационных правоотношений и таких субъективных прав, как право на информацию и право на доступ к информации.

Право на информацию закреплено ч. 4 ст. 29 Конституции Российской Федерации и раскрывается в конструкции: «...каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

Право на доступ к информации гарантировано ч. 2 ст. 24 Конституции Российской Федерации, в которой обозначено, что «органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

Правоохранительные органы, способствуя осуществлению вышеуказанных прав, выступают как субъекты информационных правоотношений, возникающих в процессе создания, распространения, использования, сохранения и уничтожения (утилизации) информации, а также в процессе предоставления информационных услуг и выполнения работ в информационной сфере, использования информационных технологий и ресурсов и обеспечения информационной безопасности.

При реализации права физических и юридических лиц на информацию от правоохранительных органов требуется занимать активную позицию по предоставлению сведений о своей деятельности в соответствии с принципом информационной открытости и гласности, кроме случаев, определенных законом (действующим законодательством)[1].

Соответствующие правовые нормы закреплены в следующих федеральных законах: от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации» (ст. 3)[2]; от 26 декабря 2008 г. № 294–ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (ч. 3 ст. 3); от 9 февраля 2009 г. № 8–ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (п. 1–2 ст. 4); (ч. 4 ст. 4); от 27 июля 2010 г. № 210–ФЗ «Об организации предоставления государственных и муниципальных услуг»; от 17 января 1992 г. № 2202–1 «О прокуратуре Российской Федерации» (абзац 2 ч. 2 ст. 4); от 28 декабря 2010 г. № 403–ФЗ «О Следственном комитете Российской Федерации» (п. 2 ч. 2 ст. 5); от 7 февраля 2011 г. № –ФЗ «О полиции» (ст. 8) и др.

---

[1] Пыхтин И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) // Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48.

[2] Федеральный закон от 27.07.2006 № 149–ФЗ (ред. от 09.03.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 20.03.2021) // Собрании законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448

Вместе с тем практика демонстрирует многочисленные факты несоблюдения контрольно-надзорными органами действующего законодательства, в частности положения о внесении в федеральном проекте «Цифровое государственное управление» в срок до 2024 г. актуальных сведений о плановых и внеплановых проверках, их результатах, выявленных нарушениях, сроках их устранения и привлеченных к ответственности виновных лиц.

В результате Федеральным законом от 26 июля 2017 г. № 206–ФЗ в ст. 19.6.1 Кодекса Российской Федерации об административных правонарушениях была включена часть 3, предусматривающая административную ответственность за нарушения законодательства о государственном контроле (надзоре) при размещении обязательной информации в федеральный проект «Цифровое государственное управление» в срок до 2024 г.

Данная ответственность наступает в случае невнесения должностными лицами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, уполномоченных на осуществление государственного контроля (надзора), органов местного самоуправления, уполномоченных на осуществление муниципального контроля, либо государственных или муниципальных учреждений, осуществляющих контрольные функции, требований законодательства о государственном контроле (надзоре), муниципальном контроле, информации о проверке в единый реестр проверок; нарушения два и более раза в течение одного года сроков внесения информации о проверке в единый реестр проверок; внесения два и более раза в течение одного года неполной или недостоверной информации о проверке в единый реестр проверок.

Рассмотрим судебную практику по данному вопросу.

«Судья Верховного Суда Российской Федерации Никифоров С.Б. установил, что Постановлением мирового судьи 2-го судебного участка Центрального района г. Калининграда от 14 марта 2019 г. заместитель

начальника отдела муниципального жилищного контроля и контроля в сфере благоустройства комитета городского хозяйства администрации городского округа «Город Калининград» Коровина И.А. признана виновной в совершении административного правонарушения, предусмотренного частью 3 статьи 19.6.1 Кодекса Российской Федерации об административных правонарушениях, и подвергнута административному наказанию в виде административного штрафа в размере 1 000 рублей».

В жалобе, поданной в Верховный Суд Российской Федерации, Коровина И.А. ставит вопрос об отмене постановления мирового судьи, ссылаясь на его незаконность.

«Суд установил, что в нарушение требований статьи 13.3 Федерального закона № 294-ФЗ, пунктов 13, 16, 18, 19, 20 Правил формирования и ведения единого реестра проверок в федеральную государственную информационную систему «Единый реестр проверок» не внесена информация о проверке, проведенной в отношении ТСЖ «Согласия 13». Статьей 2.4 КоАП установлено, что административной ответственности подлежит должностное лицо в случае совершения им административного правонарушения в связи с неисполнением либо ненадлежащим исполнением своих служебных обязанностей. Действия заместителя начальника отдела муниципального жилищного контроля и контроля в сфере благоустройства комитета городского хозяйства администрации городского округа "Город Калининград" Коровиной И.А. квалифицированы в соответствии с установленными обстоятельствами и нормами Кодекса Российской Федерации об административных правонарушениях. Порядок и срок давности привлечения к административной ответственности соблюдены. Административное наказание назначено в пределах санкции части 3 статьи 19.6.1 Кодекса Российской Федерации об административных правонарушениях».

Суд постановил решение мирового судьи оставить без изменений, а жалобу Коровиной И.А. - без удовлетворения[1].

«В Постановлении по делу об административном правонарушении № 5-289/2018 г., вынесенном мировым судьей судебного участка № 17 в Нововаршавском судебном районе Омской области в отношении Бабий Ю. В., старшего государственного инспектора безопасности дорожного движения ОГИБДД ОМВД России по Омской области, установлено, что последний не внес информацию о проверках проводимых в отношении юридических лиц в единый реестр проверок. Бабий Ю.В. вину не признал, пояснил, что его рабочее место не оборудовано выходом в Интернет, в связи с чем ему приходится разными способами искать компьютеры с выходом в Интернет, чтобы разместить информацию о проверках, за свой счет приобретал модем для работы. Суд не усмотрел в действиях Бабий Ю.В. какого-либо виновного поведения и постановил прекратить дело в связи с отсутствием состава административного правонарушения[2]».

«Решением № 12–314/2020 от 4 сентября 2020 г. по делу № 12–314/2020 Находкинского городского суда Приморского края вынесено постановление о прекращении производства по делу об административном правонарушении в отношении должностного лица – специалиста первого разряда ТО Управления Ропотребнадзора Г. Г. по ст. 19.6.1 ч. 3 КоАП Российской Федерации, в связи с малозначительностью[3]».

«Решением № 12–203/2020 от 13 июля 2020 г. по делу № 12–203/2020 Ленинского районного суда г. Н. Новгорода оставлено без изменений постановление мирового судьи судебного участка "номер" Ленинского судебного района г. Н. Новгорода от "дата" государственный жилищный

[1] Постановление Верховного Суда РФ от 19.12.2019 N 71–АД19–8 // Режим доступа: https://koapru.ru (дата обращений:11.04.2021)

[2] Постановление мирового судьи судебного участка № 17 Нововаршавского судебном района Омской области // Режим доступа: http://17.oms.msudrf.ru (дата обарщений:10.04.2021)

[3] Решение № 12–314/2020 от 4 сентября 2020 г. по делу № 12–314/2020 Находкинского городского суда Приморского края // Режим доступа: https://koapru.ru (дата обращений:10.04.2021)

инспектор Нижегородского заречного отдела государственной жилищной инспекции Нижегородской области Казанцев С. Д. привлечен к административной ответственности в виде административного штрафа в размере <данные изъяты> за совершение административного правонарушения, предусмотренного ч. 3 ст. 19.6.1 КоАП РФ[1]».

«Постановлением № 5–114/2020 от 12 мая 2020 г. по делу № 5–114/2020 Хасынского районного суда Магаданской области установлено, что начальником отдела муниципального контроля администрации Тенькинского городского округа Магаданской области Авраменко А.А. совершено административное правонарушение, предусмотренное ч. 3 ст. 19.6.1 Кодекса РФ об административных правонарушениях. Суд назначил ему административное наказание в виде предупреждения[2]».

Основным нормативным правовым документом, которым должны руководствоваться правоохранительные органы при реализации права на доступ к информации, является Федеральный закон от 27 июля 2006 г. № 152– «О персональных данных»[3] (далее – ФЗ № 152).

Согласно ч. 3 ст. 14 ФЗ № 152 правоохранительный орган (оператор персональных данных обязан предоставить физическому лицу или его представителю по требованию (обращению или запросу) имеющиеся о нем сведения, включающие, в том числе, подтверждение факта обработки персональных данных; правовые основания, цели, способы и сроки обработки, в том числе и сроки их хранения, и т. п.

Более того, оператор персональных данных обязан доказать получение согласия субъекта на обработку его персональных данных, а в случае

---

[1] Решение № 12–203/2020 от 13 июля 2020 г. по делу № 12–203/2020 Ленинского районного суда г. Н. Новгорода // Режим доступа: https://koapru.ru(дата обращения:10.04.2021)

[2] Постановление № 5–114/2020 от 12 мая 2020 г. по делу № 5–114/2020 Хасынского районного суда Магаданской области // Режим доступа: https://koapru.ru (дата обращения:10.04.2021)

[3] Федеральный закон от 27.07.2006 № 152–ФЗ (ред. от 30.12.2020) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2021) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

обработки общедоступных персональных данных на него возлагается обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными.

Весьма высокую тенденцию развития в Российской Федерации получило введение федеральной концепции для реализации государственной политики по обеспечению общественного порядка и общественной безопасности – автоматизированной системы видеонаблюдения, получившей название «Безопасный город».

Следует выделить, что введение данной системы создало необходимые условия для своевременного выявления, предупреждения и пресечения административных правонарушений в сфере общественного порядка и общественной безопасности, что оправдывает ее внедрение на федеральном уровне[1].

Первоначально создание и развитие аппаратно-программного комплекса «Безопасный город» (далее – АПК «Безопасный город») было совместно возложено на Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС России) и Федеральную службу охраны Российской Федерации (далее – ФСО России), где ключевая роль в реализации была возложена на МЧС России[2].

Рассматриваемый проект нельзя назвать окончательно удавшимся ввиду образования ряда внутриведомственных и межведомственных разногласий, а также нецелесообразной реализацией выделенного на федеральную концепцию государственного бюджета.

На текущий момент полномочия по координации данного проекта от указанных федеральных ведомств по инициативе главы МЧС России Евгения

---

[1] Ансель М. Методологические проблемы сравнительного права (фрагменты) / М. Ансель // Вестник Университета имени О.Е. Кутафина. 2015. № 5. С. 187–188.

[2] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

Зиничева должны быть переданы в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России)[1].

Сама по себе идея федеральной концепции является более чем оправдывающей себя.

На текущий момент к АПК «Безопасный город» подключено множество федеральных ведомств, в чью компетенцию входит обеспечение общественного порядка и общественной безопасности, в т. ч. и МВД России.

Таким образом, соответствующие наружные подразделения МВД России имеют круглосуточный доступ к АПК «Безопасный город» и в режиме реального времени имеют возможность для своевременного выявления, предупреждения и пресечения преступлений и административных правонарушений без участия лиц-заявителей о тех или иных противоправных действий.

Данные, полученные от системы, учитываются при расстановке постов, определении маршрутов патрулей.

Аппаратно-программный комплекс включает в себя две системы: видеонаблюдение за территорией города и мониторинг автомобилей нарядов.

Комплекс позволяет отслеживать движение экипажей и менять маршруты их патрулирования в зависимости от криминогенной обстановки и внезапно возникающих задач[2].

Основной проблемой функционала АПК «Безопасный город» является не повсеместный территориальный охват, а также низкое качество видеосъемки в некоторых участках.

Исходя из изложенного, мы можем сделать вывод, что в большей степени организация и осуществление административной деятельности в

---

[1] «МЧС съезжает из «Безопасного города» // Официальный сайт ежедневной газеты «Коммерсантъ-Daily». – Режим доступа: https://www.kommersant.ru/doc/4636274. Загл. с экрана. (дата обращения: 03.04.2021)

[2] Морозов В.А. Подготовка сотрудников полиции к выполнению профессиональных задач в системе «Безопасный город» / В.А. Морозов // Мир науки, культуры, образования. 2021. № 1 (86). С. 65.

области общественного порядка и общественной безопасности подразделениями ППСП обеспечивается благодаря межведомственному взаимодействию, в данном случае нами было рассмотрено взаимодействие с органом исполнительной власти Российской Федерации, ответственным за координацию АПК «Безопасный город».

Также в качестве одной из проблем следует выделить важность профессиональной компетенции сотрудников наружных служб органов внутренних дел.

Данный аспект, вне всякого сомнения, влияет на качество сбора материалов по делу об административном правонарушении ввиду того, что сотрудник полиции обязан при исполнении своих служебных обязанностей четко и структурированно оформлять необходимые для административного дела документы, пресекать ненадлежащее исполнение обязанностей иными лицами, чьи действия могут непосредственно влиять в негативном ключе на законность и обоснованность материалов дела об административном правонарушении.

В судебной практике имеется множество примеров ненадлежащего сбора материалов, что впоследствии приводило к прекращению производства по делу об административном правонарушении или отмене решений мировых судей.

В качестве примера можно выделить решение Златоустовского городского суда Челябинской области по делу № 12–55/2017 от 16.02.2017 на определение об отказе в возбуждении дела об административном правонарушении в отношении неустановленного лица по ч.1 ст.20.1 Кодекса Российской Федерации об административных правонарушениях, вынесенное 18 января 2017 г. участковым уполномоченным ОП «Новозлатоустовский» ОМВД РФ по ЗГО Челябинской области1, согласно которому жалоба истца

[1] Решение Златоустовского городского суда Челябинской области по делу № 12–55/2017 от 16 февраля 2017 года по жалобе на определение об отказе в возбуждении дела об административном правонарушении // Информационная система ГАС «Правосудие». 2021.(дата обращения:11.04.2021)

была удовлетворена в связи с отсутствием всестороннего, полного, объективного выяснения всех обстоятельств дела уполномоченным на то лицом.

В данном случае нельзя исключать, что нарушение связано с ненадлежащим исполнением должностных обязанностей сотрудниками медицинского учреждения, осуществлявшего освидетельствование, но, тем не менее, данный факт говорит о том, что порядок проведения процедуры и форму документов необходимо знать и сотрудникам полиции, осуществляющим сбор материалов по делу об административном правонарушении.

1. Развитие отечественного уголовного законодательства в сфере защиты компьютерной информации имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века.

В настоящее время преступные деяния в сфере компьютерной и цифровой информации, позволяет их классифицировать на:

1) преступления, квалифицируемые по статьям, входящим в главу 28 УК РФ;

2) иные преступные деяния, которые совершаются с использованием механизмов и возможностей информационно-телекоммуникационных сетей, в том числе Интернета.

Предметам исследования данной работы являются преступные деяния, предусмотренные в нормах главы 28 УК РФ.

2. Под преступлениями в сфере компьютерной информации следует понимать совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Действующее законодательство предусматривает уголовную ответственность за совершению компьютерных преступлений.

Компьютерные преступления наносят вред законным интересам непосредственно собственникам или владельцам информации, могут причинять вред жизни и здоровью личности, наносят вред правам и законным интересам человека и гражданина, а также государственной или общественной безопасности.

Так же, происходящие в современном мире процессы повышают уровень угроз информационной безопасности, обеспечения конфиденциальности, целостности и доступности информации. Необходимо отметить, что на сегодняшний день компьютерная преступность становится одним из наиболее общественно опасных видов преступных посягательств, что обусловливает актуальность темы исследования[1].

Развитие института ответственности за компьютерные преступления имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века. Несмотря на вносимые в УК РФ дополнения, кардинального изменения уголовного законодательства не происходит, по-прежнему законодательство «отстаёт» от развития технологии информационных систем и от развития отношений в кибепространстве. Преступления, совершаемые в области компьютерной информации и в киберпространстве, представляют собой достаточно распространенное противозаконное явление, при этом, число данных деяний в ближайшем будущем будет увеличиваться. Такая тенденция обусловлена активным развитием компьютерных технологий и программного обеспечения, что предопределяет необходимость разработки рекомендаций по правильной квалификации деяний, совершаемых в сфере компьютерной информации.

По убеждению Д.В. Добровольского факт наличия преступлений в

[1] Григорьев О.В. Правовые реформы - ответ на вызов социальных деструкций // Административное и муниципальное право. 2018. № 8 С. 12–14

сфере компьютерной информации можно представить как определенный способ регулирования, методов управления в целях уменьшения причиняемого вреда, категория оцениваемая с точки зрения государства как негативное явление современной действительности и обладающее основными признаками профессиональной преступности, а в правовой области представляющее собой обширное, массовое виновное нарушение уголовных норм, совокупность всех фактически деяний совершенных вменяемыми физическими лицами, достигшими возраста шестнадцати лет, преступлений в области информационных технологий[1].

Согласно ныне действующему уголовному законодательству компьютерные преступления представляют собой преступные деяния, которые совершаются в области информационных процессов, в связи с чем посягают на сферу информационной безопасности, в качестве предмета которых выступает информация, а также компьютерные средства[2]. Ежегодно осуждается более ста человек за совершение преступлений, квалифицируемых по статьям главы 28 УК РФ, только в 2019 году было осуждено 165 лиц[3] (см. приложение). Отметим, что по ст. 274 УК РФ не вынесено ни одного приговора. В действительности подобные общественно опасные деяния встречаются довольно часто и то, что действия виновных не охватываются нормами об уголовной ответственности за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, свидетельствует о наличии проблемы в правоприменении ст. 274 УК РФ, требующей правового решения. По ст. 274.1 УК РФ вынесено только четыре обвинительных приговора в 2019 году. Данное обстоятельство, как представляется связано с тем, что только в 2017 году ст. 274.1 УК РФ была введена в УК РФ.

---

[1] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: Уголовно-правовые и криминологические проблемы: автореферат дис. ... канд. юрид. наук. М., 2006. С. 8.

[2] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

[3] Судебный департамент при Верховном Суде Российской Федерации. Режим доступа: http://www.cdep.ru (дата обращения: 05.12.2020).

В данном случае показателен следующий пример из судебной практики:

Уголовное дело № 1-55/2016 возбуждено 11 марта 2016 года в г. Новокуйбышевске. Из обвинительного заключения следует, что Тимофеев, работавший в ОАО “ВымпелКом” с 28.02.2014, в период времени с 03.05.2014 года по 07.06.2014 года осуществлял неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ОАО «ВымпелКом» и их лицевых счетов, путём отключения запрета на услугу «Мобильная коммерция», установленной компетентной службой ОАО «ВымпелКом», повлекшие модификацию компьютерной информации, которая была в распоряжении собственника и законного пользователя, из корыстной заинтересованности, у Тимофеева появилась возможность пользоваться лицевыми счетами более 50 абонентских номеров.

Неправомерный доступ Тимофеев осуществлял находясь на своём рабочем месте, в офисе продаж и обслуживания ОАО «ВымпелКом», расположенном в ТЦ «Сити-Парк» по адресу: г.Новокуйбышевск, пр. Победы, д. 1 «ж» ТЦ «Сити-Парк», используя своё служебное положение, под своими индивидуальными логином «ACTrofimov» и паролем, который является конфиденциальным осуществил доступ в компьютерную программу АБС «Ensemble», которая используется сотрудниками ОАО «ВымпелКом». После чего, Тимофеев, действуя умышленно, совершил неправомерный доступ в модуль «CSM», который используется для внесения изменений в список услуг и проведения абонентских операций с номерами клиентов, где не имея соответствующего заявления клиента, с целью последующего завладения денежными средствами, находящимися на лицевых счетах абонентов ОАО «ВымпелКом», выбрал абонентский номер для проведения модификации ICCID номера сим-карты, путём внесения изменений в программу АБС «Ensemble», содержащую сведения об индивидуальных

ICCID номерах сим-карт абонентов ОАО «ВымпелКом», в результате чего у него появилась возможность распоряжаться лицевым счётом абонента.

Преступные действия подсудимого Тимофеева правильно квалифицированы по ч. 3 ст. 272 УК РФ — неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, совершенное лицом с использованием своего служебного положения[1].

Обратим внимание на мнение К.А. Шмалевой, согласно которому к компьютерным преступлениям также могут относиться: преступления, которые затрагивают область компьютерной информации, а также общеуголовные преступные деяния, которые совершаются с использованием механизмов и возможностей компьютерных технологий; сетевые компьютерные преступления и, наконец, трансграничные киберпреступления[2]. Учитывая фактор задействования в механизме совершения преступного деяния сети Интернет, И.Д. Смирнов совершенно справедливо выделяет среди преступлений в области компьютерной и цифровой информации, которые совершаются:

– внутри локальной сети;

– с использованием глобальной, общедоступной Интернет-сети[3].

Систематизацию преступлений в сфере компьютерной информации можно осуществлять по различным основаниям, и любая систематизация будет в дальнейшем совершенствоваться ввиду того, что уголовный закон постоянно претерпевает изменения, посвященные использованию информационно-телекоммуникационных технологий при совершении

---

[1] Приговор № 1-55/2016 от 25 марта 2016 г. по делу № 1-55/2016 // Режим доступа: novokuibyshevsky.sam.sudrf.ru/ (дата обращения: 03.04.2021 г.)

[2] Шмалева К.А. Преступления в сфере компьютерной информации // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей. Пенза: Наука и Просвещение, 2020. С. 109.

[3] Смирнов И.Д. Уголовно-правовое противодействие преступлениям, затрагивающим сферу компьютерной информации, совершенным с использованием сети Интернет // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник трудов конференции. Воронеж: Изд-во Воронежского института МВД РФ, 2017. С. 142.

различного рода общественных посягательств. Государство признает рост количества преступлений, совершенных с применением информационно-телекоммуникационных технологий, в результате чего наблюдается активное совершенствование уголовно-правовых норм в данной области путем добавления норм, предусматривающих ответственность за совершение преступного деяния с использованием цифровой информации, передаваемой по информационно-телекоммуникационным сетям, включая Интернет-каналы.

Представляется необходимым глубокий анализ всех статьей Особенной части УК РФ с целью выявление тех составов, в которых назрела насущная потребность в дополнении их таким квалифицирующим признаком, как использование для совершения преступления компьютерных технологий и информационных ресурсов.

В результате вышеизложенного представляется возможным преступления в сфере компьютерной информации определить в качестве совершаемых в сфере информационных процессов и посягающих на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Рассмотрим состав преступления. Общим объектом компьютерных преступлений являются общественные отношения в области гарантированности информационной безопасности[1]. Непосредственными объектами преступного деяния могут рассматриваться базы и банки определенных компьютерных систем или сетей, в том числе их отдельные файловые составляющие. В качестве непосредственного объекта в компьютерной сфере выступают, и компьютерные технологии, и программное обеспечение, включая множество средств защиты компьютерной и киберинформации.

[1] Самигуллина З.Ф. К вопросу о рассмотрении понятия «информация» как объект уголовно-правовой защиты // Аллея науки. 2019. № 2. С. 631.

Имеет место точка зрения, в рамках которой местом совершения преступного деяния следует считать непосредственное место нахождения компьютерного оборудования, являющегося средством совершения преступного акта. Вместе с тем, данный подход не позволяет учитывать случаи размещения серверов в различных государствах.

Исходя из изложенного можно констатировать, что интернет-преступления весьма часто являются транснациональными преступлениями, а порядок привлечения и степень уголовного наказания за совершение указанных деяний необходимо урегулировать международно-правовыми актами.

В настоящее время нет международных договоров, в которых бы были определены меры борьбы государств с глобальными компьютерными преступлениями отсутствуют совместные правила об уголовной ответственности за совершение таких деяний.

Следует отметить, что анализ отдельных действующих в настоящее время многосторонних договоров позволяет говорить о том, что использование компьютерной техники и Интернет-ресурсов приводит к факту совершения не только некоторые преступных деяний международного характера, но и к совершению международных преступлений.

В связи с этим считаем актуальным необходимость пересмотра международных договоров, которые содержат комплекс мер борьбы с преступными деяниями против безопасности воздухоплавания, а также морского судоходства, для того чтобы была фактическая возможность пресечения в вышеуказанной области незаконного использования компьютерных систем и технологий.

Проблематика уголовного преследования за совершение преступлений в сфере компьютерной безопасности является актуальной как для Российской Федерации, так и для зарубежных стран. В качестве общего, совпадающего для всех стран является установление уголовной ответственности за преступления в сфере компьютерной информации, исходя из понимания той

угрозы, которая от них исходит и как оценивается эта угроза в конкретном государстве[1].

Данное обстоятельство является одной из причин того, что в уголовном законодательстве разных стран перечень компьютерных преступлений достаточно отличается между собой. Вместе с тем, исследователи отмечают тенденцию к унификации, к выработке единой позиции по перечню компьютерных преступлений.

Может и согласования по данному вопросу и не происходят, но реальная практика, реально совершаемые деяния приводят к тому, что в разных государствах постепенно вырабатывается такой перечень компьютерных преступлений, который характерен и для иных государств. Кроме того, многие компьютерные преступления имеют трансграничный характер, что приводит к необходимости установления ответственности за совершение такого деяния в сопряженных странах.

Рассматривая зарубежный опыт регулирования ответственности за компьютерные преступления, следует обратить внимание на приоритеты тех или иных государств.

Для отдельных государств (США, многие страны Евросоюза) характерно установление повышенного уровня уголовного наказания в отношении деяний, посягающих на работоспособность государственных компьютерных устройств, на информацию, содержащуюся в таких устройствах, а, значит, в отношении деяния, посягающих на национальную безопасность[2]. Если обратиться к анализу уголовного законодательства стран ближнего зарубежья, то следует отметить, что в данных странах также активно осуществляется борьба с компьютерной преступностью уголовно-правовыми методами.

---

[1] Шульга А.В., Ширинян А.В. Преступления в сфере компьютерной информации в зарубежных странах // Верховенство права и правовое государство: сборник трудов конференции. Уфа: Аэтерна, 2020. С. 47.

[2]Лукьянов Н.Е. Законодательное регулирование ответственности за информационные преступления. Зарубежный опыт // Устойчивое развитие науки и образования. 2019. № 2. С. 136.

В УК Республики Беларусь[1] преступления против информационной безопасности сконцентрированы в главе 31. В УК Республики Азербайджан[2] имеет отдельная глава 30, именуемая «Киберпреступления». Опыт Азербайджана и Беларуси представляется прогрессивным, в той части, что объединение компьютерных преступлений в одной главе уголовного кодекса, т.е. их систематизация, позволяет в дальнейшем, без ущерба для общей системы особенной части УК, включать новые статьи в области киберпреступности, что неизбежно в будущем ввиду активного развития и динамики киберпреступности как в мире, так и в отдельно взятой стране.

Таким образом, борьба с современной компьютерной преступностью непосредственно связана как с возможностью использования традиционных средств, используемых международными странами.

Отсюда, следует сделать вывод по главе. Развитие института ответственности за компьютерные преступления имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века.

Несмотря на вносимые в УК РФ дополнения, кардинального изменения уголовного законодательства не происходит, по-прежнему законодательство «отстаёт» от развития технологии информационных систем и от развития отношений в кибепространстве. Преступления, совершаемые в области компьютерной информации и в киберпространстве, представляют собой достаточно распространенное противозаконное явление, при этом, число данных деяний в ближайшем будущем будет увеличиваться.

---

[1] Уголовный кодекс Республики Беларусь (принят Палатой представителей 2 июня 1999 г., с
изм. От 17 июля 2018 г.) Режим доступа: http://www.pravo.by/document/?guid=3871&p0=Hk 9900275 (дата обращения: 09.12.2020).

[2] Уголовный кодекс Азербайджанской республики. СПб.: Юридический центр Пресс, 2001. С.325.

Такая тенденция обусловлена активным развитием компьютерных технологий и программного обеспечения, что предопределяет необходимость разработки рекомендаций по правильной квалификации деяний, совершаемых в сфере компьютерной информации.

Несомненно, можно сказать, что в случае выявления этих преступлений, можно сказать, что большую роль играет объект и субъект этого вмешательства. В эпоху цифровых технологий проблема уголовного преследования преступлений, совершенных в информационном секторе, является наиболее острой.

При выявлении, раскрытии и расследовании преступлений в сфере компьютерной информации применяется комплекс оперативно-розыскных и следственных мероприятий. Особую сложность представляет процедура обнаружения, фиксации и изъятия компьютерной информации.

Что касается обнаружения следов данных в одном ряду с традиционными поисковыми мерами и специальными для этой категории преступлений, то « это комплекс действий по перехвату и расследованию трафика, установлению протоколов веб – и почтовых серверов, системных протоколов, доменов, принадлежностей адресов электронной почты, исследований кейлоггеров.»

Значительное место в деятельности по выявлению, раскрытию и расследованию данной категории преступлений занимает производство судебно-медицинских экспертиз, а именно судебно-вычислительно-технических, где проводится анализ «цифровых следов».

Одной из социальных проблем в современном российском обществе является возникновение и активное развитие компьютерной преступности, причиняющей колоссальный вред экономической, политической, культурной, научной, образовательной и информационной сферам Российской Федерации.

Все более актуальным становится вопрос о защите граждан, муниципальных и государственных учреждений, предприятий, органов

власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

В настоящее время профилактика компьютерных преступлений является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества.

Общепревентивные меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом. Достаточно ясно и лаконично, на наш взгляд, они сформулированы в указе Президента РФ «О Стратегии национальной безопасности Российской Федерации до 2020 года» № 537.

Например, к общеполитическим мерам предупреждения преступлений в сфере компьютерной информации в России можно отнести: развитие демократии и гражданского общества, обеспечение незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации; превращение Российской Федерации в мировую державу, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях многополярного мира.

Общеэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда и др.

Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе — коренное улучшение демографической ситуации; обеспечение личной безопасности, а

также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности и т.д.

К научно-техническим общепревентивным мерам относятся: формирование системы целевых фундаментальных и прикладных исследований и ее государственной поддержки в интересах организационно-научного обеспечения достижения стратегических национальных приоритетов; создание сети федеральных университетов, национальных исследовательских университетов, обеспечивающих в рамках кооперационных связей подготовку специалистов для работы в сфере науки и образования, разработки конкурентоспособных технологий и образцов наукоемкой продукции, организации наукоемкого производства и др.

Духовно-культурные меры общей превенции включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России.

Однако представляется необходимым остановиться именно на специальных мерах предупреждения компьютерной преступности.

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства, то есть решить проблемы квалификации преступлений в сфере компьютерной информации, которые обозначены в подразделе 1 данной главы. Кроме того, совершенствование судебной практики требует разъяснений Пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных ст. 272-274.1 УК РФ.

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации. До сих пор

отсутствуют разъяснения Пленума Верховного Суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними. Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

Так, 11 ноября 2013 г. Тушинским районным судом г. Москвы за совершение преступлений, предусмотренных ч. 3 ст. 30, п. «б» ч. 4 ст. 158, ч. 3 ст. 272 УК РФ, граждане Республики Молдова Б. и А. были осуждены к наказанию в виде двух лет шести месяцев лишения свободы без штрафа и без ограничения свободы с отбыванием наказания в исправительной колонии общего режима каждый. Преступная группа, состоявшая из граждан Республики Молдова, длительное время занималась скимингом в Москве, осуществляя хищение денежных средств с банковских карт физических лиц с помощью специального оборудования, устанавливаемого на картоприемник банкомата.

Несколько участников преступной группы скрылись от следствия и суда за пределами Российской Федерации[1].

Общепризнанным является вывод о том, что, для того чтобы быть эффективной, профилактика любого, в том числе и компьютерного, преступления должна носить комплексный системный характер. А применяемые на практике методы и мероприятия по обеспечению информационной безопасности объектов должны быть тесно связаны друг с другом.

[1] Уголовное дело № 1-520/2013 // Архив Тушинского районного суда г. Москвы. 2014

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Подготовка специалистов по специальностям «Информационная безопасность», «Защита информации и информационно-телекоммуникационных сетей» в высших учебных заведениях МВД, ФСБ, и др. с целью дальнейшего комплектования правоохранительных органов профессиональными и компетентными сотрудниками.

При этом следует также осуществлять повышение квалификации и профессорско-преподавательского состава вышеуказанных вузов, включая проведение стажировок, обмена опытом, мастер-классов, семинаров в соответствующих образовательных учреждениях за рубежом, а также в российских и иностранных компаниях, занимающихся информационной безопасностью, защитой информации, разработкой антивирусного программного обеспечения и т.п.

2. Создание в технических вузах, а также в НИИ МВД, ФСБ и др. научно-исследовательских лабораторий по разработке и модификации программных систем компьютерной защиты с правом реализации (продажи) своей продукции заинтересованным физическим и юридическим лицам. Работа в лабораториях должна проводиться как в научных, так и в коммерческих целях на договорной основе, в том числе для государственных и муниципальных нужд.

3. При технических образовательных учреждениях, специализирующихся на подготовке специалистов по информационной безопасности, следует создать курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений либо заинтересованных компьютерных пользователей.

4. Требуется тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации.

Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы и активно используются.

5. Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников (разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», Dr. Web, Group-IB).

К криминалистическим мерам предупреждения преступлений в сфере компьютерной ин формации можно отнести:

1. Создание новых и существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности (например, вышеуказанных специалистов компаний «Лаборатория Касперского», Dr. Web, Group-IB).

2. Обобщение и анализ юридической практики Прокуратурой РФ, СК РФ, МВД РФ, ФСБ РФ для дальнейшей выработки методических рекомендаций по вопросам раскрытия и расследования компьютерных преступлений[1].

3. Создание во всех экспертно-криминалистических центрах МВД, ГУВД, ОВД отделов компьютерных экспертиз и технологий для производства необходимых судебно-компьютерных экспертиз, выдачи заключений и справок заинтересованным лицам.

4. Совершенствование подготовки экспертов-криминалистов, осуществляющих судебно-компьютерные экспертизы, на базе единого учебного центра.

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. генер. прокурором РФ. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817 (дата обращения: 25.04.2021)

В заключении данного параграфа, следует сделать вывод, что перечень мер по предупреждению компьютерной преступности может быть продолжен.

Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным.

При этом не стоит забывать, что предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

Оптимизация уголовно-правовых норм, предусматривающих ответственность за компьютерные преступления, представляется необходимым начать с совершенствованием терминологического аппарата.

Для конкретизации общественно опасных деяний в области компьютерной информации, а также для обеспечения стабильности понятийно-терминологического аппарата считаем целесообразным использовать понятие не «преступления в сфере компьютерной информации», а прибегать к употреблению понятия «преступления в сфере информационных технологий», что поддерживается рядом ученых.

Данные преступления наносят вред законным интересам непосредственно собственникам или владельцам информации, могут причинять вред жизни и здоровью личности.

Также необходимо изменить название всей главы 28 УК РФ, сформулировав ее как «Преступления в сфере информационных технологий», так как данная корректировка даст возможность законодателю своевременно реагировать на криминализацию новых общественно-опасных деяний, а также позволит точно и своевременно включать новые нормы в УК РФ в связи с появлением новейших видов преступлений в области

компьютерной информации, даст возможность своевременно дополнять главу 28 УК РФ новыми составами.

3. Для конкретизации рассмотренных в данной работе общественно опасных деяний и обеспечения стабильности понятийно-терминологического аппарата считаем целесообразным вместо термина «преступления в сфере компьютерной информации» использовать термин «преступления в сфере информационных технологий»,

Наряду с этим необходимо изменить название всей главы 28 УК РФ, сформулировав ее как «Преступления в сфере информационных технологий», так как данная корректировка даст возможность законодателю своевременно реагировать на криминализацию новых общественно-опасных деяний, а также позволит точно и своевременно включать новые нормы в УК РФ в связи с появлением новейших видов преступлений в области компьютерной информации, даст возможность своевременно дополнять главу 28 УК РФ новыми составами.

4. Общим объектом компьютерных преступлений являются общественные отношения в области гарантированности информационной безопасности.

Непосредственными объектами преступного деяния могут рассматриваться базы и банки определенных компьютерных систем или сетей, в том числе их отдельные файловые составляющие, а также критическая информационная инфраструктура государства.

В качестве непосредственного объекта в компьютерной сфере выступают и компьютерные технологии, и программное обеспечение, включая множество средств защиты компьютерной и киберинформации.

5. Считаем целесообразным дополнить ст. 272 УК РФ указанием на киберинформацию. В частности, название ст. 272 УК РФ сформулировать следующим образом: «Неправомерный доступ к компьютерной и киберинформации». Такое изменение обосновывается различием в предмете преступного посягательства.

Киберинформация, в отличие от компьютерной информации, находящейся на жестком диске компьютера или на ином носителе (например, флэш-карте), поступает в компьютерное устройство через присоединенную или удаленную сеть.

6. Субъектами компьютерных преступлений являются вменяемые лица, достигшие 16-летнего возраста, в отдельных случаях - субъект специальный (например, ч. 3 ст. 272, ст. 274, ч. 3, 4 ст. 274.1 УК РФ).

7. Компьютерные преступления совершаются только умышленно: с прямым или косвенным умыслом.

Считаем необходимым повысить степень наказания за неправомерный доступ к компьютерной информации, совершенный с целью скрыть другое преступление или облегчить его совершение.

Также, ввиду большей общественной опасности преступлений, приводящих к разжиганию какой-либо ненависти и вражды, необходимо ч. 2 ст. 273 УК РФ дополнить следующим положением: «то же деяние, если оно повлекло модификацию компьютерной информации и было совершено по мотивам политической, идеологической, расовой, национальной или религиозной ненависти, или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы».

8. Интернет используется для совершения множества преступлений, в том числе в целях разжигания межнациональной и религиозной ненависти, однако, это обстоятельство остается без надлежащей оценки со стороны правоприменителей, поскольку диспозициями соответствующих статей УК РФ не предусмотрено квалифицирующего признака «с использованием информационно-телекоммуникационных сетей».

Представляется необходимым глубокий анализ всех статьей Особенной части УК РФ с целью выявления тех составов, в которых назрела насущная потребность в дополнении их таким квалифицирующим признаком, как использование компьютерных технологий и информационных ресурсов для совершения преступления.

В результате существенных недостатков при составлении протокола по ст. 20.21 КоАП мировым судьей судебного участка № 1 г. Еманжелинска Челябинской области были возвращены материалы дела об административном правонарушении по делу № 3–59/2016 от 29.01.2016[1].

Отсюда, мы можем сделать вывод, что весьма существенным является повышение уровня компетенции сотрудников органов внутренних дел в сфере применения норм административного законодательства.

В данном аспекте мы предлагаем введение ведомственного приказа, направленного на обеспечение штабными и кадровыми подразделениями территориальных отделов органов внутренних дел лекционных занятий по разъяснению применения административного законодательства в области общественного порядка и общественной безопасности среди сотрудников наружных служб с их последующей аттестацией[2].

Таким образом, информационные технологии широко используются в деятельности правоохранительных органов. Однако в настоящее время они требуют совершенствования, которое позволит вывести правоохранительную деятельность на качественно новый уровень.

2.2 Зарубежная практика использования информационных технологий в правовом обеспечении национальной безопасности страны

Общемировые затраты правоохранительных органов на программные средства и системы достигли по итогам 2019 года $11,6 млрд[3]. Ежегодный

[1] Определение о передаче дела об административном правонарушении по делу № 3–59/2016 от 29 января 2016 года мирового судьи судебного участка № 1 г. Еманжелинска Челябинской области // Информационная система ГАС «Правосудие». 2021.(дата обюращения:25.03.2021)

[22] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

[3] Официальный интернет-сайт МВД России // Режим доступа: https://мвд.рф (дата обращений:11.04.2021)

среднегодовой темп роста рынка составит 9,3% и к 2023 году достигнет $18,1 млрд.

Рассмотрим современные технологии, используемые российскими и зарубежными правоохранительными органами[1].

1. Дроны.

Впервые дроны в МВД России начали использовать в 2010-х годах. Например, летом 2016 года сотрудники Госавтоинспекции Хабаровского края использовали беспилотные летательные аппараты для патрулирования трассы Хабаровск–Владивосток.

Летом по этой магистрали к местам отдыха направляются туристы. Информация с дронов онлайн передавалась на бортовые компьютеры патрульных автомобилей. Радиус обзора с высоты 1,8 км превышал несколько километров. При этом отчетливо видны двойные сплошные линии, марки и цвета автомобилей. В первый день дроны помогли выявить 11 нарушителей ПДД, пересекших двойную сплошную.

За рубежом данный метод борьбы с преступностью распространён в более широком спектре возможностей. Так, например, в США дронов оснащают камерами распознавания лиц. Они необходимы для определения личности преступника. Записи основных его черт с помощью видеофиксации и одновременную проверку по базам данных. Такой подход упрощает деятельность сотрудников т.к. становится сразу понятно находится ли человек в розыске, состоит ли он в преступной группировке, что позволяет решить какие действия предпринимать дальше.

2. Большие данные.

Технологии работы с большими данными используются внутренними органами РФ для мониторинга социальных процессов общества, прогнозирования и предупреждения преступлений.

[1] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

В октябре 2018 года Сергей Собянин сообщил, что свыше 70% преступлений в Москве раскрывается с помощью систем видеонаблюдения. В столице России задействовано более 150 тыс. камер, а данные с них собираются в «Едином центре хранения и обработки данных». Столичный градоначальник рассказал об использовании больших данных структурами МВД, ЖКХ, административных инспекций.

Городские камеры подключены к единой видеоплатформе. Доступ к ней есть у правоохранительных органов и других контролирующих служб. Запись с камер видеонаблюдения можно использовать в качестве значимых материалов для суда. Чаще всего горожане резервируют видео, чтобы определить, кто виноват в дорожно-транспортном происшествии, или доказать факт порчи имущества или кражи. Также граждане обращаются за видеозаписями в случаях хулиганских действий по отношению к ним, наезда машины или по фактам вандализма в многоквартирных домах.

В данном случае можно обратиться к опыту Великобритании, где для упрощения контроля за большими пакетами данных используется система анализа искусственного интеллекта. ИИ анализирует данные полученные с камер видеонаблюдения и путём покадрового разбора выбирает на каких частях записи присутствует что-то подозрительное, а какие можно удалить и не отправлять на облачный сервер. Это позволяет сэкономить место под хранение необходимой информации.

3. Искусственный интеллект.

МВД России ведет активную работу по разработке специального программного обеспечения, которое в автоматическом режиме будет искать пробелы и противоречия в законах, фактически выполняя функции юристов.

Целью данной работы является не замена юристов на искусственный интеллект, а создание для них современного инструмента, который позволит повысить производительность труда сотрудников органов внутренних дел при подготовке и согласовании проектов правовых актов, а также снизить

трудозатраты юристов при проведении правовой и антикоррупционной экспертиз.

Основные проблемы, с которыми сталкиваются правоохранительное органы при применении информационных технологий, проявляются:[1]

– в отсутствии своевременности, регулярности и полноты сбора определенных данных;

– в недостаточной аналитической обработке информации;

– в оставлении без должного внимания требований комплексности, объективности, верификации, что отрицательно сказывается на принятии необходимых управленческих решений;

– в нерациональном использовании информации, сосредоточенной в соответствующих банках данных.

Для решения этих проблем необходимо в кратчайшие сроки разработать и постоянно обновлять передовую законодательную базу для разработки и широкого применения робототехники, искусственного интеллекта, беспилотного транспорта. Такое законодательство уже приято в ряде стран, в их числе: Япония, Китай, Сингапур, Южная Корея, США, Германия, Франция, Италия и др.

Исходя из всего вышесказанного предлагаю разработать законопроект, который будет отвечать за формирование собственных цифровых платформ.

Естественно, совместимые с глобальным информационным пространством. Это позволит по-новому организовать производственные процессы, финансовые услуги и логистику, в том числе с использованием технологий распределенного реестра, что очень важно для финансовых трансакций, для учета прав собственности и так далее. Это имеет практическое измерение.

[1] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

Основным новшеством законодательства является федеральный проект «Цифровое государственное управление» в срок до 2024 г., который предусматривает пути решения вышеобозначенных проблем в деятельности правоохранительных органов:[1]

– для органов прокуратуры – обеспечение функционирования для всех сотрудников современных автоматизированных рабочих мест и сервисов работы с цифровыми данными на базе защищенной катастрофоустойчивой инфраструктуры Генеральной прокуратуры Российской Федерации;

– для МЧС России – обеспечение высокого качества предоставления государственных и муниципальных услуг (функций), иных услуг (сервисов) и сведений в электронном виде в сфере пожарной безопасности и безопасности людей на водных объектах;

– для МВД России – создание единого информационного ресурса регистрационного и миграционного учета;

– для Росгвардии – создание системы контроля оборота огнестрельного оружия и управления охранными услугами на базе отечественных технологий для обработки больших массивов данных.

Таким образом, что с внедрением концепции «сервисного государства» и менеджериального подхода в сферу публичного управления, в частности в правоохранительную деятельность, актуальность властного начала, обязывающе-запретительных методов будет со временем уменьшаться.

Действительно, с развитием средств инфо-телекоммуникаций, появлением «электронных паспортов», повсеместного внедрения технологий «безопасного города», прогнозируемого чипирования населения, в результате которого будет «обеспечена постоянная связь каждого индивидуума с глобальными информационно-управляющими сетями», задачи

[1] Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.

предупреждения и пресечения правонарушений и проступков, розыска преступников будут решаться более оперативно[1].

Наглядным подтверждением данному тезису может служить успешность выявления фактов нарушения гражданами режима самоизоляции в период пандемии, связанной с вирусом COVID-19, обеспеченная введением цифровых пропусков и внедрением в Москве приложения «Социальный мониторинг».

Вывод: современные реалии требуют от правоохранительных органов смещение акцентов в сторону способствования реализации прав физических и юридических лиц в сфере информационно-цифровых технологий. Помимо этого стоит обратить внимание на практику использования таких технологий другими странами. Стоит изменить законодательство в сфере использования информационно-цифровых технологий сотрудниками органов внутренних дел на всех уровнях, начиная от контроля за объёмами данных и заканчивая использованием прототипов новых технологий слежения, аудио- и видеофиксации. Это упростит работу и позволит разгрузить кадровый состав.

Следующим важным моментом следует отметить взаимодействие органов внутренних дел с организациями занимающимися разработкой программного обеспечения. Ускорить их взаимодействие с уже существующими системами, которые используют юридические лица в своей деятельности (ярким примером можно считать сервисы Яндекс карт, которые позволяют отслеживать происходящие на дорогах происшествия).

Последним, но не менее важным, стоит выделить взаимодействие органов внутренних дел уже используемыми зарубежными системами, которые не могут навредить суверенитету РФ, но могут разгрузить работу кадрового состава. Системы учёта и хранения данных, а также их

[1] Приказ Минпромэнерго РФ от 07.08.2007 № 311 «Об утверждении Стратегии развития электронной промышленности России на период до 2025 года» // Еженедельник промышленного роста. 2007. № 31

упорядочения в зависимости от критериев выбираемых сотрудниками. Такие системы используются, например, в международных судах- они позволяют не хранить дела в бумажном варианте, а напрямую работать в электронном. Дела сами упорядочиваются в зависимости от сроков подачи, важности и сложности дел.

ЗАКЛЮЧЕНИЕ

По итогам исследования, проведенного в выпускной квалификационной работе, можно сделать вывод, что информационная технология – это процесс, использующий совокупность методов, производственных процессов и программно-технических средств, объединенных технологическим процессом по сбору, хранению, обработке, выводу и распространению информации для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности.

С конца 90-х годов и по настоящее время широко внедряется всемирная паутина Интернет, а также появляются технологии информационных хранилищ, электронного документооборота и поддержки принятия решений.

«Стратегия развития информационного общества», утвержденная Указом Президента РФ от 09.05.2017 № 203, – главнейший стратегический документ для сферы государственных информационных технологий.

В «Стратегии…» определены приоритеты России в сфере информационно-коммуникативных технологий:

6. Формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

7. Развитие информационной и коммуникационной инфраструктуры;

8. Создание и применение российских информационно-коммуникативных технологий, обеспечение их конкурентоспособности на международном уровне;

9. Формирование новой технологической основы для развития экономики и социальной сферы;

10. Обеспечение национальных интересов в области цифровой экономики.

Информационные технологии широко используются в деятельности правоохранительных органов. Однако в настоящее время они требуют совершенствования в том числе на основании международного опыта, которое позволит вывести правоохранительную деятельность на качественно новый уровень.

В рамках выполнения задачи, связанной с внедрением цифровых технологий в сферу государственного управления, предполагается:

– обеспечение функционирования и развития инфраструктуры электронного правительства, внедрение и эксплуатация облачной цифровой платформы обеспечения оказания государственных (муниципальных) услуг и сервисов, в том числе в электронном виде;

– внедрение в деятельность органов государственной власти юридически значимого электронного документооборота с применением электронной подписи;

– создание платформы идентификации, включая биометрическую, облачную квалифицированную электронную подпись, цифровые профили гражданина и юридического лица;

– создание платформы межведомственного взаимодействия и обмена данными;

– введение, функционирование и развитие «электронного паспорта» гражданина Российской Федерации и многое другое.

Подводя итог рассмотрению, следует отметить, что в целях совершенствования нормативно-правовой базы и как следствие общественных отношений в данной области необходимо внести изменения в Федеральный закон от 7 февраля 2011 г. № 3–ФЗ «О полиции», дополнив статью 12 примечанием следующего содержания: «Под массовым мероприятием в целях настоящей статьи необходимо понимать организованное действие (совокупность действий или явлений социальной

жизни) с участием больших групп (масс) людей, которое проводится в общественном месте в регламентируемом государством порядке для удовлетворения их политических, духовных, экономических, культурных, религиозных и других потребностей, являющееся активной формой реализации их прав, свобод и законных интересов». В данном контексте следует отметить, что в связи с нехваткой штатной численности сотрудников наружных служб, в т. ч. в подразделениях ППСП, возрастает общая нагрузка на каждую штатную единицу. В первую очередь это связано с большим количеством заявлений, поданных гражданами по линии «102» и системе «112». Указанная нами проблема является сугубо штатно-организационной и выходит за рамки правовой сферы. Решение данной проблемы, прежде всего, заключается в возрастании стимуляции в процессе привлечения новых кадров в систему Министерства внутренних дел Российской Федерации (далее – МВД России), а именно в подразделения наружных служб, в т. ч. ППСП, создании улучшенных условий труда и обеспечения физической безопасности сотрудников, а также необходимом правовом обеспечении реализации полномочий данной службы и органов внутренних дел в целом.

Весьма высокую тенденцию развития в Российской Федерации получило введение федеральной концепции для реализации государственной политики по обеспечению общественного порядка и общественной безопасности — автоматизированной системы видеонаблюдения, получившей название «Безопасный город». Следует выделить, что введение данной системы создало необходимые условия для своевременного выявления, предупреждения и пресечения административных правонарушений в сфере общественного порядка и общественной безопасности, что оправдывает ее внедрение на федеральном уровне.

Первоначально создание и развитие аппаратно-программного комплекса «Безопасный город» (далее – АПК «Безопасный город») было совместно возложено на Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий

стихийных бедствий (далее – МЧС России) и Федеральную службу охраны Российской Федерации (далее – ФСО России), где ключевая роль в реализации была возложена на МЧС России. Рассматриваемый проект нельзя назвать окончательно удавшимся ввиду образования ряда внутриведомственных и межведомственных разногласий, а также нецелесообразной реализацией выделенного на федеральную концепцию государственного бюджета.

На текущий момент полномочия по координации данного проекта от указанных федеральных ведомств по инициативе главы МЧС России Евгения Зиничева должны быть переданы в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России)[1]. Сама по себе идея федеральной концепции является более чем оправдывающей себя. На текущий момент к АПК «Безопасный город» подключено множество федеральных ведомств, в чью компетенцию входит обеспечение общественного порядка и общественной безопасности, в т.ч. и МВД России.

Таким образом, соответствующие наружные подразделения МВД России имеют круглосуточный доступ к АПК «Безопасный город» и в режиме реального времени имеют возможность для своевременного выявления, предупреждения и пресечения преступлений и административных правонарушений без участия лиц-заявителей о тех или иных противоправных действий.

Данные, полученные от системы, учитываются при расстановке постов, определении маршрутов патрулей. Аппаратно-программный комплекс включает в себя две системы: видеонаблюдение за территорией города и мониторинг автомобилей нарядов. Комплекс позволяет отслеживать движение экипажей и менять маршруты их патрулирования в зависимости от

[1] «МЧС съезжает из «Безопасного города» // Официальный сайт ежедневной газеты «Коммерсантъ-Daily». Режим доступа: https://www.kommersant.ru/doc/4636274. — Загл. с экрана. (дата обращения: 03.03.2021.)

криминогенной обстановки и внезапно возникающих задач[1]. Основной проблемой функционала АПК «Безопасный город» является не повсеместный территориальный охват, а также низкое качество видеосъемки в некоторых участках.

Исходя из изложенного, мы можем сделать вывод, что в большей степени организация и осуществление административной деятельности в области общественного порядка и общественной безопасности подразделениями ППСП обеспечивается благодаря межведомственному взаимодействию, в данном случае нами было рассмотрено взаимодействие с органом исполнительной власти Российской Федерации, ответственным за координацию АПК «Безопасный город».

Также в качестве одной из проблем следует выделить важность профессиональной компетенции сотрудников наружных служб органов внутренних дел. Данный аспект, вне всякого сомнения, влияет на качество сбора материалов по делу об административном правонарушении ввиду того, что сотрудник полиции обязан при исполнении своих служебных обязанностей четко и структурированно оформлять необходимые для административного дела документы, пресекать ненадлежащее исполнение обязанностей иными лицами, чьи действия могут непосредственно влиять в негативном ключе на законность и обоснованность материалов дела об административном правонарушении. В судебной практике имеется множество примеров ненадлежащего сбора материалов, что впоследствии приводило к прекращению производства по делу об административном правонарушении или отмене решений мировых судей.

В качестве примера можно выделить решение Брединского районного суда Челябинской области по делу № 12–30/2017 от 18.08.2017 по жалобе на

[1] Морозов, В.А. Подготовка сотрудников полиции к выполнению профессиональных задач в системе «Безопасный город» / В.А. Морозов // Мир науки, культуры, образования. 2021. № 1 (86). С. 65.

постановление по делу об административном правонарушении[1], согласно которому жалоба истца была удовлетворена в связи с нарушением порядка проведения медицинского освидетельствования на состояние алкогольного опьянения.

Так, же еще один пример. Так, решение Златоустовского городского суда Челябинской области по делу № 12-55/2017 от 16.02.2017 на определение об отказе в возбуждении дела об административном правонарушении в отношении неустановленного лица по ч.1 ст.20.1 Кодекса Российской Федерации об административных правонарушениях, вынесенное 18 января 2017 г. участковым уполномоченным ОП «Новозлатоустовский» ОМВД РФ по ЗГО Челябинской области[2], согласно которому жалоба истца была удовлетворена в связи с отсутствием всестороннего, полного, объективного выяснения всех обстоятельств дела уполномоченным на то лицом.

В данном случае нельзя исключать, что нарушение связано с ненадлежащим исполнением должностных обязанностей сотрудниками медицинского учреждения, осуществлявшего освидетельствование, но, тем не менее, данный факт говорит о том, что порядок проведения процедуры и форму документов необходимо знать и сотрудникам полиции, осуществляющим сбор материалов по делу об административном правонарушении.

Сделаем вывод по главе. Весьма существенным является повышение уровня компетенции сотрудников органов внутренних дел в сфере применения норм административного законодательства.

---

[1] Решение Брединского районного суда Челябинской области по делу № 12–30/2017 от 18 августа 2017 года по жалобе на постановление по делу об административном правонарушении // Информационная система ГАС «Правосудие». 2021.

[2] Решение Златоустовского городского суда Челябинской области по делу № 12-55/2017 от 16 февраля 2017 года по жалобе на определение об отказе в возбуждении дела об административном правонарушении // Информационная система ГАС «Правосудие». 2021.(дата обращения:21.03.2021)

В результате существенных недостатков при составлении протокола по ч. 2 ст. 20.12 КоАП мировым судьей судебного участка № 3 г. Снежинска Челябинской области были возвращены материалы дела об административном правонарушении по делу № 3–958/2018 от 04.12.2018[1].

Отсюда, мы можем сделать вывод, что весьма существенным является повышение уровня компетенции сотрудников органов внутренних дел в сфере применения норм административного законодательства. В данном аспекте мы предлагаем введение ведомственного приказа, направленного на обеспечение штабными и кадровыми подразделениями территориальных отделов органов внутренних дел лекционных занятий по разъяснению применения административного законодательства в области общественного порядка и общественной безопасности среди сотрудников наружных служб с их последующей аттестацией.

Таким образом, полиция оказывает в пределах своих полномочий содействие государственным и муниципальным органам, общественным объединениям и организациям в обеспечении защиты прав и свобод граждан, осуществляет соблюдение законности и правопорядка, а так же оказывает поддержку гражданских инициатив в сфере предупреждения правонарушений и обеспечения правопорядка.

Кодификация национального законодательства в области информационной безопасности может решить проблему систематизации данной сферы государственной и общественной жизнедеятельности.

Важно лишь, чтобы такая кодификация происходила на основе четко разработанных и структурно выстроенных теоретико-методологических основ исследования информационно-безопасного сегмента деятельности государства и гражданского общества.

[1] Определение о передаче дела об административном правонарушении по делу № 3-958/2018 от 04 декабря 2018 года мирового судьи судебного участка № 3 г. Снежинска Челябинской области // Информационная система ГАС «Правосудие». 2021.

Кроме того, теоретическая проблематика информационной безопасности исследуется в рамках современного философско-политологического дискурса, доказывает свою актуальность и в вопросах государственного и общественного управления. Именно информация становится инклюзивным, интегративным, сквозным ресурсом, что позволяет максимально эффективно управлять сообществом в рамках современной информационной цивилизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ 1 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Декларация Четвертой Конференции Министров ВТО в Доха, Катар «Относительно Соглашения TRIPS и общественного здоровья» 2001 г. // Режим доступа: http://www.consultant.ru

2. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. № 237.

3. Федеральный закон от 20.02.1995 № 24–ФЗ (ред. от 10.01.2003) Об информации, информатизации и защите информации // Собрание законодательства РФ. 1995. № 8. Ст. 609. утратил силу

4. Федеральный закон от 27.07.2006 № 152–ФЗ (ред. от 30.12.2020) О персональных данных (с изм. и доп., вступ. в силу с 01.03.2021) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

5. Указ Президента РФ от 20.01.1994 № 170 (ред. от 09.07.1997) Об основах государственной политики в сфере информатизации // Российская газета. 1994. № 19

6. Указ Президента РФ от 09.05.2017 № 203 О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы // Собрание законодательства РФ. 2017. № 20. Ст. 2901

7. Указ Президента РФ от 10.10.2019 № 490 О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // Собрание законодательства РФ. 2019. № 41. Ст. 5700

8. Постановление Правительства РФ от 21.10.2016 № 1083 О внесении изменений в Государственную программу Российской Федерации Информационное общество (2011 – 2020 годы) // Собрание законодательства РФ. 2016. № 44. Ст. 6139

9. Распоряжение Правительства РФ от 01.11.2013 № 2036–р (ред. от 18.10.2018) Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года // Собрание законодательства РФ. 2013. № 46. Ст. 5954.

10. Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // Режим доступа: http://www.consultant.ru (дата обращения:10.04.2021)

11. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр–212) // Российская газета. 2008. № 34. утратил силу

12. Постановление ЦК КПСС и Совета Министров СССР от 20.03.1986 № 361 Об улучшении координации работ в области вычислительной техники и о повышении эффективности ее использования // Режим доступа: http://www.consultant.ru (дата обращения:10.04.2021)

13. Приказ МВД России от 30 марта 2012 г. № 205 Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012 – 2014 годах // Режим доступа: http://www.consultant.ru (дата обращения:10.04.2021)

14. Приказ Минпромэнерго РФ от 07.08.2007 № 311 Об утверждении Стратегии развития электронной промышленности России на период до 2025 года // Еженедельник промышленного роста. 2007. № 31

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

15. Венедиктова, А.А. Влияние информатизации общества на экономическую безопасность государства / А.А. Венедиктова // Сборник статей-презентаций научно-исследовательских работ студентов, магистров, аспирантов, молодых ученых – участников Международной Межвузовской

Студенческой конференции по проблеме «Национальная безопасность как основа конкурентоспособности и экономического роста страны». 2019. С. 51–59.

16. Грейскоп, А.А. Актуальные вопросы цифровизации и информатизации / А.А. Грейскоп // Экономика и бизнес: теория и практика. 2021. № 1–1 (71). С. 81–83.

17. Шеяфетдинова, Н.А. Взаимоотношения государства и общества в фокусе новых технологий и информатизации / Н.А. Шеяфетдинова // Современное право. 2021. № 1. С. 5–10.

18. Архипова Е.А. Применение видеоконференцсвязи в уголовном судопроизводстве России и зарубежных стран сравнительно-правовое исследование: диссертация кандидата юридических наук. URL: https://www.dissercat.com/content/primenenie-videokonferentssvyazi-v-ugolovnom-sudoproizvodstve-rossii-i-zarubezhnykh-stran/read (дата обращения: 30.03.2021)

19. Голованова Н.А. Уголовно- юрисдикционная деятельность в условиях цифровизации: монография. "ИЗиСП", "КОНТРАКТ". 2019. URL:мhttp://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CMB&n=17312#083 77625251830942 (Дата обращения: 30.03.2021)

20. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: Дис канд. юрид. наук. Н.Новгород. 2016. URL: https://search.rsl.ru/ru/record/01006659588 (дата обращения: 30.03.202021)

21. Антонович, Е.К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства российской федерации и законодательства некоторых иностранных государств) / Е.К. Антонович // Актуальные проблемы российского права. 2019. № 6 (103). С. 125–136.

22. Жогин, Н.В. Предварительное следствие в советском уголовном процессе. 1965. 367 с.

23. Журкина, О.В. Доказательства в уголовно-процессуальном законодательстве зарубежных стран. Вопросы российского и международного права. 2016. № 3. С.109–116.

24. Зуев, С.В. Электронное уголовное дело: за и против. Правопорядок: история, теория, практика. 2018. №4(19). С.6–12.

25. Мещеряков, В.А. Формирование доказательств на основе электронной цифровой информации / В.А. Мещеряков // Вестник Воронежского института МВД России. 2018. № 2. С. 108–110.

26. Родивилина, В.А. Использование видеоконференцсвязи при допросе в досудебном производстве / В.А. Родивилина // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. С. 133–138.

27. Россинский, С.Б. Понятие и сущность следственных действий в уголовном судопроизводстве: дискуссия продолжается. Законы России: опыт, анализ, практика.2015. N 2. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=86632#020907250793770316 (дата обращения:10.04.25021)

28. Шейфер, С.А. Следственные действия. Система и процессуальная форма. М.: Юрлитинформ. 2017. 206 с.

29. Шейфер, С. А. Система следственных действий: каковы пути ее развития? Законы России: опыт, анализ, практика. 2017. № 2. С. 5–16.

30. Андреева, О. И. Уголовный процесс: учебник для бакалавриата юридических вузов. Феникс. 2017. 445 с.

31. Гаврилов, А.Н. Следственные действия по советскому уголовно-процессуальному праву. Волгоград: ВСШ МВД СССР, 1975. 112 с.

32. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. 3-е изд., стереотип. Москва : Горячая линия Телеком, 2018. 542 с.

33. Антонов, В. Ф. «Big data»: проблемы, технология обработки и хранения / В. Ф. Антонов, Р. А. Мамедов // Современная наука и инновации. 2015. № 2 (10). С. 50–56.

34. Иванов, А. А. О глубине машинизации права / А. А. Иванов // Закон. 2018. № 5. С. 35–41.

35. Измалкова, С. А. Использование глобальных систем «Big data» в управлении экономическими системами / С. А. Измалкова, Т. А. Головина // Известия Тульского государственного университета. Экономические и юридические науки. 2015. № 4. С. 151–158.

36. Никифорова, Т. С. Оставят ли роботы юристов без работы? / Т. С. Никифорова, К. М. Смирнова // Закон. 2017.№ 11. С. 120 –102.

37. Новикова, О. Ю. Методы и алгоритмы поддержки принятия решений центрами оперативно-розыскной информации : дисс. ... канд. техн. Наук / О. Ю. Новикова. М., 2015.

38. Развитие информационных технологий в уголовном судопроизводстве / под ред. С. В. Зуева. М. : Юрлитинформ, 2018.

39. Созыкин, А. В. Обзор методов обучения глубоких нейронных сетей / А.В. Созыкин // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. 2017. № 3. С. 28–59.

40. Авдеев, В.А. Преступность террористического характера и экстремистской направленности в РФ: состояние и тенденции правового регулирования // Рос. судья. 2018. № 8. С. 18–23.

41. Авдеев, В.А. Правовой плюрализм в оценке делинквентности: проблемы онтологической сущности в российском и зарубежном законодательстве // Междунар. уголовное право и междунар. юстиция. 2018. № 5. С. 3–6.

42. Ильяшенко, А.Н. Особенности использования оперативно-розыскной информации в криминалистической регистрации ОВД // Общество и право. 2011. № 6. С. 26–28.

43. Мечтаков, С.Г. Единая система информационно-аналитического обеспечения деятельности МВД России // Пожарная безопасность: проблемы и перспективы. 2016. № 4. С. 14–17.

44. Цимбал, В.Н. Некоторые вопросы использования сотрудниками полиции информационных технологий // Общество и право. 2015. № 51. С. 321–324.

45. Монгуш, Д.Р. Возраст уголовной ответственности в преступлениях в сфере компьютерной информации / Д.Р. Монгуш // Евразийские исследования: сборник трудов конференции. Сочи, 2018. С. 5–10.

46. Настоящий, А.В. История появления и развития преступлений в сфере компьютерной информации / А.В. Настоящий // Студенческий вестник. 2020. № 7–1. С. 62–63.

47. Новичков, В.Е. Понятие видового и непосредственного объекта неправомерного воздействия на критическую информационную структуру Российской Федерации выражающегося в заведомом создании, распространении и использовании вредоносных компьютерных программ либо иной компьютерной информации (ч. 1 ст. 274.1 УК РФ) / В.Е. Новичков // Европейская наука будущего: сборник трудов конференции. Смоленск, 2019. С. 140–143.

48. Озерский, С.В. и др. Компьютерные преступления: методы противодействия и защиты информации: учебное пособие / С.В. Озерский. Саратов, 2004. С.156 .

49. Пыхтин, И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) / И.Г. Пыхтин // Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48–51.

50. Рахманин, Е.М. Проблемные вопросы терминологии УК РФ, используемой при регулировании вопросов в сфере информационной

безопасности / Е.М. Рахманин // Современные научные исследования и инновации. 2019. № 2. С. 15–17.

51. Рускевич, Е.А. Проблемы систематизации современного уголовного законодательства об ответственности за преступления, совершаемые с использованием инфрмационно-коммуникационных технологий / Е.А. Рускевич // Уголовная политика и правоприменительная практика: сборник трудов конференции. СПб., 2019. С. 351–358.

52. Самигуллина, З.Ф. К вопросу о рассмотрении понятия «информация» как объект уголовно-правовой защиты / З.Ф. Самигуллина // Аллея науки. 2019. № 2. С. 630–633.

53. Сафонов, О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук: 12.00.08 / Олег Михайлович Сафонов. М., 2015. С.222.

54. Смирнов, И.Д. Уголовно-правовое противодействие преступлениям, затрагивающим сферу компьютерной информации, совершенным с использованием сети Интернет / И.Д. Смирнов // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник трудов конференции. Воронеж: Изд-во Воронежского института МВД РФ, 2017. С. 142–144.

55. Строчкина, А.И. Информация как предмет преступления в сфере компьютерной информации / А.И. Строчкина // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 238–243.

56. Токарь, И.Д. Особенности определения и классификации преступника в компьютерных преступлениях / И.Д. Токарь // Синергия Наук. 2018. № 24. С. 899–905.

57. Трунцевский, Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев

и эксплуатантов / Ю.В. Трунцевский // Журнал российского права. 2019. № 5. С. 99 – 106.

58. Шарков, А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08 / Александр Евгеньевич Шарков. Ставрополь, 2004. С.174.

59. Шмалева, К.А. Преступления в сфере компьютерной информации / К.А. Шмалева // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей. Пенза: Наука и Просвещение, 2020. С. 109–111.

60. Шульга, А.В. Преступления в сфере компьютерной информации в зарубежных странах / А.В. Шульга, А.В. Ширинян // Верховенство права и правовое государство: сборник трудов конференции. Уфа: Аэтерна, 2020. С. 46–48

61. Дорофеева, М.М. Международные аспекты противодействия преступлениям в сфере компьютерной информации / М.М. Дорофеева // Международный академический вестник. 2018. № 27. С. 89–93.

62. Евдокимов, К.Н. Субъективная сторона неправомерного доступа / К.Н. Евдокимов // Вестник Академии генеральной прокуратуры РФ. 2009. № 12. С. 61–64.

63. Золотухин, С.Н. Уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие / С.Н. Золотухин, А.З. Хун. Краснодар, 2008. С.180 .

64. Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид.наук: 12.00.08 / Виктор Сергеевич Карпов. Красноярск, 2002. С.202 .

65. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.М. Лебедева. М.: Юрайт, 2014. С.1077 .

66. Курбанов, Г.С. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации / Г.С. Курбанов // Правовая информатика. 2013. № 4. С. 16–18.

67. Лукьянов, Н.Е. Законодательное регулирование ответственности за информационные преступления. Зарубежный опыт / Н.Е. Лукьянов // Устойчивое развитие науки и образования. 2019. № 2. С. 134–139.

68. Лядова, К.Э. Расследование преступлений в сфере компьютерной информации: типичные следственные ситуации / К.Э. Лядова // Евразийское научное объединение. 2018. № 1. С. 160–162.

69. Магомедалиев, Р.А. Объективная сторона преступлений в области компьютерной информации / Р.А. Магомедалиев // Проблемы совершенствования законодательства: сборник научных статей. Махачкала: Алеф, 2020. С. 171–177.

70. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия: учебно-практ. Пособие. М.: Логос, 2002. С.148 .

71. Малышенко, Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Дмитрий Геннадьевич Малышенко. М., 2002. С.166.

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ СУДЕБНОЙ ПРАКТИКИ

72. Постановление Верховного Суда РФ от 19.12.2019 N 71-АД19-8 // Режим доступа: https://koapru.ru (дата обращения:10.04.2021)

73. Постановление мирового судьи судебного участка № 17 Нововаршавского судебном района Омской области // Режим доступа: http://17.oms.msudrf.ru (дата обращения:10.04.2021)

74. Решение № 12-314/2020 от 4 сентября 2020 г. по делу № 12-314/2020 Находкинского городского суда Приморского края // Режим доступа: https://koapru.ru (дата обращения:10.04.2021)

75. Решение № 12-203/2020 от 13 июля 2020 г. по делу № 12-203/2020 Ленинского районного суда г. Н. Новгорода // Режим доступа: https://koapru.ru (дата обращения:10.04.25021)

76. Постановление № 5-114/2020 от 12 мая 2020 г. по делу № 5-114/2020 Хасынского районного суда Магаданской области // Режим доступа: https://koapru.ru (дата обращения:10.04.2021)

77. Официальный интернет-сайт МВД России // Режим доступа: https://мвд.рф (дата обращения:10.04.2021)

ПРИЛОЖЕНИЕ

Результаты анкетирования

В опросе приняли участие 18 человек (100%), из которых 6 (33%) являлись студентами Южно-Уральского государственного университета, а ещё 12 (67%) – сотрудниками правоохранительных органов. Анкетирование проводилось анонимно.

Участникам предлагалось ответить на вопросы, касающиеся внедрения новых информационных технологий в деятельность сотрудников судов.

На вопрос о том, стоит ли увеличить количество цифровой техники на судебных участках, 14 человек (78%) ответили положительно. Отрицательно проголосовали 4 человека (22%).

10 человек (56%) посчитали, что необходимо создание резерва технических устройств на судебных участках, противоположного же мнения придерживаются 8 человек (44%).

9 человек (50%) считали, что необходимо провести обновление программного обеспечения на действующих устройствах, другая половина была против.

14 человек (78%) считают, что стоит применять программное обеспечение используемое в других странах, в то время как всего 4 человека (22%) не согласны с этим; 16 человек (89%) считают возможным внедрение новых технологий в деятельность сотрудников аппарата суда, 2 человека же (11%) посчитали, что такая система улучшений и нововведений не требует.

Среди предложенных способов информирования 10 человек (56%) выбрали самым предпочтительным для себя такое информирование посредством Интернета и социальных сетей; по 3 человека (17%) считают эффективным информирование через размещение плакатов на стендах перед зданиями органов государственной власти, а также через телевидение; по 1 человеку (6%) отметили радио и периодические СМИ.

13 человек (72%) готовы переобучению для использования нового программного обеспечения, обратного мнения придерживаются 5 человек (28%).

Также, участниками опроса были высказаны предложения по вопросу совершенствования нормативно-правового регулирования в сфере

информационных технологий, среди которых такие, как совершенствование законодательства в сфере ИТ, использование сети интернет для раскрытия преступлений.

АНКЕТА

- Укажите ваш пол:

А) мужской

Б) женский

- Укажите ваш возраст:

А) 21-30

Б) 31-40

В) 40 и более

- Укажите род вашей деятельности:

А) студент

Б) сотрудник Правоохранительных органов

В) иная деятельность_____

- Стоит ли увеличить количество цифровой техники на судебных участках?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____

- Необходимо ли создание резерва технических устройств на судебных участках?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____

- Необходимо ли провести обновление программного обеспечения на действующих устройствах?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____

- Стоит ли применять программное обеспечение используемое в других странах?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____

- Как Вы считаете возможно ли внедрение новых технологий в деятельность сотрудников аппарата суда?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____

- Готовы ли вы к переобучению для использования нового программного обеспечения?

А) да

Б) нет

В) затрудняюсь ответить

Г) Другой вариант: _____